Privacy Impact Assessment for
Community Safety Unit Update
PIA#AG19044

4Part 1 – General

Name of Ministry:	Ministry of Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter:	Deputy Director, Community Safety Unit		
Email:	Katelyn.mackellen@gov.bc.ca	Phone:	250-387-1751
Program Manager:	Jamie Lipp, Executive Director, Community Safety Unit		
Email:	Jamie.lipp@gov.bc.ca	Phone:	250-387-1751

1. Description of the Initiative

The Community Safety Unit (CSU), under the Policing and Security Branch of the Ministry of Public Safety and Solicitor General, is responsible for compliance and enforcement under the *Cannabis Control and Licensing Act* (referred to as the 'CCLA' or the Act), in regard to those who do not hold a retail licence under the Act. Community Safety Unit officers focus on carrying out compliance and enforcement activities against unlicensed non-medical cannabis retailers and suppliers.

The Community Safety Unit (CSU) can undertake a range of enforcement activities, including conducting inspections, issuing violation tickets, obtaining warrants and issuing demands for information, summoning witnesses, conducting hearings, seizing cannabis, and issuing administrative monetary penalties.

The Director of the CSU may issue a Notice of Administrative Monetary Penalty to those who have sold or produced cannabis without a licence. The Notice of Administrative Monetary Penalty will include information on the alleged contravention(s), the amount of monetary penalty, and the option to sign a waiver which if signed provides that the person waives the opportunity for a hearing, admits to the contravention, and agrees to pay the penalty.

The administrative monetary penalty is equal to two times the retail value of the cannabis sold, produced, or possessed for the purpose of sale. If the person signs the waiver, the administrative monetary penalty is equal to the retail value of the cannabis sold, produced or possessed for the purpose of sale in contravention of the CCLA.

The CSU can also recommend the prosecution of offences under the CCLA. Conviction of a provincial offence under the CCLA can result in fines up to $100,000 for corporations and $50,000 for individuals, imprisonment for up to 12 months, or both. In addition to enforcement action by the CSU, a person illegally selling cannabis may be subject to enforcement action by the police.

Case Management System and Portal

The CSU will be launching a public facing OpenShift online complaint portal (the "Portal") to collect complaints regarding illegal sales of cannabis and related activities. In Summer 2020, CSU will start accepting complaints through the Portal.

Complaints received through the Portal will be automatically loaded into CSU's new case management system, called Community Safety System (CSS). CSS will automatically send emails to complainants acknowledging the receipt of their complaint and only information that is deemed necessary will be collected. All other information will be deleted.

CSS will be a Microsoft Dynamics 365 Customer Relationship Management (CRM) Customer Service application with SharePoint integration for document management. This will provide the ability for applicants to upload and view documents (e.g. investigation notes, photos etc.). CSS will be installed and run on the BC Government Information Technology Infrastructure (i.e. on prem) and CSU employees (e.g. CSU officers, Managers, and administrative staff) will work directly with CSS to carry out their compliance and enforcement duties along with managing the administrative hearing process. Information Systems Branch of the Ministry of Attorney General will develop and maintain CSS.

CSS will support the following business processes:

i. Intake of complaints against individuals and companies suspected of contravening the CCLA, including illegal unlicensed cannabis retailers;
ii. Management of all CSU case files; and
iii. Management of the CSU administrative hearing process.

Payment

1. Monetary Penalties

Individuals that receive an order under the CCLA to pay a monetary penalty will be required to pay that monetary penalty within 30 days of receipt of the order. The CSU will accept payment by way of certified cheque or money order. All payments will be provided to the Corporate Management Services Branch (CMSB) of the Ministry of Public Safety and Solicitor General for processing. Once the payment has been processed and the money transferred to the Ministry of Finance, CMSB will notify Policing and Security Branch (PSB).

2. Reconsideration

Under the CCLA, a person that receives a Compliance Order has the right to apply for a reconsideration of that order. The application fee for applying for reconsideration is $500. The CSU will accept payment of that fee by way of certified cheque, money order, or through online payment using a credit card. The process for certified cheques or money orders will follow the process identified above.

If the individual wants to pay the application fee using their credit card, they will be required to enter their financial information through the Portal. Payment info will be collected on a separate webpage (which will look seamless to the user) than the order page and all payment information (i.e. credit card information) will be sent to the Ministry of Finance through the BC Express Pay 2.0 /Bambora solution. PSB Finance Department will access Bambora to confirm payment and will notify the CSU of the fact that the application fee was paid.

JUSTIN

The CSU will have access to JUSTIN to assist in the management of CSU files that are in the court system. JUSTIN is an integrated case management and tracking system that supports the administration of criminal justice cases from initial submission through to the court process. JUSTIN is managed by the Court Services Branch of the Ministry of Attorney General (CSB) and the BC Prosecution Service (BCPS). It provides a database comprising of almost every aspect of a criminal case, including reports to crown counsel, peace officer scheduling, Crown case assessment and approval, Crown witness notification, court scheduling, recording results, document production, and trial scheduling.

The CSU's application for JUSTIN access was approved by the Justin Access and Security Committee (JACS). The initial application was also reviewed by Court Services Branch, prior to submission to the JACS. The CSU will be a signatory to the JUSTIN Electronic Access Agreement.

Authorized CSU employees will gain access to JUSTIN using individualized Oracle passwords. If the CSU wants to recommend charges to Crown, the Report to Crown Counsel will be uploaded to JUSTIN. If charges are approved by Crown, cases are scheduled through the courts and information on the court process will be submitted and tracked through JUSTIN.

Application for the Return of Seized Cannabis

Pursuant to section 105(4) of the CCLA, non-licensees who have their cannabis seized by a peace officer where it is seized in plain view, or by the CSU, can apply to the Director of the CSU within 30 days after the seizure of the cannabis for the return of the cannabis or for compensation if it was destroyed.

The applicant will send evidence to the Director of the CSU to show that the cannabis was not possessed in contravention of the CCLA. Once an application is received by the CSU, the CSU will satisfy its duty of procedural fairness by disclosing the relevant evidence in its possession to the applicant. That evidence will usually consist of a section 106 report submitted by the peace officer who conducted the seizure, a summary of the police occurrence report, or a summary of the report written by the CSU officer who conducted the seizure. All personal information not belonging to the applicant will be redacted prior to disclosure to the applicant. All evidence will be reviewed by a CSU Administrative Hearing Officer who will write a decision on the outcome of the application. That decision will be provided to the applicant and to the peace officer who conducted the seizure if applicable.

ICBC

The CSU will have an Information Sharing Agreement (ISA) with ICBC. Under that ISA, the CSU have direct access to three databases operated by the Insurance Corporation of British Columbia (ICBC). Those systems are:

a. Motor Vehicle Branch BC Driver's License (MVB BCDL);
b. ICBC Vehicle System; and
c. BCID.

("ICBC Systems")

Access to ICBC Systems will assist CSU officers acting as Special Provincial Constables to identify individuals and vehicles belonging to those suspected of contravening the CCLA and Regulations. The illegal sale, supply, production and possession of cannabis can occur anywhere in British Columbia in businesses and residences as well as through vehicular transport.

Vehicle information will be used by CSU officers to connect a vehicle to a suspect which will be important evidence in connection to an offence. The CSU will have direct access to ICBC Systems so that CSU officers are getting the data efficiently and to ensure that all pertinent information available through ICBC Systems required for their investigations is obtained.

2. Scope of this PIA

This PIA will assess the privacy implications of CSS, payments, access to JUSTIN, direct access to ICBC Systems, and the application for the return of seized cannabis process. A separate PIA has been done on the implementation of the CSU. Note that the information sharing between CSU and the Community Safety Program will be assessed as part of another PIA.

