



OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F12-03

USE OF EMPLOYMENT-RELATED CRIMINAL RECORD CHECKS: GOVERNMENT OF BRITISH COLUMBIA

Elizabeth Denham
Information and Privacy Commissioner

July 25, 2012

Quicklaw Cite: [2012] B.C.I.P.C.D. No. 16
CanLII Cite: 2012 BCIPC No. 16
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF12-03.pdf

TABLE OF CONTENTS

| | <u>PAGE</u> |
|--|--------------------|
| COMMISSIONER’S MESSAGE | 3 |
| EXECUTIVE SUMMARY | 5 |
| 1.0 PURPOSE AND SCOPE OF REPORT | 7 |
| 1.1 Introduction | 7 |
| 1.2 Investigative Process | 8 |
| 1.3 Application of FIPPA to the Government of British Columbia | 9 |
| 1.4 BC Public Service Security Screening Policy | 9 |
| 2.0 ISSUES IDENTIFIED | 13 |
| 3.0 ANALYSIS | 13 |
| 3.1 Collection of Personal Information | 13 |
| 3.1.1 Personal Information Collected by Government to Perform Checks | 15 |
| 3.1.2 Timing of Government’s Criminal Record Checks | 16 |
| 3.2 Notification Requirements | 25 |
| 3.3 Use of Personal Information | 27 |
| 3.4 Retention of Personal Information | 28 |
| 4.0 FURTHER CONSIDERATIONS | 30 |
| 4.1 Privacy Impact Assessments | 30 |
| 4.2 Publishing Annual Report | 31 |
| 5.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS | 32 |
| 5.1 Summary of Findings | 32 |
| 5.2 Summary of Recommendations | 33 |
| 6.0 CONCLUSIONS | 35 |
| 7.0 ACKNOWLEDGEMENTS | 36 |
| APPENDIX A – BC PUBLIC SECTOR SECURITY SCREENING POLICY | 37 |
| APPENDIX B – BEST PRACTICES FOR PUBLIC SECTOR RECORD CHECKS | 42 |

Commissioner's Message

A growing number of employers are using criminal record checks and police information checks as employment screening tools. For some job seekers, submitting to a record check has become as routine as preparing a resume or providing a list of references.

The reality is that criminal record checks and police information checks are highly privacy invasive. They stand to reveal sensitive personal information about a person's past activities, including prior convictions, penalties or outstanding charges – and in the case of police information checks, details about adverse contact with police, including investigations that do not result in charges and charges approved by Crown Counsel that do not result in convictions.

Privacy concerns are heightened as the storage capacity of information systems continues to grow and information about individuals is increasingly collected and stored within those systems.

The information contained in a record check may have no relevance to the job in question; yet could be the factor that causes an employer to decide not to hire a particular individual.

In my view, there must be a nexus between the job requirements and duties and the proposed record check. Checks should be related to the character of the employment. And where record checks are used, controls must be in place to minimize the privacy implications for affected individuals.

In March 2011, I initiated an investigation into whether public bodies and organizations are conducting employment-related record checks in a manner that is compliant with BC's access and privacy laws and to provide some guidance to employers.

As I moved forward with my investigation, it became clear that the BC government was conducting a significant number of criminal record checks on its employees. In 2010, government expanded its record check policy as a result of a single incident. Today, an estimated 85 per cent of government's 33,500 employees are required to submit to a criminal record check. I initiated this investigation to examine whether government is conducting these record checks in compliance with the *Freedom of Information and Protection of Privacy Act*.

I have made eight recommendations to improve government's practices. Some aspects of the government's record check policy are overly broad and must be refined in order to more effectively target the appropriate employees.

Government must also make changes to its notification policies, in order to accurately explain to individuals who they can contact at government should they have questions about these checks. I have also recommended that government make changes to its policy for ongoing criminal record checks for current employees.

This report also includes **best practices for employment-based record checks**, which will be of use to government as well as other public bodies who use record checks to manage the employment relationship. My office will be releasing best practices for private sector record checks at a future date.

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

Executive Summary

Employers regularly use criminal record checks in their hiring process as one of a number of screening tools to help ensure prospective employees meet standards of honesty and integrity required for positions of trust. They are also used for ongoing monitoring of the behaviour of current employees.

Criminal record checks are inherently privacy invasive. They involve the collection of sensitive personal information about criminal convictions, penalties or outstanding charges. There must be a balance between the legitimate needs of employers and the privacy rights of citizens. The collection, notification, use, and retention of this personal information by public bodies must be compliant with the *Freedom of Information and Protection of Privacy Act* (“FIPPA”).

In an attempt to offer public guidance on the privacy implications of record checks, I decided to conduct an investigation of whether the policy of the Government of British Columbia (“BC”) in relation to its prospective and current employees complies with FIPPA and best practices from a privacy perspective. The government policy that applies to employees appointed under the *Public Service Act* is the subject of this investigation. This policy is separate and distinct from the requirements in the *Criminal Records Review Act* for individuals working or volunteering with children or vulnerable adults. The specific statutory requirements for individuals working with society’s most vulnerable individuals are not at issue in this report.

As a result of this investigation, I found the following aspects of government’s policy as it applies to its prospective and current employees to be among its practices that are consistent with privacy best practices:

- Responsibility for conducting criminal record checks and assessing the relevance of criminal records in relation to job responsibilities, rests with an office that is external to an employee’s working group.
- Police information checks are not required. These are substantially more privacy invasive than criminal record checks in that they also include a search for adverse police contact such as charges approved by Crown Counsel that do not result in convictions and investigations that do not result in charges.
- Government does not require a criminal record check until it has made a conditional offer of employment to an individual.
- Government’s use of criminal record history is compliant with FIPPA [s. 32].

Despite these positive features, government must make changes to its policy to protect the privacy rights of employees and to bring the policy into compliance with FIPPA. My findings and recommendations are as follows:

- Government is collecting more information than is necessary to perform a criminal record check on its prospective and current employees and is not in compliance with FIPPA [s. 26(c)].
- Government's collection of criminal record history for some of its prospective and current employees contravenes FIPPA and it should revise its policy to reduce the number of positions that will require criminal record checks [s. 26(c)].
- Government unnecessarily conducts multiple checks on some employees; for example, on a transfer to a similar position, contrary to FIPPA [s. 26(c)].
- Government does not have authority to re-administer criminal record checks to employees a minimum of every five years. Government should perform ongoing checks not more frequently than every five years and only where an employee exercises a particularly sensitive function that requires ongoing scrutiny.
- Government does not meet the requirements in FIPPA to notify prospective and current employees of the collection of their personal information. It does not clearly set out the information it is collecting and there is no statement regarding the contact information of a government employee who can answer questions from concerned individuals [s. 27(2)].
- Government's retention of the personal information it collects contravenes s. 31 of FIPPA. I recommend that government retain criminal record checks for one year.
- When government makes substantive changes to its criminal record check policy, it should update its privacy impact assessment and provide my office with the opportunity to review and comment on the changes.
- In order to promote openness and transparency, I recommend that government collect statistics and publish an annual report on its practices in relation to criminal record checks.

The current policy of the Government of British Columbia with respect to criminal record checks contravenes FIPPA. It fails to achieve the balance required between its business needs as an employer and the privacy rights of employees. The policy should be rectified in accordance with my recommendations.

I have attached as an appendix to this report a guidance document that sets out best practices for record checks required by employers in the public sector. It is based on the findings and recommendations made in this report.

1.0 PURPOSE AND SCOPE OF REPORT

1.1 Introduction

There is an increasing trend in society towards the use of criminal record checks and police information checks as an employment screening measure.¹ A partial explanation for this trend is an increase in society's security awareness since 9/11.

In the United States, courts have found employers liable for negligent hiring in instances where they have failed to use reasonable care in the employment selection process. There is a perception amongst employers that conducting criminal record checks is a means to reduce the risk of liability for subsequent actions of employees. In Canada, this perception is not supported by case law as Canadian courts have not followed the American model of negligent hiring and no such tort currently exists in Canada.

The primary purpose of criminal record checks is to assist an employer in determining the suitability of an employee, by looking at past conduct, to address possible workplace safety and security issues. However, there is a lack of evidence available on the effectiveness of criminal record checks in the employment context. As such, it is largely an assumption by employers that conducting criminal record checks on prospective and current employees is an effective means by which an employer can prevent subsequent work-related incidents.

Nonetheless, there are studies associated with conducting criminal record checks that show that an individual with a previous criminal record is more likely to commit further crimes than is someone without a criminal record.²

At a minimum, in order for a criminal record check to be a relevant consideration, the offence should relate to the character of the employment. This is reflected in human rights law, where employers in British Columbia ("BC") cannot refuse to employ or to continue to employ an individual because that person has been convicted of an offence that is unrelated to their employment.³

Criminal record checks are highly invasive of the privacy of individuals who are required to submit to these checks in order to be hired or to continue working. As a result, it is critical that the process for record checks balance the legitimate needs of employers with the privacy rights of citizens.

¹ The trend towards increased use of record checks is noted in the Executive Summary of BC Centre for Non-Profit Development's 2010 report titled, "Criminal Record Checks for the Non-Profit Sector in British Columbia".

² See Part 3.1.2 of this report for a further discussion on the nature of this increased likelihood.

³ See s. 13(1) of the *Human Rights Code*.

In an attempt to offer public guidance on the privacy implications of record checks, I initiated an investigation into whether public bodies and organizations are conducting employment-related record checks in a manner that is compliant with privacy legislation. In this investigation report, I focus on whether the Government of British Columbia is conducting criminal record checks in a manner that is compliant with the *Freedom of Information and Protection of Privacy Act* (“FIPPA”).

For clarity, government’s **criminal record check** process involves a search of the federal Canadian Police Information Centre’s (“CPIC”) central database to determine whether an individual has prior criminal convictions, penalties or outstanding charges. A **police information check** (also called a police record check) is broader in scope as it also includes a search of local police databases (i.e. Police Records Information Management Environment (“PRIME”)) for adverse police contact. Adverse police contact includes charges approved by Crown Counsel that do not result in convictions and investigations that do not result in charges. These types of adverse contact have either not been court-tested because the Crown did not lay charges against the individual or contain information that courts have heard and decided was insufficient to result in a conviction. Police information checks are considerably more privacy invasive than criminal record checks and their use by employers results in collection of personal information that is seldom justifiable under privacy legislation in British Columbia.

This report is a privacy analysis of the Government of British Columbia’s criminal record check process in its capacity as an employer with respect to employees appointed under the *Public Service Act*. It does not deal with the requirement for criminal record checks conducted pursuant to the *Criminal Records Review Act* (“CRRRA”) for those working or volunteering with children or vulnerable adults. Because the collection of personal information for those working with society’s most vulnerable individuals is expressly authorized under that Act, it is compliant with FIPPA⁴ and is therefore not at issue in this report.

1.2 Investigative Process

As the Information and Privacy Commissioner for British Columbia (“Commissioner”), I have a statutory mandate to monitor the compliance of public bodies with FIPPA to ensure its purposes are achieved. The purposes, as stated in s. 2(1), are to make public bodies more accountable to the public and to protect personal privacy by, among other things, preventing the unauthorized collection, use or disclosure of personal information by public bodies. Under s. 42(1)(a) of FIPPA, I have the authority to conduct investigations and audits to ensure compliance with any provision of FIPPA.

⁴ See s. 26(a).

In July 2011, I advised the Minister of Justice and the Head of the BC Public Service Agency (“BCPSA”) that my office was investigating the issue of employment-related record checks in British Columbia. The BCPSA oversees the development and implementation of government’s BC Public Service Security Screening Policy (“Policy”), which sets out government’s criminal record check process.⁵ The Personnel Security Screening Office (“PSSO”) of the Ministry of Justice is responsible for conducting criminal record checks on a government-wide basis.

My office provided the BCPSA with an extensive list of questions regarding the Policy and received their written response. My staff subsequently met with the BCPSA on numerous occasions to discuss the Policy.

My staff also met with the Director of Security Services for the PSSO and contacted him on several occasions to further our understanding of government’s process for conducting criminal record checks. We also received a demonstration from the Victoria Police Department on how it performs record checks.

As part of our investigation, we conducted research on record checks with a view towards better understanding the relevant privacy issues. We also contacted numerous lawyers, public bodies and organizations to discuss their use of employment-related record checks.

1.3 Application of FIPPA to the Government of British Columbia

As is stated in s. 3(1), FIPPA “applies to all records in the custody or under the control of a public body”. The record produced from a criminal record check conducted by government is ultimately in the custody or under the control of the PSSO within the Ministry of Justice. The definition of “public body” in Schedule 1 of FIPPA includes “a ministry of the Government of British Columbia”. The Ministry of Justice is a ministry of the Government of British Columbia. As such, FIPPA applies to criminal record checks conducted by the Government of British Columbia.

1.4 BC Public Service Security Screening Policy

In April 2010, the Government of British Columbia created a new BC Public Service Security Screening Policy. The Policy replaced the Public Service Criminal Record Check Policy, which government last revised in March 2009. The main difference in the new Policy is an expansion of the positions that are subject to criminal record checks. It applies to new employees and employees changing positions within government.

⁵ The Security Screening Policy is attached as Appendix A.

Government created the Policy primarily as a result of concerns arising from an incident in 2009 where police recovered records from the home of a government employee which contained the personal information of 1,400 clients of the ministries of Children and Family Development and Housing and Social Development. The Provincial Court of British Columbia subsequently convicted this individual of forging a criminal record check to conceal from government his previous convictions and, by committing this forgery, the Court also found the individual guilty of fraud. The Court did not convict the employee of any misuse of personal information during his employment by government.

In creating the Policy, government expanded on its previous practice and set out its current process for conducting criminal record checks on prospective and current employees. In the new Policy, government identifies 10 types of positions within government that will be subject to a criminal record check (“Designated Positions”). Government believes that approximately 85 per cent of the positions of its 33,682 employees⁶ fit into the descriptions of one or more of these Designated Positions.⁷ I will set out each of these Designated Positions and evaluate whether government’s collection of criminal record history is compliant with FIPPA under Part 3 of this report.

Under the Policy, government requires completion of a criminal record check before it will confirm an applicant for a Designated Position within the public service.

Government does not require a criminal record check until it has made a conditional offer of employment. Nor does government require criminal record checks for positions that do not fit within the criteria of a Designated Position. If prospective employees do not consent to a criminal record check, government will not make an offer of employment.

As is stated in the Policy, government re-administers criminal record checks a minimum of every five years. The requirement for a re-check is included in the offer of employment. If the employee subsequently refuses to consent to a re-check, government can terminate employment.

⁶ This figure was provided to our office by the Public Service Agency. It represents the number of government employees as of October 29, 2011.

⁷ The PSSO has informed my office that each criminal record check conducted by government costs \$20. Based on these numbers, once enough time has passed that the Policy applies to all employees, government will spend an average of almost \$115,000 per year on criminal record checks. This figure does not take into account multiple checks that government does on the same employee. Nor does it account for relevant staffing expenses and operational costs that government also incurs in the process, which I expect would significantly increase government’s yearly expenses on criminal record checks.

Government can also require additional enhanced security screening checks for some applicants in particularly sensitive positions where it believes that a criminal record check is inadequate for addressing the associated risk. Security checks and credit checks are examples of the type of screening that government might require in addition to a criminal record check. Government considers the necessity of the additional screening measures, and approves enhanced security screening checks, on a case-by-case basis. Enhanced security screening checks are beyond the scope of this investigation, but government should assess their privacy impacts as well.

Where a government organization can demonstrate that it will exceed the objectives set out in the Policy, it is not required to apply the specific record check set out in the Policy.

The Policy covers criminal record checks within the Government of British Columbia other than those required under the CRRA.

Process for a Government Criminal Record Check

When an individual receives a conditional offer of employment from government for a job that fits within the criteria of a Designated Position, government asks the prospective employee for written consent to conduct a criminal record check and collects personal information from the individual before conducting the check.⁸

As previously mentioned, the PSSO is responsible for government's record check process. The CPIC database is used to conduct these checks. CPIC is a federal database maintained by the Royal Canadian Mounted Police ("RCMP"). The PSSO does not have access to the CPIC database; it contracts with the RCMP to have criminal record checks performed on its behalf.

The PSSO receives the results of the criminal record check from the RCMP after it sends information such as an individual's name, date of birth, gender and any aliases to the RCMP. If the search of the CPIC database does not show any convictions, penalties or outstanding charges, the PSSO clears the individual for work with the prospective employee's hiring manager.

If, on the other hand, the search of the CPIC database shows the existence of convictions, penalties or outstanding charges, the PSSO receives notification from the RCMP that the search resulted in a positive match for the prospective employee. The RCMP checks a box indicating that convictions, penalties or outstanding charges "May or May Not Exist". The RCMP does not provide the PSSO with any specifics as to the prospective employee's criminal history.

⁸ See Part 3.1.1 of this report for an analysis of the information government collects to conduct a criminal record check.