3. Related Privacy Impact Assessments

JAG13045	JUSTIN
PSSG18057	Community Safety Unit
FIN15017	BC Express Pay (BCEP) 2.0 Lite-Banking and Cash Management
FIN12020	BC Express Pay-Banking and Cash Management
FIN12039	TACS V9 Upgrade PIA and Update "TACS V9 Upgrade for the Revenue Transformation Initiative (RTI) Phase 1 Rollout 2 Non-Tax Operations (NTO)"
FIN13029	TACS V9 Upgrade for the Revenue Transformation Initiative (RTI) Phase 1 Rollout 2 Non-Tax Operations (NTO)" PIA update

4. Elements of Information or Data

The CSU will collect, seize or demand several types of information which may include:

- Copies of identification from all persons on the premises;
- Driver's Licence information from Insurance Corporation of British Columbia (ICBC) of owners and affiliates;
- The names, dates of birth, addresses, emails, and phone numbers of all persons on the premises;
- If the illegal unlicensed retail store is in the control of a corporation, the corporate information such as Business Incorporation Numbers, shareholders, partners, directors/officers and their names, titles, addresses, telephone numbers, email addresses, percentages of shares, and types of shares;
- The names of all businesses currently or presently owned by unlicensed retail store owners;
- Assets (vehicles, real property, etc.);
- Banking information;
- Information from BC Land Titles regarding ownership of the building in which the cannabis is being sold;

s.15

s.15

- Information about suppliers or service providers;
- Agreements such as lease agreements, hydro services agreements;
- Emails, letters, and other correspondence which could include information about the sale, supply, production, or storage of cannabis;
- Employee records with names, addresses, salaries, job responsibilities, shift schedules, and dates of employment;
- information from LCRB regarding the licensing status of the retailer;
- Criminal and security clearance information of owners and affiliates;
- Records of tickets, court orders or judgments against the unlicensed retailer, its owners, or affiliates;
- Reports to Crown Counsel;
- Evidentiary disclosure documents from individuals attending administrative hearings or appealing the seizure of their cannabis;
- Payment information from individuals and/or corporations paying payments of administrative monetary penalties or application fees;
- Information from applicants under section 105(4) of the CCLA that shows that the person lawfully possessed the seized cannabis such as purchase receipts and affidavits;
- Any other evidence related to the sale, supply, production, or storage of cannabis; and

- Vehicle registration (current and historical), driver's license information, license plates information, and names, addresses, and other personal information from ICBC Systems.

The CSU will be disclosing a copy of the order to the Ministry of Finance which will include the name of the individual or corporation, the address, and the imposed monetary penalty, and may also provide the following information on a case-by-case basis (if collected by the CSU):

- Names
- Date of birth;
- Date of death;
- Gender;
- Occupation;
- Name and contact information of employer;
- Current, last known and previous residential, business and email address(es), and care of (c/o) addresses;
- Current, last known and previous cellular phone and facsimile numbers, care of (c/o) phone numbers;
- Account/file/reference number(s);
- Driver's License number/BC Identification number;
- BC Services number;
- Business Incorporation Number (BIN);
- Assets (vehicles, real property, etc.);
- Financial institution name, branch, transit and account numbers;
- Liabilities, income, expenses, bankruptcy/insolvency details,
- Account/file number, account balance and status, payments received, payment arrangements negotiated, effective date of balance, interest/penalties and other associated charges, notes and alerts.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information will be stored or located on CSS, BC Government LAN, the Exchange Web Services (EWS) system, and JUSTIN; and will be located within the BC Government infrastructure located on Canadian data centres. This data will only be accessed within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	The citizen or a member of an organization will refer the matter or make a complaint to CSU using the online portal. Note that the information provided in the portal will be automatically stored in CSS. Information gathered by CSU employees will also be entered into CSS manually.	Collection Use	26(b) and (c) 27(1)(c)(iv) 32(a) and (c)
2.	If the information is not relevant, CSU will forward the information to the appropriate agency, if applicable, and delete the information.	No Collection	27.1
3.	CSS will auto-generate an email to the complainant or organization acknowledging the receipt of their information.	Disclosure	33.1(7)
4.	As discussed in the CSU phase one PIA (PSSG18057), CSU will hold administrative hearings which may result in the issuance of a compliance order. Administrative monetary penalties on a compliance order may be paid by cheque or money order. A person may apply for reconsideration of the compliance order and pay the reconsideration application fee by cheque or money order. All payments will be made payable to the Minister of Finance. All cheques or money orders received by the CSU will be sent to the CMSB for processing.	Collection Use Disclosure Collection	26(a) [s.16.1 of the *Financial Administrative Act*] and (c) 32(a) 33.1(1)(i)(i) 33.2(a) and (c) 26(c) 27(1)(b)
5.	Once the payment has been processed and the money transferred to the Ministry of Finance, CMSB will notify Policing and Security Branch (PSB).	Use Disclosure Collection Use	32(a) and (c) 33.1(1)(i.1), 33.2(a), and (c) 26(c) 27(1)(b) 32(a) and (c)

6.	Reconsideration application fees may also be paid by credit card. A person will be required to enter their financial information and personal information through a government-approved online payment portal (BC Express Pay 2.0/Bambora). Payment info will be collected on a separate webpage (which will look seamless to the user) than the order page and all payment information (i.e. credit card information) will be sent to Ministry of Finance through the BC Express Pay 2.0/Bambora portal.	Outside of the scope of this PIA.	Not applicable
7.	The PSB Finance Department will access Bambora to confirm payment and will notify CSU of the fact that the application fee was paid.	Collection Use Disclosure Collection Use	26(c) 27(1)(b) and (c)(iii) 32(a) and (c) 33.1(1)(i.1), 33.2(a) and (c) 26(c) 27(1)(b) and (c)(iii) 32(a) and (c)
8.	CSU may access JUSTIN to upload Reports to Crown Counsel in circumstances where CSU recommends charges to the BCPS.	Out of Scope of FoIPPA	3(1)(h)
9.	CSU investigators may collect information from JUSTIN in cases where a charge has been approved.	Collection Use	26(b) and (c) 27(1)(c)(iv) 32(a) and (c)
10.	The CSU will collect an application for the return of seized cannabis and associated evidence from an applicant applying under section 105(4) of the CCLA for the return of their seized cannabis.	Collection Use Disclosure	26(a) [s.105(4) of CCLA], (b) and (c) 27(1)(a)(iii) and (c)(iv) 32(a) and (c) 33.2(a) and (i)

11.	s.15	Collection	26(a) [s.106 of CCLA], (b) and (c) 27(1)(a)(iii) and (c)(iv)
12.		Use Disclosure	32(a) 33.2(a)
13.	The CSU will provide applicants under section 105(4) of the CCLA with a written decision articulating the outcome of their application. The CSU will also provide the police detachment/department with a copy of the written decision if the cannabis was seized by the police.	Use Disclosure	32(a) and (c) 33.2(a)
14.	When conducting investigations, the CSU will directly access ICBC Systems to run license plates, suspect's names, and obtain vehicle registration and driver's license information to assist in the investigation and to obtain Search Warrants and Production Orders.	Collection Use	26(b) and (c) 27(1)(c)(iv) 32(a) and (c)
15.	If the person has not paid the enforcement related debt within 30 days, CSU notifies Ministry of Finance by accessing their systems so that they can begin collection activities.	Use Disclosure	32(a) 33.1(1)(c) [s. 16.1 of the Financial Administrative Act] and 33.1(1)(i)(i) 33.2(a)
16.	Ministry of Finance will communicate the outcome of the collection activities to CSU, who will enter the information in CSS and update their file.	Collection Use	26(c) 27(1)(c)(iii) 32(a) and (c)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and could use or disclose it for personal purposes.	Oath of Employment Privacy Training Enhanced Criminal Records Checks Standards of Conduct	Low	High
2.	Personal information is compromised when transferred from ICBC to CSU.	The personal information will be collected through direct access to the ICBC Systems.	Low	High
3.	Personal information is compromised when transferred to and from CSB and BCPS.	The personal information will be exchanged through direct access to JUSTIN.	Low	High
4.	Personal information is compromised when transferred to Ministry of Finance.	PSB will have direct access to Ministry of Finance's systems (i.e. Bambora and TACS).	Low	High

10. Collection Notice

A Collection Notice is not required as per section 27(3)(a) and (c) of the *Freedom of Information and Protection of Privacy Act* (FoIPPA) as the personal information, which will be collected directly from the individual, will be collected in the context of law enforcement.

In circumstances when the personal information will not be collected directly from the individual, the indirect collection will be authorized as per section 27(1)(c)(iv) and in some circumstances as per section 27(1)(a)(iii) of FoIPPA and the Collection Notice will not be required as per section 27(3)(c) of FoIPPA.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

s.15

s.15

12. Please describe the technical security measures related to the initiative (if applicable).

CSS, JUSTIN, the LAN and EWS will be on the BC Government infrastructure secured by BC Government firewalls as well as a security multilayered approach, which applies multiple mitigation strategies to protect resources from external and internal threats, will be used to protect the personal information. Sometimes referred to as security-in-depth or layered security, defense-in-depth is a term used to describe the layering of security countermeasures to form a cohesive security environment. The access will be restricted based on roles and responsibilities.

With regard to information located in JUSTIN, users will access the JUSTIN application from a government workstation in a multi-step process. First, they log into their workstations and local network using their government provided IDIR user ID and password. Then they log into the JUSTIN applications with their JUSTIN Oracle user ID and password.

Personal information shared between CSU and CSB, BCPS, and ICBC Systems will be transferred through direct access to JUSTIN and ICBC Systems.

13. Does your branch rely on security policies other than the Information Security Policy?

- Policies prohibiting the sharing of passwords and user ID's
- Policies prohibiting users from posting passwords
- Policies requiring screens to be locked when not in use
- Security incidents must be reported immediately.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

CSS, the CSU LAN, and EWS are only accessible through a valid BC government user ID and password. These are secured via role-based access.

With regard to information located in JUSTIN, the system requires an individual JUSTIN Oracle user ID and password and access is role-based and limited on a need to know basis.

Access to ICBC Systems requires an individual ICBC user ID and password and access is limited to when a CSU officer is acting in their capacity as a Special Provincial Constable and conducting an investigation for the purpose of prosecution.

15. Please describe how you track who has access to the personal information.

CSS will log which users have edited a case, viewed a case and what changes have been made.

CSB has the ability to track access to JUSTIN by providing an audit record of who has accessed court records. Auditing will be undertaken on receipt of a credible complaint, information incident, data quality concerns, criminal or operational intelligence (with data security implications).

ICBC has the ability to track access to ICBC Systems by providing an audit record of who has accessed their systems. ICBC also conducts random audits of those who have access to ICBC Systems.

There will be the ability to track who has accessed the documents on the LAN Drive but there will not be audit logging. Changes to permissions are also tracked, so administrators have a record of who was granted access, by whom and when.

In terms of the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.
- Message Transport logs include message tracking (Exchange server to Exchange server - internal only) which provides a detailed record of message activity, such as sent, received, date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.

- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

If an individual requests that the collected information be changed, the file will be either corrected or annotated and if the personal information was disclosed to another party, the other party will be advised of the request.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Yes, the information will be used for investigations into violations of the CCLA, to determine the outcomes of applications for the return or compensation of seized cannabis, to apply for warrants, court orders, and injunctions, in response to Judicial Review, and to recommend charges to BCPS.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

CSU officers will collect identification from all occupants of illegal cannabis retailer stores and other premises during inspections and investigations to confirm identity. CSU will also review databases such as ICBC and BC Online, as well as information provided to them by the police to confirm validity of the collected information. CSU staff will also be in contact with illegal cannabis retail store owners, their representatives, and their affiliates throughout the duration of the file which will provide multiple opportunities for the staff to confirm the accuracy of the collected personal information.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

CSU is currently working with the Corporate Information and Records Management Office to develop an approved records retention and disposition schedule for the program. In the interim, the personal information collected will be retained for at least two years after it was used to make the decision.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Yes, CSU will be sharing personal information with CSB, BCPS, and ICBC as part of the investigations. An Information Sharing Agreement (ISA) will be developed with ICBC. The information sharing with BCPS and CSB is outside of the scope of the FoIPPA and is within our sector for consistent purpose and as such does not require an ISA.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.	x

Information Sharing Agreement – Required Information	
Description	A regular exchange of personal information between the Ministry of Public Safety and Solicitor General (PSSG), Policing and Security Branch and the ICBC in order to assist in CSU investigations and inspections.
Primary ministry/government agency involved	PSSG
All other ministries/government agencies and public bodies involved	ICBC
Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751
Indication of whether or not personal information is involved	Yes
Start date	Winter 2019
End date (if applicable)	n/a

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative?

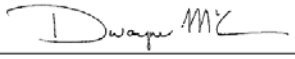
Yes, a PIB will be developed as part of this initiative.

Personal Information Bank – Required Information	
Description	Community Safety Unit files in CSS, a Microsoft Dynamics 365 Customer Relationship Management Customer Service application with SharePoint integration for document management.
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General, Policing and Security Branch
All other ministries/government agencies and public bodies involved	N/A
Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751

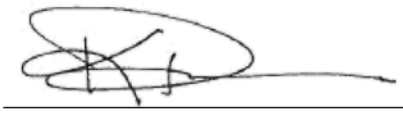
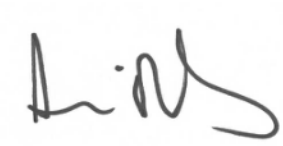
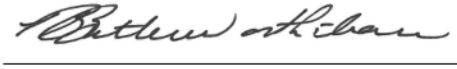
Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Tim Perry		2019-12-06
Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Officer Ministry of Citizens` Services	Signature	Date

Dwayne McCowan		December 10, 2019
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens` Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua		December 11, 2019
Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Ian Bailey		December 12, 2019
Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Jamie Lipp		December 16, 2019
Executive Director of the Community Safety Unit Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date
Brenda Butterworth-Carr		December 20, 2019
Tr'injà shär njit dintlät Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date

Privacy Impact Assessment for

[Title]

PIA# [will be assigned by PCT]

Part 1 – General

Name of Ministry:	Ministry of Public Safety and Solicitor General		
PIA Drafter:	Jenni Bard		
Email:	jenni.bard@gov.bc.ca		778-572-3397
Program Manager:	Jenni Bard		
Email:	jenni.bard@gov.bc.ca		778-572-3397