If the prospective employee does not wish to pursue his/her application further at this point in the process, he/she can choose not to disclose the particulars of the convictions, penalties or outstanding charges to the PSSO. In that case, government will not hire the individual.

Alternatively, the prospective employee can consent to a self-declaration process, whereby he/she informs the PSSO of his/her convictions, penalties or outstanding charges. The PSSO then goes through a process of confirming the prospective employee's self-declaration with the RCMP. In some circumstances, a prospective employee may not have accurately or fully self-disclosed his or her criminal history and may need to revise the self-declaration. At no time does the RCMP provide the PSSO with a written list of the prospective employee's criminal record history. Instead, the RCMP is only able to confirm the accuracy and completeness of the record provided to the PSSO by the prospective employee.

Once the self-declaration process is complete and an accurate history is before the PSSO, it makes a decision as to whether government should hire the prospective employee. The PSSO considers the relevance of any convictions, penalties or outstanding charges when making this decision and compares this information to the risk factors associated with the particular position that government is hiring for. As part of this process, the PSSO may contact the applicant for further information about his or her record and may also contact the hiring manager for further information about the duties of the position to better understand the risks associated with that position.

The PSSO also looks at the amount of time that has passed since an individual's conviction, penalty or outstanding charge as well as rehabilitation measures undertaken by that individual. The PSSO determines relevance on a case-by-case basis. Where necessary, the PSSO discusses the circumstances of a case with the individual before it makes a determination. The PSSO only communicates to the prospective employee's hiring manager whether or not the applicant is "cleared to work" or "not cleared". It does not provide the hiring manager with any specific details regarding the prospective employee's criminal record.

If the PSSO does not clear the prospective employee to work, the hiring manager will write a letter to the individual stating that he/she is not eligible based on the results of the criminal record check. The hiring manager's letter directs the applicant to seek further information from the PSSO regarding government's reasons for not hiring the individual. The letter also informs the applicant of the option of seeking a review from the Deputy Minister within seven days of receipt of the letter. The availability of a review process is also set out in the Policy.

If the individual requests a review of a decision, the hiring manager will forward the request to the Deputy Minister. The Deputy Minister of the hiring ministry conducts the review process.

The PSSO provides the Deputy Minister with a summary setting out that the PSSO found that one or more offences were relevant to the duties and responsibilities of employment.

The prospective employee can provide a submission to the Deputy Minister explaining his or her criminal history and, if applicable, what he or she has done in terms of rehabilitation. The Deputy Minister then makes a final decision as to whether the ministry will hire this individual.

2.0 ISSUES IDENTIFIED

The issues in this investigation are:

1. Does the Government of British Columbia have authority to collect personal information regarding the criminal record history of prospective and current employees? [s. 26 of FIPPA]
2. Does the Government of British Columbia properly notify its prospective and current employees about its collection of personal information? [s. 27(2) of FIPPA]
3. Does the Government of British Columbia have authority for the use of its prospective and current employees' personal information regarding criminal record history? [s. 32 of FIPPA]
4. Does the Government of British Columbia properly retain the personal information of prospective and current employees? [s. 31 of FIPPA]

3.0 ANALYSIS

3.1 Collection of Personal Information

“Personal information” is defined in Schedule 1 of FIPPA as “recorded information about an identifiable individual other than contact information”. At the completion of a criminal record check, the PSSO will have a form that contains details about a prospective employee’s criminal record history. The details on this form may confirm that the individual has no criminal record or may confirm specifics about a criminal record as provided directly from the prospective employee. Regardless, this completed form is “recorded information” under FIPPA. The prospective employee is an “identifiable individual”. As such, the form that results from a criminal record check is personal information of the prospective employee as defined in Schedule 1 of FIPPA.

Issue 1: *Does the Government of British Columbia have authority to collect personal information regarding the criminal record history of prospective and current employees?*

Section 26 of FIPPA sets out the purposes for which a public body may collect personal information. Sections 26(a) to (c) state:

- 26 A public body may collect personal information only if:
- (a) the collection of the information is expressly authorized under an Act;
 - (b) the information is collected for the purposes of law enforcement; and
 - (c) the information relates directly to and is necessary for a program or activity of the public body.

Government relies on s. 26(c) of FIPPA as authority for its collection of personal information relating to employee criminal record checks.⁹

By introducing a requirement of necessity for a public body to collect personal information under s. 26(c) of FIPPA, the Legislature has imposed a high standard. In interpreting this section in Order F07-10, former Commissioner Loukidelis stated:

[48] The collection of personal information by state actors covered by FIPPA ... will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.

[49] At the same time, I am not prepared to accept, as the Complainants contend, that in all cases personal information should be found to be “necessary” only where it would be impossible to operate a program or carry on an activity without the personal information. There may be cases where personal information is “necessary” even where it is not indispensable in this sense. The assessment of whether personal information is “necessary” will be conducted in a searching and vigorous way.

⁹ In very limited instances, such as the s. 55 of the *Gaming Control Act*, government has authority under s. 26(a) of FIPPA to conduct a criminal record check. Section 55 (when read with s. 27 of the *Gaming Control Regulation*) provides government with authority to conduct checks on employees of the Gaming Policy and Enforcement Branch.

In assessing whether personal information is “necessary”, one considers the sensitivity of the personal information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection. In addition, FIPPA’s privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited collection.¹⁰

In looking to whether government has authority for collection of employee criminal record history under s. 26(c) of FIPPA, I must consider whether government’s collection of personal information resulting from its criminal record checks is necessary for the activity of government managing its responsibilities as an employer. In order to make this determination, I must look at the type of personal information collected by government to perform checks as well as the circumstances where government conducts criminal record checks on its employees and prospective employees.

3.1.1 Personal Information Collected by Government to Perform Checks

Government requires that individuals sign a form titled “Consent for Disclosure of Criminal Record Information” prior to a criminal record check taking place.¹¹ On this form, government collects personal information such as an individual’s name, gender and date of birth to pass along to the RCMP before conducting a criminal record check. In addition, government collects information so that it can contact the individual should the need arise during the criminal record check process.

Government also photocopies two pieces of identification from the individual. One of these pieces must be issued by either the Insurance Corporation of British Columbia (“ICBC”) (i.e. driver’s licence or BC identification card), a provincial or territorial government (i.e. Canadian birth certificate) or by the Government of Canada (i.e. passport).

It is not necessary for government to collect photocopies of two pieces of identification to perform a criminal record check. Instead, government should simply examine an individual’s identification to confirm identity and not record any information or retain a copy of any identification. Unnecessary collection of personal information leads to an increased potential for harm such as identity theft from misuse or unauthorized disclosure of this information.

I find that government is collecting more personal information than is necessary to perform a criminal record check on its prospective and current employees and is not in compliance with s. 26(c) of FIPPA.

¹⁰ [2007] B.C.I.P.C.D. No. 15.

¹¹ Government has provided us with a copy of its most recent version of this document dated November 30, 2011.

RECOMMENDATION 1:

I recommend that government only collect the minimum amount of personal information necessary to conduct criminal record checks on prospective and current employees. Government should only examine an individual's identification to confirm identity and not record any information from the identification or retain a copy.

3.1.2 Timing of Government's Criminal Record Checks

Government conducts criminal record checks at various times in the employment relationship for Designated Positions under the Policy. Government performs pre-employment criminal record checks, subsequent checks in situations such as before an employee changes positions or is permanently hired into a position that he or she has been temporarily working in, and also re-checks on employees at least as frequently as every five years.

I will look at each of these types of checks to determine whether government's process is compliant with the collection provisions under FIPPA.

Pre-Employment Criminal Record Checks

A criminal record check is only one element of an employer's screening process. Employers typically employ other methods of assessing suitability, such as interviews and reference checks with previous employers. There is limited data available on the effectiveness of criminal record checks as a pre-employment screening tool. As a result, it is largely an assumption that conducting criminal record checks on prospective and current employees is an effective means by which an employer can prevent subsequent work-related incidents.

There is an assumption associated with conducting criminal record checks that individuals who have offended in the past are relatively more likely to offend in the future. While government has not provided my office with any evidence on this point, research shows that this increased likelihood diminishes over time so that the risk of new offences among individuals who have not offended for six or seven years begins to approximate the risk of new offences among persons with no previous criminal record.¹²

¹² See Kurlychek, M, Brame, R., & Bushway, S., "Scarlet Letters and Recidivism: Does an Old Criminal Record Predict Future Offending?" *Criminology & Public Policy* (2006), Volume 5, Issue 3, pp. 483 – 504 as well as "Enduring Risk? Old Criminal Records and Short-Term Predictions of Criminal Involvement", *Crime & Delinquency* (2007), Volume 53, Issue 1, pp. 64 – 87. Also see Blumstein, A, & Nakamura, K., "Redemption In the Presence of Widespread Criminal Background Checks", *Criminology* (2009), Volume 47, Issue 2, pp. 327 – 359.

It is not necessarily true that an increase in the likelihood to offend will be directly work-related. There can be various aspects to an individual's life that are relevant to a criminal conviction. As such, employers should not assume that any individual with a criminal history is not suitable for employment.

Under BC privacy legislation, employers cannot automatically subject every employee they hire to a criminal record check. Instead, employers must take a more nuanced approach to implementing criminal record checks and ensure that they are not collecting more information than is necessary to determine suitability for employment for each specific position.

It is with this consideration in mind that I will evaluate government's authority under s. 26(c) of FIPPA for the collection of personal information regarding the criminal history of its prospective and current employees.

In assessing the necessity of government's collection of the criminal record history of prospective and current employees, I will consider the sensitivity of the personal information and the amount of personal information collected.

There can be little disputing that an individual's criminal record is highly sensitive personal information. This is an important factor when evaluating the necessity of criminal record checks under FIPPA.

For each prospective and current employee who is applying for a Designated Position, the amount of information collected can vary from simple knowledge that the person does not have a criminal record to knowledge of specifics about a multitude of past convictions, penalties and charges.

In my view, government can implement criminal record checks in a manner that strikes a proper balance between meeting business interests and the privacy of employees by considering whether specific positions are of such a nature that criminal record checks are justifiable under privacy legislation.

I will evaluate each of the Designated Positions in the Policy to evaluate whether government has achieved this balance in a manner that complies with s. 26(c) of FIPPA.

Designated Positions subject to Criminal Record Checks

I have reviewed each of the 10 Designated Positions set out in government's Policy (see Appendix A). As I will explain below, I am satisfied that government's description for Designated Positions 1, 3, 4, 7, 8 and 10 under the Policy is specific enough to target a particular group for whom government is authorized to conduct criminal record checks:

1. **Law enforcement** where duties involve enforcement, investigations, inspections, the control, care and custody of people and/or property, access to sensitive enforcement or investigations information, the administration of the justice system and the prosecution service.
3. Positions with **expense authority** and/or **revenue authority** in excess of \$500,000.
4. Positions with access to, control and/or custody of **significant assets**, where damage to or loss of the asset could cause harm to the Province (e.g., warehouse operations, significant inventories).
7. Positions responsible for and who **have unrestricted access to operational, data and information management systems** where the disruption of such a system could significantly impact the services to citizens and government's financial and economic interests or reveal confidential information.
8. Positions with responsibilities related to government's **financial and economic interests** including those with access to:
 - a. Confidential budget and investment information.
 - b. Cabinet confidence (any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees).
 - c. Legal advice.
 - d. Financial, commercial, scientific, technical or other proprietary information that belongs to the government of BC and that has, or is reasonably likely to have, monetary value.
 - e. Information about intergovernmental relations or negotiations carried on by the government of BC.
10. **Senior executive positions** (Assistant Deputy Minister, Associate Deputy Minister, Deputy Minister, or equivalent).

These six Designated Positions have specific law enforcement responsibilities or unique access to valuable government resources or particularly sensitive government information.

That government requires criminal record checks for these positions appears proportional to government's business purposes in using these checks, the nature of the information government is seeking to protect, and the perceived risks from misuse of this information. As such, it is a reasonable assertion that the nature of the work performed by employees in each of these six Designated Positions justifies government's use of criminal record checks as part of the pre-employment screening process.

With respect to Designated Positions 1, 3, 4, 7, 8 and 10 under the Policy, I find that government's collection of its prospective and current employees' criminal record history is in compliance with s. 26(c) of FIPPA.

On the other hand, I have concerns that I will discuss below regarding government's use of criminal record checks with respect to Designated Positions 2, 5, 6 and 9:

2. Positions responsible for **accessing personal information**.
5. Positions responsible for the **corporate security** and protection of personal and confidential information and assets.
6. Positions responsible for conducting financial, operational and performance **audits**, disciplinary **investigations**, fraud investigations and any other investigations required by policy or provincial statute.
9. Positions with responsibility for interfacing with third-party and/or alternate service delivery organizations where the **third party requires** a criminal record check.

Accessing Personal Information (Designated Position 2)

Personal information is defined in Schedule 1 of FIPPA as "recorded information about an identifiable individual other than contact information". This is a broad definition that can apply to information as sensitive as medical records, financial records and criminal record history. It also includes far less sensitive personal information, such as an individual's name and gender. The harm caused by an unauthorized disclosure of personal information is very much dependent on the nature of the personal information at issue.

In describing Designated Position 2 as "Positions responsible for accessing personal information" there is such a lack of specificity that the particular concern government is trying to address cannot be determined. In fact, the wording of this Designated Position is so broad as to render the nine other Designated Positions largely unnecessary.

Most positions within the public service are “responsible for accessing personal information” and thus, by this provision alone, would require a criminal record check.

I find that government’s collection of its prospective and current employees’ criminal record history for “positions responsible for accessing personal information” contravenes s. 26(c) of FIPPA.

Given the overly broad wording of Designated Position 2, this wording will subject employees to criminal record checks where government’s collection of their criminal record history may not be related directly to or necessary for making a decision to hire an individual for that position.

Rather than conducting criminal record checks, there are other steps the government can take to prevent harm from employee misuse of personal information.

In order to comply with the requirements under s. 33 of FIPPA for disclosure of personal information, government must ensure the access that employees have to personal information is restricted to only those employees who require access and that these employees only gain access to the personal information necessary to perform their duties.¹³

Government must also comply with s. 30 of FIPPA, which requires public bodies to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. To this end, government should ensure that it has measures in place such as logging employee access to sensitive personal information, including an employee’s searching for or viewing of this information. Government should also regularly review the logs to verify that employees are accessing information appropriately and should ensure that employee access of especially sensitive personal information results in an automated supervisor notification.

Corporate security (Designated Position 5)

Designated Position 5 (corporate security) suffers from many of the same problems as I have described above for Designated Position 2 (accessing personal information). In part, this again deals with positions responsible for the protection of personal information. As I have stated above, personal information is too broad of a topic to be overly helpful in describing a position.

Designated Position 8 (financial and economic interests) already addresses confidential information of various types and Designated Position 4 deals with “positions with access to, control and/or custody of significant assets”.

¹³ Also see s. 33.1(1)(e) of FIPPA.

As such, it is not clear what, if any, additional information government is intending to cover with the “confidential information and assets” portion of Designated Position 5 (corporate security).

On the other hand, I understand the rationale for government conducting criminal record checks on positions responsible for corporate security due to the sensitive nature of the work associated with this area.

I find that government’s collection of its prospective and current employees’ criminal record history for positions responsible for the protection of personal and confidential information and assets contravenes s. 26(c) of FIPPA.

The wording of Designated Position 5 (corporate security) is redundant with other Designated Positions in some instances and worded in an overly broad manner in other instances.

Audits and investigations (Designated Position 6)

There appears to be overlap between the various investigations described in Designated Position 6 (audits and investigations) and those set out in Designated Position 1 (law enforcement). Government should re-visit these descriptions to eliminate any unnecessary duplication.

While I can accept that criminal record checks are reasonable for positions responsible for conducting audits and investigations that are required by provincial statute, I do not accept that record checks are justifiable for positions required to conduct audits or investigations that are required by policy. The open-ended nature of policy requirements, as compared to the certainty of provincial statutes, results in a lack of clarity as to the positions that will be subject to criminal record checks.

I find that government’s collection of its prospective and current employees’ criminal record history for positions responsible for various types of audits and investigations required by policy contravenes s. 26(c) of FIPPA.

Third party requires a criminal record check (Designated Position 9)

Designated Position 9 has a fundamental flaw in that government is allowing third parties such as the federal government to dictate when it will conduct criminal record checks on government employees. This should not be the case. Government should determine when it will conduct criminal record checks on its employees and it should ensure that it only conducts record checks when it is authorized by FIPPA to do so.

I find that government’s collection of its prospective and current employees’ criminal record history for “positions with responsibility for interfacing with third-party and/or alternate service delivery organizations where the third party requires a criminal record check” contravenes s. 26(c) of FIPPA.