1. **Description of the Initiative**
   The Director of Police Services is initiating a review, under the authority of s. 42 of the Police Act. The overall purpose of the review is to examine matters related to the Vancouver Police Board's (the Board) response to a Service and Policy complaint (the Complaint) filed jointly by the Union of BC Indian Chiefs (UBCIC) and the BC Civil Liberties Association (BCCLA) regarding street checks by Vancouver Police Department (VPD). The review will consist of two parts:
   · Part A will be focused on a 3rd party study commissioned by the Board to assist in responding to the Complaint. The purpose of Part A is to consider whether the 3rd party study provided the Board with information needed to inform the Board's response to the Complaint, and to undertake further study required to fill gaps.
   · Part B will be focused on the Board's activities in relation to the Complaint. The purpose of Part B is to consider the Board's activities in relation to the 3rd party study, its level of independence from the Vancouver Police Department, and the resources and training available to assist members of the Board in responding to Service and Policy complaints. Part B will produce recommendations for improving the governance capabilities of the Board and all municipal police boards when responding to Service and Policy complaints.
   Consultant services are being sought to complete each of these components through separate Short Requests for Proposals (SRFPs), to be posted on BC Bid.
2. **Scope of this PIA**

3. **Related Privacy Impact Assessments**

4. **Elements of Information or Data**

Existing documents and records that the consultants may require access to include:

- The Complaint as filed with the Police Complaint Commissioner;

- Reports and memos provided to, or produced by, the Board and/or its Service and Policy Complaints Review Committee related to the Complaint, including status reports related to the 3rd party study;
- Documents and records related to the selection of the contractor for the 3rd party study (e.g., the Request for Proposals or other tendering process documents, records documenting the evaluation of responses)
- Board or Service and Policy Complaints Review Committee minutes related to the Complaint;
- The terms of the contract with the successful respondent, Pyxis consulting;
- Draft and final copies of the Pyxis report;
- Records that document and support the conclusions reached in the report, with identifying information removed;
- Publicly available studies, literature and legal opinions related to the practice of street checks in Canada;
- Board policies and procedures related to Service and Policy complaints and the engagement of contractors; and
- Police board training materials, manuals or other resources which are currently used by the Board to provide guidance regarding Service and Policy complaints, or which could be relevant to use moving forward.
- Correspondence from the Police Complaint Commissioner and the Complainants to the Director of Police Services related to the Complaint;

It is anticipated that the consultants may need to collect:

- Business contact information for members of the Board responsible for Service and Policy complaints; VPD staff involved in assisting with or facilitating the 3rd party study or other aspects of the response to the Complaint; staff/consultants of Pyxis Consulting; Policing and Security Branch (PSSG) staff; Office of the Police Complaint Commissioner (OPCC) staff; representatives of the Complainants; and representatives of other organizations or individual persons the consultants determine may have information relevant to the scope of the review.
- information from members of the Board, VPD staff, staff/consultants of Pyxis Consulting concerning what decisions were made and what actions were taken in relation to the Complaint and the 3rd party study and who was involved in those decisions (e.g., decisions about procurement process, the scope and methodology of the 3rd party study, and the process of finalizing the report).

Commented [BJP1]: The consultants will not need to see/use any identifying information in these records – the focus will be whether the process was objective and robust. However, it may be onerous for the Board/VPD staff to remove this information before providing it to the consultants so it's hard to say at this point if we could say 'with identifying information removed'. (it's possible this work will have already been done in response to a FOIPPA request)

Commented [BJP2]: The focus would be on establishing what occurred, clarify events that may not be clear from examining the written records

- Information from representatives of the OPCC and the Complainant concerning the gaps in the Pyxis report and how those gaps might be addressed.

Commented [BJP3]: This information has been provided in writing to the Director; the consultants would need access to this correspondence to inform their work (included in the list of existing records/documents above) but they may also identify a need to delve further into the concerns directly with the Complainants/the OPCC.

- Information from members of the Board, PSB staff and representatives of the OPCC concerning what resources, training or other strategies may help to improve the governance capabilities of police boards with respect to Service and Policy complaints.

Part A may also require the consultant to conduct primary research in order to address gaps in the Pyxis report. This may include collecting information from members of the public about their experiences with street checks or their opinions about street checks. The methodology for this research (if needed) is not known at this time but could include, for example, focus groups or online surveys. Depending on the methodology, identifying information may be needed for the purpose of making arrangements to obtain/submit information about their experiences/opinions however information about their experiences/opinions will not need to be associated with their identifying information and this information will be de-identified as soon as possible and stored in a de-identified manner.

Part 2 – Protection of Personal Information

5. **Storage or Access outside Canada**
6. **Data-linking Initiative***

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	n/a

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.			
2.			
3.			

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes	Privacy Training Standards of Training Criminal Records Check	Low	High
2.	Request may not actually be from client (i.e. their email address may be being used by	Implementation of identification verification procedures	Low	High

	someone else)			
3.	Client's personal information is compromised when transferred to the service provider	Transmission is encrypted and over a secure line	Low	High
4.	Inherent risks in sending personal information to a client via email	Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail	Medium	Medium

10. Collection Notice

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

12. Please describe the technical security measures related to the initiative (if applicable).

13. Does your branch rely on security policies other than the Information Security Policy?

No.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

15. Please describe how you track who has access to the personal information.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.	

Information Sharing Agreement – Required Information	
Description	
Primary ministry/government agency involved	
All other ministries/government agencies and public bodies involved	
Business contact title	
Business contact telephone number	
Indication of whether or not personal information is involved	
Start date	
End date (if applicable)	

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative?

Privacy Impact Assessment for [Title]

PIA# [will be assigned by PCT]

Personal Information Bank – Required Information	
Description	
Primary ministry/government agency involved	Ministry of
All other ministries/government agencies and public bodies involved	
Business contact title	
Business contact telephone number	

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Privacy & Policy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date
Sr. Privacy and Policy Advisor Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Charmaine Lowe A/Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	Date
	Signature	Date
	Signature	Date
Assistant Deputy Minister	Signature	Date

Privacy Impact Assessment for

Livescribe

PIA#PSSG18026

Part 1 – General

Name of Ministry:	Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter:	s.22		
Email:	s.22 @gov.bc.ca	Phone:	s.22
Program Manager:	Ardys Baker, Director, Legislation and Policing Programs		
Email:	ardys.baker@gov.bc.ca	Phone:	250-387-0269

1. **Description of the Initiative**

The Echo Livescribe recording pen ("Livescribe") facilitates digital notetaking and audio recording for professionals who identify as having a written output disability and who cannot produce effective handwritten or typed notes, particularly during meetings. It creates digital recordings of the sound within the room, as well as a PDF file of any visual items that are scribed into the specialized notebook. The user can stop and start the recording by tapping the pen on the notebook. The pen transfers notes and audio to a workstation using a USB connection, has a built in microphone for capturing meetings or lectures and a speaker for playback and recorded audio. Additional specifications include:

- Micro-USB Connector - Transfers notes and audio to your computer and recharges your Smartpen using a USB connection.
- Audio Jack - Standard 3.5mm jack fits your own earphones or the Livescribe 3–D Premium Recording Headset to enable binaural recording.
- OLED Display - High–contrast OLED display.
- Microphone - Capture your meetings or lectures with crisp clear sound.
- Built-in Speaker - Built–in speaker produces rich, full sound to play back your recorded audio.
- Memory Storage - 2GB model holds 200 hours of audio.

The user will only use the Livescribe to record meetings held with members of s.2 work unit and, occasionally, members of other work units within the Branch. The user requires the Livescribe to do s.2 work, as she does not take handwritten notes.

The user will advise all meeting participants that they are being recorded when using the Livescribe. Additionally, the user will pro-actively stop the recording when personal information is discussed.

Furthermore, when discussing information that may fall under cabinet confidence or which would divulge any law enforcement operations, the user will identify in the recording that the information is not to be disclosed.

2. **Scope of this PIA**

The PIA will assess the privacy implications of using Livescribe.

3. **Related Privacy Impact Assessments**

There is no related Privacy Impact Assessments.

4. **Elements of Information or Data**

Recordings and notes may include the names, voices and business contact information of stakeholders and BC Government employees, as well as the substance of information to be provided to Cabinet.

Part 2 – Protection of Personal Information

5. **Storage or Access outside Canada**

The personal information collected will be stored in the Livescribe pen and on the employee's H drive of s.2 government desktop computer, located in the Policing and Security Branch headquarters located in Canada, until it is downloaded on the BC Government infrastructure located within Canada. The information will only be accessed within Canada.

6. **Data-linking Initiative***

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	n/a
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	n/a

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	The employee will use the Livescribe Pen to digitally take notes and record the audio of the room.	Collection	26(c)
2.	The employee will download the gathered information as an mp3 on the BC Government infrastructure.	Use	32(a) and (c)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	The employee could access the personal information and use or disclose it for personal purposes.	Oath of Employment Privacy Training Standards of Conduct Criminal Records Checks	Low	High

2.	The information could be accessed by a third party by having access to the tool.	The Livescribe pen will be stored in a secure storage receptacle in a locked office when not in use.	Low	High
3.	Personal information of meeting participants may be collected as part of the recording.	The user will notify all meeting participants that an audio of the meeting will be recorded and advise them to not share personal information during the meeting. The user will also advise the participants that the recording may be requested under the *Freedom of Information and Protection Privacy Act*. Furthermore, the user will stop the recording in circumstances where participants start sharing personal information.	Low	High

10. Collection Notice

The employee will advise all meeting participant that the Livescribe will digitally take notes and record the audio of the room to support the employee in taking notes of the meeting.
The employee will also advise that there is authority under section 26(c) of the *Freedom of Information and Protection of Privacy Act* to collect the information and that if anyone has any questions about the collection of the information, they can contact her outside of the meeting to discuss.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

The Livescribe pen will be stored in a secure storage receptacle in a locked office when not in use. Access to the office is secured by card access on a 24 hrs basis and the building is monitored by security personnel and video surveillance.

The personal information stored on the H Drive will be located on BC Government servers, located in Canadian datacenters. The datacenters have 24 hour security and access to the buildings and floors is protected by a door access system ran by corporate security. The facilities are surrounded by chain link and barbed wire and access by motorized vehicle involves two sets of gates, neither opening at the same time.

Walk-in access to the buildings requires one to go through a "man trap," which isolates the individual between two locking sets of doors. The man trap is lined with bulletproof glass and Kevlar protection. Government data centres are also located off earthquake zones and flood plains.

12. **Please describe the technical security measures related to the initiative (if applicable).**

    The information on the Livescribe pen will be encrypted and registered to the employee's email, and access to the information will require the individual to log in through the software. Only the employee using the pen will have access to the information.

    The mp3 files will be saved on the employee H Drive which is protected by government firewalls. The Policing and Security branch abides by the 'Need-to-know' principle where access is restricted to authorized Employees that require it to carry out their work.

13. **Does your branch rely on security policies other than the Information Security Policy?**

    No.

14. **Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.**

    The information on the Livescribe pen will be registered to the employee's email and access to the information will require the individual to log in through the software. Only the employee using the pen will have access to the information.

    The Policing and Security branch abides by the 'Need-to-know' principle where access is restricted to authorized Employees that require it to carry out their work.

15. **Please describe how you track who has access to the personal information.**

    Only the user of the Livescribe pen will have access to the collected information.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?**

    The personal information collected will be the voice of the individual which cannot be updated or corrected.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

    No.

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

    N/a

19. **If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

    N/a

Part 5 – Further Information

20. **Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

    No.

21. **Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.**

    No.

22. **Will a personal information bank (PIB) result from this initiative?**

    Yes there will be a temporary PIB on the Livescribe pen.

Personal Information Bank – Required Information	
Description	Voice of meeting participants
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General
All other ministries/government agencies and public bodies involved	None

Business contact title	Ministry of Privacy Officer
Business contact telephone number	250-889-6771

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Simon Munn		July 9, 2018
Privacy Analyst Privacy, Compliance and Training Corporate Information and Records Management Officer Ministry of Citizens` Services	Signature	Date

Dwayne McCowan		July 9, 2018
A/Sr. Privacy and Policy Advisor Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens` Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	July 09, 2018 Date
Ardys Baker Director, Legislation and Policing Programs Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	July 9, 2018 Date
Clayton Pecknold Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	July 9/18 Date

Privacy Impact Assessment for

Community Safety Unit

PIA#PSSG18057

Part 1 – General

Name of Ministry:	Ministry of Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter:	Deputy Director, Community Safety Unit		
Email:	Katelyn.mackellen@gov.bc.ca	Phone:	250-387-1751
Program Manager:	Jamie Lipp, Executive Director, Community Safety Unit		
Email:	Jamie.lipp@gov.bc.ca	Phone:	250-387-1751

1. Description of the Initiative

Non-medical cannabis was legalized in Canada on October 17, 2018. The federal *Cannabis Act* and regulations and the provincial *Cannabis Control and Licensing Act* (CCLA) and *Cannabis Distribution Act* (CDA) and their accompanying regulations form important components of the regulatory regime for non-medical cannabis.

The CCLA and CDA establish provincial control over the sale, supply, and possession of non-medical cannabis. The CCLA and Cannabis Licensing Regulation establish the BC licensing regime for private cannabis retailers. The legislation also establishes restrictions on the possession, personal cultivation, and consumption of cannabis by adults and prohibitions for minors.

Prior to legalization of non-medical cannabis, the responsibility for enforcement action against illegal dispensaries rested with the police, local governments, and the courts, and the nature and extent of enforcement activity against illegal dispensaries varied from community to community. In order to operate legally, all non-medical cannabis retail applicants are required to submit applications for licences under the CCLA, regardless of whether or not they have received a business licence from the appropriate local government and regardless of whether they operated prior to October 17, 2018.

Under the CCLA, the Liquor and Cannabis Regulation Branch (LCRB) of the Ministry of Attorney General reviews applications and issues licences to private non-medical cannabis retailers. The LCRB regulates those licensees and is responsible for enforcement of the regulatory regime in relation to licensees.

Concerns arise that a significant number of illegal cannabis sellers, particularly those operating illegal 'dispensaries' prior to October 17, 2018, may seek to continue retail operations without first obtaining a provincial retail license through LCRB. Enforcement in relation to illegal cannabis retail sellers operating outside of the LCRB licensing regime is within the mandate of the Community Safety Unit (CSU).

The CCLA sets out a compliance and enforcement regime intended to protect children and youth, prioritize public health and safety, and keep organized crime out of the legal non-medical cannabis industry. Under the CCLA, the Minister must appoint a Director. The Director is responsible for the newly established CSU, which operates a regulatory compliance and enforcement program with respect to the sale of cannabis without a licence. The Director's authority in relation to cannabis enforcement matters is established under the CCLA.

The CCLA provides the Director with the authority to undertake a range of activities, including conducting inspections, obtaining warrants and issuing demands for information, summoning witnesses, conducting hearings, seizing cannabis, and issuing administrative monetary penalties. The CSU will have over 40 positions located in four regional offices across the province. The CSU will employ a team of investigators who will be appointed as Special Provincial Constables. Their enforcement activities may result in administrative monetary penalties or provincial or criminal charges for those found in violation of the CCLA.