RECOMMENDATION 2:

I recommend that government cease conducting criminal record checks on the following types of positions as set out in its Security Screening Policy:

- Positions responsible for accessing personal information;
- Positions responsible for the protection of personal and confidential information and assets;
- Positions responsible for conducting financial, operational and performance audits, disciplinary investigations, fraud investigations and any other investigation required by policy; and
- Positions with responsibility for interfacing with third-party and/or alternate service delivery organizations where the third party requires a criminal record check.

Criminal Record Checks Post-Employment

The mere fact that an employee has a change in position or status should not automatically lead to the need for government to conduct a further criminal record check. Government has recognized this as an area of concern under the Policy and is working to address this issue. In November 2011, government made some changes to the interpretation of the Policy in this regard. I believe that these changes do not go far enough and that government should make the changes to the Policy itself.

There may be circumstances where an individual has already had a criminal record check, but government will reasonably request an additional check. It is possible that the PSSO could determine that an identified previous criminal record was not relevant to the characteristics of a previous position, but may be relevant to the new position. An additional check would not be justifiable if government was instead hiring the individual into a new position whose primary function was the same as the individual’s current position.

Government is not entitled to regular updates on an individual’s criminal record history without a justifiable reason for an additional check. Further, additional checks result in government retaining and having to securely store personal information for longer than would otherwise be necessary.

I find that government is unnecessarily conducting multiple criminal record checks on the same employee contrary to s. 26(c) of FIPPA.

RECOMMENDATION 3:

I recommend that government revise its Security Screening Policy to indicate that where an employee has completed a criminal record check, government should not perform an additional check when the employee moves from one position to another:

- for coverage of short-term absences;
- as part of a transfer or hire to a position with substantially similar risk factors; and
- where an employee is being hired permanently into a position that he or she has previously been working on a temporary basis.

Re-Checks Every Five Years

Government's position is that it is not sufficient to conduct a criminal record check only when it hires a person or when the person transfers positions. Instead, government believes it is necessary to collect criminal record check information on a regularly scheduled basis to ensure an employee remains suitable for employment.

Under the Policy, government requires that "criminal record checks must be re-administered a minimum of every five years." This leaves open the potential for multiple checks within a five-year period.

Included in government's offer of employment letter is a requirement that employees notify their manager or supervisor of any arrests, charges or criminal convictions. Nonetheless, it is understood that employees may not always report these occurrences as required.

The Ontario Superior Court of Justice¹⁴ upheld the decision of a labour arbitrator that did not permit the City of Ottawa to conduct criminal record checks on a regularly scheduled basis on all firefighters. Arbitrator M.G. Picher discussed the privacy concerns regarding re-checks as follows:

[42] ...there is a significant distinction between the point of initial hire and the normal course of business in an ongoing employment relationship. The person who presents himself or herself at the door of a business or other institution to be hired does so as a stranger.

¹⁴ *Ottawa (City) v. Ottawa Professional Firefighters Assn.*, [2009] O.J. No. 2914 (S.C.J.).

At that point the employer knows little or nothing about the person who is no more than a job applicant. In my view, the same cannot be said of an individual who has, for a significant period of time, been an employee under the supervision of management. The employment relationship presupposes a degree of ongoing, and arguably increasing, familiarity with the qualities and personality of the individual employee. On the whole, therefore, the extraordinary waiver of privacy which may be justified when a stranger is hired is substantially less compelling as applied to an employee with many months, or indeed many years, of service.¹⁵

There are circumstances where ongoing scrutiny of criminal history can be justified as necessary under FIPPA, but these should be exceptions rather than the norm. For instance, under the CRRA, an individual who works with children or vulnerable adults must receive a criminal record check “at least once every five years”.¹⁶ Other examples where ongoing scrutiny is justifiable include “highly sensitive police or airport services, or as might be expected the services which involve security guards or the handling and transportation of substantial sums of money or other valuable goods.”¹⁷

Arbitrator Picher stated that ongoing checks could be justifiable where “... the employment, by its very nature, is such as to require ongoing scrutiny with respect to the character and trustworthiness of the person exercising a particularly sensitive function.”¹⁸

Once an employer hires an applicant, in most instances the employer should largely be reliant on having in place adequate methods to supervise employee performance. As such, government should not require ongoing criminal record checks for all positions that require a check prior to being hired. Instead, government should only require ongoing checks where the employee exercises a “particularly sensitive function” that requires ongoing scrutiny. For example, from Designated Position 1 (law enforcement), ongoing checks may be justifiable for law enforcement positions with access to sensitive enforcement or investigations information.

I find that government does not have authority under s. 26(c) of FIPPA to re-administer criminal record checks to employees a minimum of every five years.

¹⁵ See *Ottawa (City) v. Ottawa Professional Firefighters Assn. (Criminal Records Check Grievance)* [2007] O.L.A.A. No. 731.

¹⁶ See s. 10(1)(b) of the *Criminal Records Review Act*.

¹⁷ *Supra*, note 15 at para 46.

¹⁸ *Supra*, note 15 at para 44.

RECOMMENDATION 4:

I recommend that government remove the requirement that employees submit to criminal record checks a minimum of every five years. Government should require ongoing checks:

- only where an employee exercises a particularly sensitive function that requires ongoing scrutiny; and
- not more frequently than every five years.

3.2 Notification Requirements**Issue 2: *Does the Government of British Columbia properly notify its prospective and current employees about its collection of personal information? [s. 27(2) of FIPPA]***

Section 27(2) of FIPPA sets out notification requirements that apply to government's collection of the criminal record history of its prospective and current employees. Section 27(2) states:

- 27(2) A public body must ensure that an individual from whom it collects personal information is told:
- (a) the purpose for collecting it;
 - (b) the legal authority for collecting it; and
 - (c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

As I stated in my recent Investigation Report F12-01¹⁹ regarding the ICBC's use of facial recognition technology:

[60] While it is generally understood that public bodies are made more accountable to the public mainly through the access provisions of the Act, the notification provision in s. 27 is also an important accountability mechanism. Without notification, individuals would be unaware of the types of personal information collected and the purposes for the collection and so would be unable to take advantage of their rights to access the information and to request correction or annotation of the information.

¹⁹ [2012] B.C.I.P.C.D. No. 5.

Without proper notification, the public is unable to ensure that their rights under FIPPA are preserved. Individuals with questions regarding government's criminal record check process cannot easily object to the collection of their personal information or ask questions that might help satisfy their concerns.

As stated earlier in this report, government requires that individuals sign a form titled "Consent for Disclosure of Criminal Record Information" prior to a criminal record check taking place. This form has a section entitled "Permission, Waiver and Release" where the employee consents "to a check for records of criminal convictions, outstanding charges, offences or any other documents in the custody of the police, the court, or crown counsel."

Government notes that in some instances the PSSO might need to adjudicate information found as a result of a criminal record check (i.e. where there is a dispute as to the accuracy). In some instances, government states the PSSO is required to investigate "offences or any other documents in the custody of the police, the court, or crown counsel." I believe that such instances must be quite rare.

The description of the check performed by government is actually far broader than the information government collects from the majority of criminal record checks and could cause concerns for employees unnecessarily. It might even dissuade otherwise qualified individuals from completing the application process. Government should revise the consent form to clarify that in most instances it collects information regarding prior criminal convictions, penalties and outstanding charges and that only in exceptional circumstances it has to collect further information.

Government states that it collects this information "for the purposes of determining [the employee's] suitability for a position in the BC Public Service." This is a reasonable explanation of government's purpose for collecting criminal record history information.

Government has accurately stated that its authority for collection of criminal record history information is s. 26(c) of FIPPA.

The consent form provides that "Any questions about the collection and use of this information can be directed to the BC Public Service Agency, HR Services at: MyHR@gov.bc.ca." The form does not include the title, business address and business telephone number of a government employee who can answer questions about government's collection of criminal record history information.

I find that government's notification to prospective and current employees does not comply with s. 27(2) of FIPPA as it does not clearly set out the information government is collecting and there is no statement regarding the title, business address and business telephone number of a government employee who can answer questions about government's collection of criminal record history.

RECOMMENDATION 5:

I recommend that government create a clear notification that it provides prospective and current employees prior to its request for consent to a criminal record check. In addition to the purpose and legal authority for its collection that government has already included, this notification should provide clear wording with respect to its collection of information regarding prior criminal convictions, penalties and outstanding charges. Government must also include the title, business address and business telephone number of an employee who can answer questions about government's collection.