The CSU is mandated to deliver an effective and fair province-wide cannabis compliance and enforcement program to enhance public safety through compliance and enforcement actions against illegal unlicensed cannabis retailers and other related illegal operations. Public safety objectives will be achieved by:

- Promoting voluntary compliance of provincial cannabis laws through targeted education and awareness activities;
- Delivering an effective province-wide inspection and investigative program in relation to unlicensed cannabis operations;
- Developing and maintaining strong partnerships at the federal, provincial and local levels; and

- Taking enforcement action when necessary, including
    - Issuing administrative monetary penalties and upholding a fair administrative hearing process;
    - Applying to the Supreme Court for injunctions;
    - Seizing cannabis that is possessed illegally;
    - Issuing violation tickets; and
    - Working with the police and making recommendations to the BC Prosecution Service when provincial and/or criminal charges are appropriate.

The CSU receives information regarding illegal unlicensed retailers and other illegal operations from multiple sources. These sources include: members of the public, open source information, community groups, local governments and First Nations, the police, and from the LCRB.

If an unlicensed retailer is suspected of engaging in illegal activity that is within the CSU's jurisdiction, the CSU will obtain information from the LCRB to determine whether the retailer is licensed or if they are in the application process for obtaining a license. If an unlicensed retailer is owned by a corporation, the CSU will obtain corporate information from BC Registries including the names of the Directors. The CSU will contact the police and request information regarding the owners, the corporation, and the unlicensed retailer in order to determine whether there are any ongoing police investigations, and to gather intelligence about potential safety or security issues (e.g. whether weapons or gangs have been associated to a particular unlicensed retailer).

s.15

Once the initial investigation or inspection has begun, CSU investigators will enter premises where illegal selling is believed to be taking place (or has taken place). Information and records, along with illegal cannabis, may be seized pursuant to sections 89, 93 and 101 of CCLA depending on whether it's an inspection or an investigation). That evidence may then be presented to the B.C. Supreme Court in order to apply for injunctions, search warrants, and warrants for the production of records.

The CSU will obtain witness information, including full names, dates of birth, addresses, phone numbers, email addresses and organizations that they are associated with (if applicable). These witnesses may be required to submit written statements or attend oral hearings where their testimony may be recorded. The CSU can also demand a written statement from anyone believed to be selling or producing cannabis illegally or from anyone with information regarding the same as per section 93 of the CCLA.

Pursuant to section 106 of the CCLA, a peace officer that seizes cannabis under the CCLA is required to submit a report to the Director within 10 days of the seizure. The report includes the amount and type of cannabis seized, and details of the offence that led to the seizure, including personal information about the individual from whom the cannabis was seized. Further information about the seizure may be requested by the Director, including the police file, to assist the Director in their determination of whether to take further action against the person who had the cannabis seized by the police.

Using the regulatory powers established under section 94 of the CCLA, the Director may issue a notice of administrative monetary penalty to those who have sold cannabis, or possessed cannabis for the purpose of sale, without a licence. That penalty is equal to up to two times the value of the cannabis sold or possessed for the purpose of sale.

A person who receives the notice has a right to sign a waiver, which reduces the penalty to the actual value of the cannabis sold or possessed for the purpose of sale; however, by signing the waiver they are admitting to the contravention of the CCLA and waiving their right to a hearing. The person has a right to a hearing if they choose not to sign a waiver.

The administrative hearings are conducted by an Administrative Hearing Officer within the CSU. Hearings are conducted primarily through written submissions and occasionally by phone. The Administrative Hearing Officer receives evidence obtained by CSU investigators in addition to evidence from the person from whom the cannabis was seized, prior to producing a written decision. Occasionally, witnesses may be asked to provide written statements or oral testimony over the phone.

After the hearing has been conducted, the Administrative Hearing Officer issues his or her decision to uphold, vary, or rescind the administrative monetary penalty. The Director issues a Compliance Order based on the decision, which outlines the amount of the administrative monetary penalty (if applicable) that the person is required to pay. The person who receives the Compliance Order may apply for reconsideration of the decision by the Director under limited circumstances as per section 95(3) of CCLA.

Individuals from whom cannabis is seized by the CSU, or the police under certain sections of the CCLA, may also apply to the Director within 30 days of the seizure for the return of the cannabis or for compensation if the cannabis was destroyed. The person submits a written application along with applicable evidence to the CSU. The Director will also contact the police for the full police file to assist in their decision. If the Director is satisfied that the cannabis (or a portion of the cannabis) was not possessed by the person in contravention of the CCLA, the Director will return the cannabis or pay compensation to the person if the cannabis was destroyed (if the cannabis was seized by the CSU) or order the police to return the cannabis or pay compensation to the person if the cannabis was destroyed (if the cannabis was seized by the police).

Investigators will also conduct investigations and gather evidence for the purpose of prosecution. Their notes form part of the file. They also write Reports to Crown Counsel (RTCCs) which articulate all evidence obtained in the investigation. Their RTCCs are submitted to the BC Prosecution Service for review when charges are recommended by the CSU.

The CSU is developing a new case management system, but the new system is not yet operational. In the meantime, the CSU will use a manual process for storing and collecting its data, including the use of Excel spreadsheets and storage of documents on a secured LAN drive. An update to the PIA will be submitted when the CSU transitions to the proposed case management system.
With respect to collection of payments, the CSU will receive cheques or money orders for payments of administrative monetary penalties or application fees directly.

Any disclosure documentation related to the hearing process will be submitted or received through email or by regular mail.

2. Scope of this PIA

The PIA will assess the privacy implications of the implementation of the CSU. Note that the PIA will not assess the privacy implications of the video surveillance at the CSU cannabis storage facility. Another PIA will assess that element.

3. Related Privacy Impact Assessments

CITZ17025 - Exchange

4. Elements of Information or Data

The CSU will collect, seize or demand several types of information which may include:

- Copies of identification from all persons on the premises;
- Driver's Licence information from Insurance Corporation of British Columbia (ICBC) of owners and affiliates;
- The names, dates of birth, addresses, emails, and phone numbers of all persons on the premises;
- If the premise is a corporation, the corporate information such as shareholders, partners, directors/officers and their names, titles, addresses, telephone numbers, email addresses, percentages of shares, and types of shares;
- The names of all businesses currently or presently owned by unlicensed retail store owners;
- Information from BC Land Titles regarding ownership of the building in which the cannabis is being sold;
- Criminal intelligence from police related to the unlicensed retailer, its owners, and affiliates;
- Section 106 reports from the police on seizures made under the CCLA;

s.15

s.15

- Agreements such as lease agreements, hydro services agreements;
- Emails, letters, and other correspondence which could include information about the sale, supply, production, or storage of cannabis;
- Employee records with names, addresses, salaries, job responsibilities, shift schedules, and dates of employment;
- information from LCRB regarding the licensing status of the retailer
- Criminal and security clearance information of owners and affiliates;
- Records of tickets, court orders or judgments against the unlicensed retailer, its owners, or affiliates;
- Reports to Crown Counsel;
- Evidentiary disclosure documents from individuals attending administrative hearings or appealing the seizure of their cannabis;
- Cheques, money orders, and credit card information from individuals and/or corporations paying payments of administrative monetary penalties or application fees; and
- Any other evidence related to the sale, supply, production, or storage of cannabis.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information will be stored or located on the BC Government LAN, on the Exchange Web Services (EWS) System, and the Secure File Transfer Service (SFTS) and will be located within the BC Government infrastructure located on Canadian data centres. This data will only be accessed within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	The CSU receives a complaint/tip from various sources including members of the public or the police about a contravention of the CCLA within the CSU's jurisdiction, or receives information through open source research.	Collection Use	26(b) and (c) 27(1)(c)(iv) 32(a) and (c)
2.	The CSU communicates with the LCRB to determine whether the suspected illegal cannabis retailer has a licence or is in the process of obtaining one.	Disclosure Collection Use	33.2(a) and (i) 26(a) [s. 93 of the CCLA], (b) and (c) 27(1)(a)(iii), (b), and (c)(iv) 32(a) and (c)
3.	The CSU receives reports from the police pursuant to section 106 of the CCLA regarding seizures of cannabis under the CCLA.	Collection	26(a) [s. 106 of CCLA], (b) and (c) 27(1)(a)(iii) and 27(1)(c)(iv)
4.	The CSU requests police files related to section 106 reports to determine whether to issue administrative monetary penalties.	Disclosure Collection	33.1(1)(c) [s. 93(2)(b) of the CCLA]26(a) [s. 93 of the CCLA], (b) and (c) 27(1)(a)(iii)and (c)(iv)
5.	The CSU communicates with police agencies to obtain information on individuals and/or businesses regarding potential security or safety risks.	Disclosure Collection	33.2(a) and (i) 26(a) [s. 93 of the CCLA], (b) and (c) 27(1)(a)(iii)and (c)(iv)