3.3 Use of Personal Information**Issue 3: *Does the Government of British Columbia have authority for the use of its prospective and current employees' personal information regarding criminal record history? [s. 32 of FIPPA]***

Section 32 of FIPPA requires government to ensure that personal information in its custody or under its control is used only in accordance with the limits imposed under that section:

- 32 A public body may use personal information in its custody or under its control only:
- (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34);
 - (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use; or
 - (c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

For positions that fit within the criteria of the Designated Positions, government collects the criminal record history of these prospective employees prior to hiring the individual and “a minimum of every five years” after that. Once the PSSO has ensured through the individual's self-declaration process that it has the entirety of the individual's criminal record history, it uses this information to make a determination as to whether government should hire the individual.

This is precisely the purpose for which government obtained this information and thus is in compliance with s. 32(a) of FIPPA. Government does not use this personal information for any other purpose.

I find that government's use of criminal record history information complies with s. 32 of FIPPA.

3.4 Retention of Personal Information

Issue 4: *Does the Government of British Columbia properly retain the personal information of prospective and current employees? [s. 31 of FIPPA]*

Section 31 of FIPPA sets out a public body's requirements for the retention of personal information as follows:

- 31 If an individual's personal information:
- (a) is in the custody or under the control of the public body;
 - (b) is used by or on behalf of the public body to make a decision that directly affects the individual; and
 - (c) the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.

Public bodies may need to keep records for longer periods in accordance with other legislation such as the *Limitation Act*.

I found that the PSSO's practices differ depending on whether government subsequently hires an individual who has consented to a criminal record check or not.

Where an individual consents to a criminal record check, but government does not subsequently hire him or her, government's practice is that the PSSO retains this individual's record check documentation until after the PSSO has made its decision to not hire the individual and any opportunity for review of the decision has passed. At that time, the PSSO securely disposes of the individual's criminal record check documentation.

Where a record check has been performed and the individual is hired, the PSSO retains the criminal record check documentation until a subsequent re-check is performed (i.e. a change of position has occurred or it has been five years since the last record check).

Section 31 of FIPPA requires that a public body retain an individual's personal information that is in its custody or under its control for at least one year if that information has been used to make a decision directly affecting that individual. Under FIPPA, the purpose of the mandatory one-year retention is to give individuals a reasonable opportunity to gain access to their personal information. Government is not retaining the criminal record checks of individuals that it does not hire for the mandatory one-year period.

In order to be compliant with FIPPA, and to allow people a reasonable time period to request access to their personal information, government needs to retain this information for at least one year.

On the other hand, government is retaining the criminal record checks of individuals who it hires for up to five years, or until it performs a subsequent re-check. While this practice is compliant with the one-year minimum requirement in s. 31 of FIPPA, it does raise concerns with respect to best practices as in some instances there is no apparent reason for government to retain criminal record checks beyond the one-year statutory requirement.²⁰

A more reasonable practice for government is to ensure that the PSSO retains the record checks for one year and, after that time, it only retains documentation that shows when a record check was completed.

An exception to this one-year retention period should be when a criminal record check reveals that an individual has a criminal record, but the PSSO determines this record does not affect the individual's employability. In such instances, government should retain a document noting that it performed a criminal record check as well as a brief summary of the individual's criminal record. This retention will ensure government makes consistent decisions regarding this individual's employability.

I find that government's practice of not retaining criminal record checks for at least one year of individuals who have consented to a check, but subsequently have not been hired, contravenes s. 31 of FIPPA.

RECOMMENDATION 6:

I recommend that government retain criminal record checks for one year after making its decision on whether to hire an individual. One exception is where a check reveals an individual has a criminal record, but government determines that the individual is suitable for employment. In such instances, government should retain a document noting when it performed the check as well as a brief summary of the individual's criminal record.

²⁰ Government retains individuals' consent forms for five years in order to comply with RCMP policy regarding auditing of the process. I do not take issue with this retention.

4.0 FURTHER CONSIDERATIONS

4.1 Privacy Impact Assessments

Too often the decision to conduct a criminal record check fails to consider whether the check is justified in the context of a specific position and does not consider the privacy implications of the check. Government should prepare privacy impact assessments (“PIAs”) to assess and mitigate privacy implications of any new or revised initiatives that involve criminal record checks. Government should treat PIAs as evergreen documents that they review and update on a regular basis as required.

Government completed a PIA regarding the 2010 changes to the Policy, but did not provide it to my office. Had government done so, my office would have had the opportunity to review the PIA and provide comments before government implemented changes to the Policy. While there is not a requirement under FIPPA for government to provide me with this PIA, I believe it is a best practice for programs or initiatives with significant privacy implications. I did not feel it necessary to review the PIA as part of this investigation as it was more useful to review the current Policy.

As government moves through the various stages of determining classes of positions subject to criminal record checks, identifying circumstances where an additional check may be necessary (i.e. for transfer of positions where there are completely different risk factors), and determining the types of positions that might require ongoing checks, it should be documenting and updating its decision-making process in a PIA.

RECOMMENDATION 7:

I recommend that when government makes substantive changes to its criminal record check policy, it update its privacy impact assessment and provide my office with the opportunity to review and comment on the changes.

4.2 Publishing Annual Report

Government does not currently issue a public report on its criminal record check process. Publishing an annual report with statistics of government's record check process would increase government's transparency and align with its Open Government initiative.²¹ Government employees and other citizens, whose tax dollars ultimately fund the record checks, have a vested interest in this process. An annual public report would enable government to analyze statistics and make necessary adjustments to the Policy. Such a report would also be useful to help the public understand the basis for and effectiveness of the Policy.

The annual report should, among other things, include the following information:

- the number of criminal record checks that government has conducted;
- the total cost of the checks conducted that year;
- the results of the checks (i.e. whether a criminal record found was found);
- the number of recommendations from the PSSO to hire or not hire employees based on the results of these checks; and
- the number of requests for review of a decision of the PSSO to not hire, as well as the results of these reviews.

Government should also include in its annual report the following statistics regarding re-checks:

- the number of criminal record re-checks it has performed for each type of re-check (i.e. change of positions, five or more years has passed since last criminal record check);
- for each type of re-check, the number of checks where the results were no different than the initial check; and
- the number of re-checks that resulted in a change to an employee's criminal record history as well as the number of times the PSSO found this change to be relevant to the position of the employee.

Government's annual reports should not personally identify any individuals.

RECOMMENDATION 8:

I recommend that government collect statistics and publish an annual report on its criminal record checks.

²¹ See the B.C. government's Open Information website at: <http://www.openinfo.gov.bc.ca/> and government's Open Data website at: <http://www.data.gov.bc.ca/>.

5.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

5.1 Summary of Findings

I have made the following findings in this investigation:

Government is collecting more information than is necessary to perform a criminal record check on its prospective and current employees and is not in compliance with s. 26(c) of FIPPA.

Government's collection of its prospective and current employees' criminal record history for positions responsible for accessing personal information contravenes s. 26(c) of FIPPA.

Government's collection of its prospective and current employees' criminal record history for positions responsible for the protection of personal and confidential information and assets contravenes s. 26(c) of FIPPA.

Government's collection of its prospective and current employees' criminal record history for positions responsible for various types of audits and investigations required by policy contravenes s. 26(c) of FIPPA.

Government's collection of its prospective and current employees' criminal record history for positions with responsibility for interfacing with third-party and/or alternate service delivery organizations where the third party requires a criminal record check contravenes s. 26(c) of FIPPA.

Government is unnecessarily conducting multiple criminal record checks on some employees under the Policy contrary to s. 26(c) of FIPPA.

Government does not have authority under s. 26(c) of FIPPA to re-administer criminal record checks a minimum of every five years under the Policy.

Government's notification to prospective and current employees does not comply with s. 27(2) of FIPPA. It does not clearly set out the information government is collecting and there is no statement regarding the title, business address and business telephone number of a government employee who can answer questions about government's collection of criminal record history.

Government's use of criminal record history information complies with s. 32 of FIPPA.

Government's practice of not retaining criminal record checks for at least one year of individuals who have consented to a check, but subsequently have not been hired, contravenes s. 31 of FIPPA.

5.2 Summary of Recommendations

RECOMMENDATION 1

I recommend that government only collect the minimum amount of personal information necessary to conduct criminal record checks on prospective and current employees. Government should only examine an individual's identification to confirm identity and not record any information from the identification or retain a copy.

RECOMMENDATION 2

I recommend that government cease conducting criminal record checks on the following types of positions as set out in its Security Screening Policy:

- positions responsible for accessing personal information;
- positions responsible for the protection of personal and confidential information and assets;
- positions responsible for conducting financial, operational and performance audits, disciplinary investigations, fraud investigations and any other investigation required by policy; and
- positions with responsibility for interfacing with third-party and/or alternate service delivery organizations where the third party requires a criminal record check.

RECOMMENDATION 3

I recommend that government revise its Security Screening Policy to indicate that where an employee has completed a criminal record check, government should not perform an additional check when the employee moves from one position to another:

- for coverage of short-term absences;
- as part of a transfer or hire to a position with substantially similar risk factors; and

- where an employee is being hired permanently into a position that he or she has previously been working on a temporary basis.

RECOMMENDATION 4

I recommend that government remove the requirement that employees submit to criminal record checks a minimum of every five years. Government should require ongoing checks:

- only where an employee exercises a particularly sensitive function that requires ongoing scrutiny; and
- not more frequently than every five years.

RECOMMENDATION 5

I recommend that government create a clear notification that it provides prospective and current employees prior to its request for consent to a criminal record check. In addition to the purpose and legal authority for its collection that government has already included, this notification should provide clear wording with respect to its collection of information regarding prior criminal convictions, penalties and outstanding charges. Government must also include the title, business address and business telephone number of an employee who can answer questions about government's collection.

RECOMMENDATION 6

I recommend that government retain criminal record checks for one year after making its decision on whether to hire an individual. One exception is where a check reveals an individual has a criminal record, but government determines that the individual is suitable for employment. In such instances, government should retain a document noting when it performed the check as well as a brief summary of the individual's criminal record.

RECOMMENDATION 7

I recommend that when government makes substantive changes to its criminal record check policy, it update its privacy impact assessments and provide my office with the opportunity to review and comment on the changes.

RECOMMENDATION 8

I recommend that government collect statistics and publish an annual report on its criminal record checks.

6.0 CONCLUSIONS

I am concerned about the societal trend towards increased employment-related criminal record checks without clear evidence as to their benefit. Criminal record checks are among the most privacy invasive of pre-employment screening measures and, where used inappropriately, can result in employers unfairly denying an individual employment. Where employers decide to put in place such a process, it is essential that they respect the privacy rights of the employees subjected to these checks.

By placing the responsibility for conducting criminal record checks with an office that is external to an employee's working group, government has designed a framework that respects the privacy of its employees. The PSSO is able to collect an employee's criminal record history on behalf of government and, where the employee has a criminal record, make a decision based on relevance to the actual nature of the position they are seeking.

The prospective employee's hiring manager does not find out any specific details regarding the prospective employee's criminal record, but instead only whether the PSSO has cleared the individual for hiring. An employee's hiring manager has no need to know specifics of an employee's criminal record history and this process ensures this information is not disclosed to the manager. Further, the PSSO brings a consistency to the decision-making process for determining the relevance of an employee's criminal record history that might otherwise be difficult to achieve.

However, by retaining copies of an employee's identification, government is collecting more personal information from individuals than it requires to conduct a criminal record check. In some instances government is conducting criminal record checks on prospective and current employees that are not justified in the context of a specific position.

Government is not adequately respecting the privacy rights of individuals who after an initial criminal record check have gone on to establish a working relationship with government that makes an additional criminal record check harder to justify. Government also needs to make changes to the notification it provides to employees prior to their giving of consent for a criminal record check.

Government is in a position to dictate terms of employment to those interested in working in the public sector. Where many individuals would otherwise be unwilling to disclose information as sensitive as their criminal record history, employees will often do so if the alternative is that they will not be hired or will not be able to keep their current jobs.

Given the power imbalance that exists in an employment relationship, it is imperative that government's criminal record check process finds a balance that protects both its legitimate business interests as well as the privacy interests of its prospective and current employees. In conducting this investigation I have found that government has not yet achieved this balance.

I have attached as an appendix to this report a document outlining best practices for public sector record checks. My office will be releasing best practices for private sector record checks at a future date.

7.0 ACKNOWLEDGEMENTS

The Government of British Columbia has cooperated fully with our investigation.

Troy Taillefer, Senior Policy Analyst, conducted this investigation and prepared this report.

July 25, 2012

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

OIPC File No.: F11-45048

APPENDIX A:

BC Public Sector Security Screening Policy²²

This policy covers the requirement for criminal record checks and enhanced security screening for designated positions within the BC Public Service. The directive supports the Core Policy of ensuring that “government is supported by a professional public service that has the knowledge, skills, and abilities to achieve current and future objectives.”

This policy covers criminal record checks other than those required under the [Criminal Records Review Act](#). This policy applies to new employees and employees changing positions only.

A criminal record check and enhanced security screening may form part of the process of assessing an applicant’s relative suitability for a designated position. The Canadian Charter of Rights and Freedoms, the Human Rights Code, and Supreme Court of Canada decisions impose strict limits on how the employer uses the information from these records. A criminal record check must relate to the requirements of the position.

A criminal record check is a search for convictions, penalties and outstanding charges as required under this policy.

Successful completion of a criminal record check and/or enhanced security screening is required before an applicant can be confirmed for a designated position within the public service.

A Deputy Minister may require additional enhanced security screening checks for some applicants in particularly sensitive positions by submitting a business case for approval by the Deputy Ministers Committee on the Public Service to ensure corporate consistency. The business cases must be developed in consultation with the Assistant Deputy Minister of Employee Relations, BC Public Service Agency and the Assistant Deputy Minister responsible for Security Programs, Ministry of Public Safety and Solicitor General.

The types of enhanced security screening that may be required include: fingerprinting, RCMP conducted Background Investigations, Professional/Education Verification Checks, Financial/Credit Checks, and any personnel security screening checks required by the Province of BC.

²² The Policy is reproduced as found online at http://www.bcpublicserviceagency.gov.bc.ca/policy/HR_policy/14_Security_Screening.htm.

Purpose of Security Screening

The purpose of security screening is to:

1. Protect the safety and security of vulnerable people in the care of public service employees.
2. Maintain the security and integrity of provincial law enforcement.
3. Protect significant financial and information assets of the province.
4. Maintain the public trust and confidence in public service employees.

Designated Positions

A director, on the recommendation of the hiring manager, will designate positions requiring criminal records checks. The Deputy Minister must approve all designated positions. Positions with the following primary functions must be designated:

1. Law enforcement, where duties involve enforcement, investigations, inspections, the control, care and custody of people and/or property, access to sensitive enforcement or investigations information, the administration of the justice system and the prosecution service.
2. Positions responsible for accessing personal information defined in the Freedom of Information and Protection of Privacy Act as “recorded information about an identifiable individual other than contact information”. Personal information can be about government employees, government clients or others and may be held by government or administered by service providers on behalf of government. Personal information includes, but is not limited to:
 - a. name, home address, home telephone number, home email;
 - b. race, national/ethnic origin, colour, religious or political beliefs or associations;
 - c. age, sex, sexual orientation, marital status;
 - d. identifying number or symbol such as social insurance number or driver’s license number;

-
- e. fingerprints, blood type, DNA prints;
 - f. health care history;
 - g. educational, financial, criminal, employment history;
 - h. anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else.
3. Positions with expense authority and/or revenue authority in excess of \$500,000.
 4. Positions with access to, control and/or custody of significant assets, where damage to or loss of the asset could cause harm to the Province (e.g., warehouse operations, significant inventories).
 5. Positions responsible for the corporate security and protection of personal and confidential information and assets.
 6. Positions responsible for conducting financial, operational and performance audits, disciplinary investigations, fraud investigations and any other investigation required by policy or provincial statute.
 7. Positions responsible for and who have unrestricted access to operational, data and information management systems where the disruptions of such a system could significantly impact the services to citizens and government's financial and economic interests or reveal confidential information.
 8. Positions with responsibilities related to government's financial and economic interests including those with access to:
 - a. confidential budget and investment information;
 - b. cabinet confidence (any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees);
 - c. legal advice;
 - d. financial, commercial, scientific, technical or other proprietary information that belongs to the government of British Columbia and that has, or is reasonably likely to have, monetary value; and;

- e. information about intergovernmental relations or negotiations carried on by the government of British Columbia.
9. Positions with responsibility for interfacing with third-party and/or alternate service delivery organizations where the third party requires a criminal record check.
10. Senior executive positions (Assistant Deputy Minister, Associate Deputy Minister, Deputy Minister, or equivalent).

For additional information, see the Position Security Screening Designation form.

Administration

Applicants must consent to criminal records checks before they are conducted. If applicants do not give their consent, their appointment cannot be confirmed.

Care must be taken to balance the rights of applicants to personal privacy and freedom from discrimination with the government's responsibility to protect the public, employees, and assets. The results of criminal record checks will be held in strictest confidence. Records must be stored in a secure manner and records for applicants who are not hired must be destroyed.

Criminal record checks must be re-administered a minimum of every five years. The requirement for a recheck must be included in the offer of employment letter and is a condition of employment. If the employee refuses to consent to a recheck they can be terminated.

All criminal record checks are conducted by Ministry of Public Safety and Solicitor General Personnel Security Screening Office staff based on the information provided on the criminal record check consent form. If an applicant is found to have a criminal record, the decision on the applicant's suitability for employment will be made by Ministry of Public Safety and Solicitor General staff and the result communicated to the hiring manager.

Deputy Ministers are responsible for the final decision where an applicant requests a review of the decision not to appoint because of his or her record.

Hiring Practice

The BC Public Service recommends best practices in the [Hiring and Deployment Policy Statement](#). This process of evaluating the trustworthiness and reliability of applicants could also include checks of provincial records, where the province maintains information systems related to its own compliance or enforcement activities.

All of the Information gathered during the hiring process will be considered in the adjudication of criminal record check results. This information provides verification of the accuracy of the information the applicant has provided on their background, their reliability and past work performance.

Compliance with *Criminal Records Review Act* Requirements

The [Criminal Records Review Act](#) requires a criminal record check for every employee who works with children under the age of 19 years or works with vulnerable adults as defined under the Act. If a position is designated in accordance with this policy and is also subject to the *Criminal Records Review Act*, and if risk identified for the position relates only to the safety of the children, organizations may choose not to require an additional criminal record check under this policy provided one has been completed under the *Criminal Records Review Act*.

Exceptions

Where an organization can demonstrate that it will exceed the objectives set out in this policy, it will not be obliged to apply the specific record check procedures as set out in this policy.

APPENDIX B:

Best Practices for Public Sector Record Checks

The following best practices are intended to assist public bodies in British Columbia in their efforts to establish an employment-related record check process that is compliant with the *Freedom of Information and Protection of Privacy Act* (“FIPPA”). These best practices are not intended to cover checks required by the *Criminal Records Review Act* for individuals working or volunteering with children or vulnerable adults.

What is a criminal record check?

In the employment context, a criminal record check is a search that employers use to determine whether an individual has prior criminal convictions or outstanding charges. The search is performed by checking information such as an individual’s name, date of birth and gender against the national repository of criminal records maintained by the RCMP.

What is a certified criminal record check?

A certified criminal record check is similar to a criminal record check, except that it requires the individual to submit to fingerprinting before the check is performed. Fingerprints provide the highest level of assurance of completeness and accuracy of a check, but can also result in the unnecessary collection of personal information in many instances where a search of name, date of birth and gender is sufficient.

What is a police information check?

A police information check (also called a police record check) is a comprehensive check of a local police agency’s records management system (which in BC includes the Police Records Information Management Environment (“PRIME”)) as well as the national repository of criminal records maintained by the RCMP. The query might also include a search of court records as well as records management systems in other jurisdictions.

In addition to showing whether an individual has prior convictions or outstanding charges, a police information check also includes adverse police contact such as charges approved by Crown Counsel that do not result in convictions and investigations that do not result in charges.

1. **Conduct criminal record checks and not police information checks.** A public body will seldom have authority under FIPPA to collect the breadth of information found under a police information check [s. 26(c) of FIPPA].
2. **Collect only the minimum amount of personal information necessary to conduct criminal record checks and do not retain a copy of an individual's identification.** Prior to conducting a criminal record check, a public body should limit its collection to that which is necessary to conduct a check [s. 26(c) of FIPPA] – an individual's surname, given name, date of birth, gender and any aliases or previous names. A public body should only examine an individual's identification to confirm identity and not record any information or retain a copy of any identification.
3. **Conduct certified criminal record checks only where criminal record checks are inconclusive.** It will seldom be necessary for public bodies to require individuals to submit to fingerprinting as part of the application process. Public bodies only require this type of record check where the results a criminal record check are inconclusive (i.e. there are multiple potential matches of the original check and the identity of the individual can only be confirmed by fingerprinting).
4. **Criminal record checks should not be required for all positions.** Public bodies should require criminal record checks only for positions with unique access to valuable resources and sensitive information. A public body should determine on a case-by-case basis whether it has the authority under FIPPA to collect personal information regarding the criminal record history of an individual.
5. **Criminal record checks should be only one minor element of an employer's screening process.** Employers should be more reliant on other screening methods to assess employee suitability, such as interviews, oral and/or written examinations, and reference checks.
6. **Ensure that proper notification is given to individuals before a check occurs.** Before an individual agrees to a criminal record check, the public body must ensure that the individual is told: the public body's purpose for collecting criminal record history; the public body's legal authority for collecting this information; and the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection [s. 27(2) of FIPPA].
7. **Conduct criminal record checks on prospective employees only after a public body has made a conditional offer of employment.** Public bodies should not perform criminal record checks at any earlier stage of the hiring process [s. 26(c) of FIPPA].

-
8. **Criminal record check results should go to the individual before they are disclosed to the public body.** Public bodies should not ask individuals to consent to providing record check results directly to them. The individual should receive the results of his or her record check and have the opportunity to review the check for accuracy. Where a potential error exists, the individual will have the opportunity to challenge the results of the criminal record check before he or she discloses the results to the public body. This also gives individuals an opportunity to abandon their pursuit of a job where they do not wish to disclose the results of a record check to the public body.
 9. **Consider the relevance of an individual's criminal record history in relation to the specific requirements of a position.** In the event that a criminal record check reveals that an individual has a previous conviction or outstanding charge, an employer must determine whether this has any effect on the hiring of the individual by considering the characteristics of the position the individual has applied for. Employers should create a list of potentially relevant convictions for the various positions that they will subject to criminal record checks. Employers must not refuse to employ or to continue to employ an individual because that person has a criminal record that is unrelated to their employment. Employers must also consider the amount of time that has passed since any conviction.
 10. **Allow individuals the opportunity to request a review of a decision to not hire them based on the results of a criminal record check.** A public body should ensure that it clearly communicates the availability of a review process to individuals who it decides not to hire after receiving the results of a criminal record check. Someone who was not involved in the initial decision of the public body should conduct the review process.
 11. **Do not use the results of employment-related criminal record checks for any purpose other than to make a hiring decision.** A public body does not have authority under FIPPA for uses that are not consistent with making a hiring decision [s. 32 of FIPPA].
 12. **Set retention periods for criminal record check information.** A public body should not retain an individual's criminal record history indefinitely. Instead, it should retain the results of an individual's criminal record check for one year [s. 31 of FIPPA]. This one-year period should apply whether the individual is subsequently hired or not, with an exception where a check reveals an individual has a criminal record but the public body determines that the individual is nonetheless suitable for employment. In such instances, the public body should retain a document noting when it performed a criminal record check as well as a brief summary of the individual's criminal record. This retention will ensure the public body's future decision-making process is consistent with past decisions regarding this individual's employability.

-
- 13. Do not require unnecessary additional checks on employees who change positions within the public body.** It is not necessary to conduct an additional criminal record check on an employee simply because of a change in position. An additional check may be justifiable where an employee had a criminal record check performed, but the public body subsequently hires him or her into a position with substantially different responsibilities and risk factors.
- 14. Do not automatically require employees to submit to ongoing criminal record checks even where an initial criminal record check prior to hiring is justifiable.** Public bodies should require ongoing checks only where an employee exercises a particularly sensitive function that requires ongoing scrutiny. There is a significant distinction between a public body's ability to justify the need for criminal record checks at the point of initial hire as compared to as part of an ongoing employment relationship. The waiver of privacy which may be justified when hiring a new employee is substantially less compelling when applied to an employee with many years of service.
- 15. Where possible, assign responsibility for the criminal record check process to a central agency such as a human resources department rather than to a supervisor of the prospective employee.** Members of the working group for a prospective employee do not need to know the specifics of the individual's criminal history. As a result, where possible, a public body's human resources department or other central agency should be responsible for its criminal record check process.
- 16. Prepare privacy impact assessments to assess and mitigate privacy implications of any new or revised usage of criminal record checks.** Public bodies should treat privacy impact assessments as evergreen documents that they review and update on a regular basis as required.

This document offers suggested best practices for public bodies to refer to when conducting employment-related criminal record checks. These best practices are for information only and do not constitute a decision or finding by the OIPC with respect to any matter within the jurisdiction of the Information and Privacy Commissioner under the Freedom of Information and Protection of Privacy Act ("FIPPA"). The suggestions do not affect the powers, duties or functions of the Information and Privacy Commissioner regarding any complaint, investigation or other matter under or connected with FIPPA, respecting which the Information and Privacy Commissioner will keep an open mind. Responsibility for compliance with FIPPA remains with each public body.