6.	In cases where the Director decides to conduct regulatory enforcement, the CSU file, including information provided by the police, is provided to the investigators to conduct an inspection of the suspected illegal cannabis retailer or related operation.	Use	32(a) and (c)
7.	During the inspection, evidence of violations is collected. If the inspection requires entry of premises that are occupied as a residence, consent or a warrant to enter the premises must be obtained before entry.	Collection Use	26(a) [ss. 89 and 91 of CCLA], (b) and (c) 27(1)(a)(iii) 32(a) and (c)
8.	CSU investigators may collect information from several databases including ICBC, the Corporate Registry Director Search, BC Online, BC Land Titles, and Court Services Online.	Collection Use	26(b) and (c) 27(1)(c)(iv) 32(a) and (c)
9.	The CSU provides information collected to a contracted forensic accountant to calculate the value of the cannabis sold or possessed for the purpose of sale. That calculation will determine the amount of administrative monetary penalty assessed.	Disclosure Collection Use	33.2(a) and (c) 26(c) 27(1)(b) 32(a) and (c)
10.	The CSU provides notice of the administrative monetary penalty to all applicable parties.	Outside of the scope of FoIPPA	n/a
11.	A person may sign a waiver where they admit to the contravention and agree to forego a hearing in exchange for a reduced penalty. If they do not sign the waiver they may attend a hearing to dispute the administrative monetary penalty.	Collection	26(c)
12.	If they attend a hearing, a person may supply supporting evidence of their position.	Collection Disclosure	26(c) 33.2(a)
13.	All evidence is reviewed by an Administrative Hearing Officer who writes a final decision. That decision is provided to all applicable parties.	Disclosure	33.2(a)

14.	A person may apply for a reconsideration of the Administrative Hearing Officer's decision and may supply supporting evidence in support of their application.	Collection Disclosure	26(c) 33.2(a)
15.	If the person's reconsideration application is accepted, a new hearing is held, and all evidence is reviewed by the CSU. A new decision is written and provided to all applicable parties.	Disclosure	33.2(a)
16.	A person may apply for Judicial Review of hearing decisions. The record before the decision-maker is supplied to the Supreme Court in defense of the application.	Outside of the scope of FoIPPA	n/a
17.	Evidence is supplied to a Justice to get a warrant or production of record order and to the Supreme Court to get an injunction.	Outside of the scope of FoIPPA	n/a
18.	In cases where the Director decides to investigate for the purposes of prosecution, the file is provided to the investigators to conduct a criminal investigation and develop a Report to Crown Counsel.	Collection Use	26(b) and (c) 27(1)(c)(iv) 32(a) and (c)
19.	For those files going to prosecution, the Report to Crown Counsel outlining all evidence gathered in the investigation is shared with the BC Prosecution Service.	Outside of the scope of FoIPPA	n/a
20.	The investigators may be required to testify in court.	Outside of the scope of FoIPPA	n/a
21.	A person may pay for an enforcement related debt or application for reconsideration fee by submitting a cheque or money order payable to the Ministry of Finance (FIN) to the CSU and the CSU will send the cheque or money order to FIN.	Collection Use Disclosure	26(a) [s. 16.1 of the *Financial Administrative Act*] and (c) 32(a) 33.1(1)(i)(i) 33.2(a)

22.	If the person has not paid the enforcement related debt within 30 days, CSU notifies FIN so that they can begin collection activities.	Use Disclosure	32(a) 33.1(1)(c) [s. 16.1 of the *Financial Administrative Act*] and 33.1(1)(i)(i) 33.2(a)
23.	Individuals may consent to their information being shared with a representative (i.e. legal counsel).	Disclosure	33.1(1)(b)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and could use or disclose it for personal purposes.	Oath of Employment Privacy Training Criminal Records Check Standards of Conduct	Low	High
2.	Information may not actually be from the correct individual.	As part of their investigations, CSU will confirm the identity of the individuals. As part of the investigation/inspection process, individuals will also have the opportunity to correct their personal information (including personal contact details).	Low	High
3.	Personal information is compromised when transferred to the LCRB, police agencies, forensic accountant, or other parties.	The personal information will be shared with the LCRB and the forensic accountant using BC Government email system and with police agencies using the SFTS. Some personal information may also be shared with LCRB by using the BC Government EWS email infrastructure or by phone.	Low	High

10. Collection Notice

A Collection Notice is not required as per section 27(3)(a) and (c) of the *Freedom of Information and Protection of Privacy Act* (FoIPPA) as the personal information, which will be collected directly from the individual, will be collected in the context of law enforcement.

In circumstances when the personal information will not be collected directly from the individual, the indirect collection will be authorized as per section 27(1)(c)(iv) and in some circumstances as per sections 27(1)(a)(iii) and 27(1)(b) of FoIPPA and the Collection Notice will not be required as per section 27(3)(c) of FoIPPA.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

s.15

12. Please describe the technical security measures related to the initiative (if applicable).

EWS, SFTS, and the BC Government LAN will be on the BC Government infrastructure secured by BC Government firewalls as well as a security multilayered approach, which applies multiple mitigation strategies to protect resources from external and internal threats, will be used to protect the personal information.

Sometimes referred to as security-in-depth or layered security, defense-in-depth is a term used to describe the layering of security countermeasures to form a cohesive security environment. The access will be restricted based on roles and responsibilities.

Personal information shared between CSU and LCRB or other BC Government agencies will be transfer over the phone or by email. Necessary personal information disclosed to other relevant parties will use the SFTS and/or telephone.

In the context of email, the EWS system is only accessible through a valid BC Government user ID and password.

13. Does your branch rely on security policies other than the Information Security Policy?

- Policies prohibiting the sharing of passwords and user ID's
- Policies prohibiting users from posting passwords
- Policies requiring screens to be locked when not in use
- Security incidents must be reported immediately.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

The SFTS administrator accounts, the BC Government LAN and EWS systems are only accessible through a valid BC government user ID and password. These are secured via role-based access.

15. Please describe how you track who has access to the personal information.

LAN and SFTS data has complete, real-time audit logs of all system activities. The logging capabilities are being integrated into the Hosting Services Log Aggregation service (ArcSight logger) and will be monitored for irregularities. Log analysis is under the control of the Ministry of Citizen's Services and is outside the scope of this PIA.

In terms of the EWS, Microsoft Exchange generates several logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.

- Message Transport logs include message tracking (Exchange server to Exchange server - internal only) which provides a detailed record of message activity, such as sent, received, date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.

- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

If an individual request that the collected information be changed, the file will be either corrected or annotated and if the personal information was disclosed to another party, the other party will be advised of the request.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Yes, the information will be used to assess penalties, determine the outcomes of appeals for the return or compensation of seized cannabis, to apply for warrants, court orders, and injunctions, in response to Judicial Review, and to recommend charges to BC Prosecution Services.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

CSU investigators will collect identification from all occupants of illegal cannabis retailer stores and other premises during inspections and investigations to confirm identity. CSU will also review databases such as ICBC and BC Online, as well as information provided to them by the police to confirm validity of the collected information. CSU staff will also be in contact with illegal retail store owners and their affiliates throughout the duration of the file which will provide multiple opportunities for the staff to confirm the accuracy of the collected personal information.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

CSU is currently working with the Corporate Information and Records Management Office to develop an approved records retention and disposition schedule for the program. In the interim, the personal information collected will be retained for at least two years after it was used to make the decision.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Yes, CSU will be sharing personal information with the Ministry of Attorney General (AG), Liquor and Cannabis Regulation Branch, Insurance Corporation of British Columbia, Ministry of Finance, and the Police Forces in BC as part of the investigations and Information Sharing Agreements (ISAs) will be developed.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.	x

Information Sharing Agreement – Required Information	
Description	A regular exchange of personal information between the Ministry of Public Safety and Solicitor General (PSSG), Policing and Security Branch and the Ministry of Attorney General (AG), Liquor and Cannabis Regulation Branch in order to confirm licensing status of private non-medical cannabis retailers.
Primary ministry/government agency involved	PSSG
All other ministries/government agencies and public bodies involved	AG
Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751
Indication of whether or not personal information is involved	Yes
Start date	Winter 2019
End date (if applicable)	n/a

Information Sharing Agreement – Required Information	
Description	A regular exchange of personal information between the Ministry of Public Safety and Solicitor General (PSSG), Policing and Security Branch and Police Forces in BC in order to assist in Community Safety Unit investigations.
Primary ministry/government agency involved	PSSG
All other ministries/government agencies and public bodies involved	Police Forces in BC
Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751
Indication of whether or not personal information is involved	Yes
Start date	Winter 2019
End date (if applicable)	n/a

Information Sharing Agreement – Required Information	
Description	A regular exchange of personal information between the Ministry of Public Safety and Solicitor General (PSSG), Policing and Security Branch and the Insurance Corporation of British Columbia (ICBC) in order to assist in Community Safety Unit investigations and inspections.
Primary ministry/government agency involved	PSSG
All other ministries/government agencies and public bodies involved	ICBC
Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751
Indication of whether or not personal information is involved	Yes
Start date	Winter 2019

End date (if applicable)	n/a
Information Sharing Agreement – Required Information	
Description	A regular exchange of personal information between the Ministry of Public Safety and Solicitor General (PSSG), Policing and Security Branch and the Ministry of Finance (FIN) in order to assist in the collection of the enforcement related debts.
Primary ministry/government agency involved	PSSG
All other ministries/government agencies and public bodies involved	FIN
Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751
Indication of whether or not personal information is involved	Yes
Start date	Winter 2019
End date (if applicable)	n/a

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative?

Yes, a PIB will be developed as part of this initiative.

Personal Information Bank – Required Information	
Description	Community Safety Unit Files
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General, Policing and Security Branch
All other ministries/government agencies and public bodies involved	N/A

Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751

Personal Information Bank – Required Information	
Description	Forensic Accountant Community Safety Unit Files
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General, Policing and Security Branch
All other ministries/government agencies and public bodies involved	N/A
Business contact title	Deputy Director, Community Safety Unit
Business contact telephone number	250-387-1751

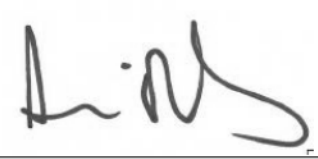
Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Cole Lance		January 15, 2019
Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Officer Ministry of Citizens` Services	Signature	Date

Quinn Fletcher		January 23, 2019
Director, Operations and Privacy Management Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens` Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua		January 31, 2019
Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Ian Bailey		January 31, 2019
Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Jamie Lipp		February 1, 2019
Executive Director of the Community Safety Unit Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date
Tonia Enger		Feb 11, 2019
A/Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date

Privacy Impact Assessment for Pill Press and Related Equipment Control Program

PIA#PSSG18062

Part 1 - General

Name of Ministry:	Ministry of Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter and Program Manager:	Heather Stewart, Director Security Services, Security Programs Division		
Email:	Heather.Ann.Stewart@gov.bc.ca	Phone:	(250) 356-1512

1. Description of the Initiative

There has been a marked increase in opioid overdoses in BC. In 2017, there were 1,422 suspected drug overdose deaths. This is a 43% increase from the number of overdose deaths in 2016 (993), and a 528% increase since 2012 (269). The number of illicit drug overdose deaths in 2017 equates to about 3.9 deaths per day for the year.

Overdose deaths without fentanyl have remained relatively stable since 2011, providing evidence that fentanyl is directly related to the surge of overdoses in the province. Fentanyl can be bought very cheaply and made into counterfeit pills with pill press, tableting, and other pharmaceutical equipment. These pills have a very high resale value, creating a sizable incentive for drug traffickers to introduce fentanyl into the illicit drug market. Poor quality control over opioid dosage in these pills, and the presence of opioids in non-opioid counterfeit medication, are thought to be contributing significantly to higher opioid overdose and death rates in BC.

The federal government passed Bill C-37 to prohibit the unregistered importation of designated devices that may be used in the illicit manufacture of controlled substances, such as pill presses and encapsulators. However, representatives of law enforcement find this is insufficient to address the counterfeit pill problem as it does not restrict ownership, use, or resale of pill press equipment once it enters Canada.

In May 2018, BC passed the *Pill Press and Related Equipment Control Act* (PPRECA) to restrict access to pill press ownership, use, and possession to those with a legitimate business or professional purpose, such as production of drugs or natural health food products, those given a waiver to produce other products that rely on this technology, and registered pill-press sellers. This will be done through the creation of a regulatory program managed by the Security Program Division (SPD) of the Policing and Security Branch of the Ministry of Public Safety and Solicitor General in which the Registrar will regulate the registration, possession, use, and resale of controlled equipment.

PPRECA also sets out significant penalties for offences committed in relation to controlled equipment and activities and notification requirements for when businesses acquire and dispose of the equipment, as well as powers to appoint inspectors, so that compliance with the legislation can be monitored. All of the provisions will make it easier to track where controlled equipment is, and easier to take it out of the hands of those who are not authorized owners.

The Pill Press Online Registry will support the following processes and registries:

- Application to become a waiver holder
- Application to become a registered seller
- Confirmation of authorized owners
- Registry of waiver holders
- Registry of registered sellers
- Registry of authorized owners
- Notifications of equipment (i.e. inventory of equipment)
- Reporting sales of equipment (i.e. sales and purchases)
- Change to equipment (i.e. lost, stolen, or destroyed)
- Registries of equipment locations, and changes to locations
- Inspection of controlled equipment
- Public complaints and investigations

This program will utilize an OpenShift online application portal which will be integrated with a Microsoft Dynamics 365 Customer Relationship Management Service application with SharePoint integration for document and case management. The system, called Paprika, will be installed and run on the BC Government Information Technology infrastructure. Data submitted through the application portal will only persist within the case management system. The portal will have a landing page that will guide users to the relevant application links. The portal will also contain interactive screens that will allow clients to change business information, review owner category information, and equipment inventories. Paprika will make an application programming interface (API) call to write the information into the case management system every time a user changes interactive screens on the portal.

Authentication

The Provincial Identity Information Management (IDIM) program will support SPD authentication of a business or a person.

The Business BCeID will be used to authenticate a business that is applying for a waiver to produce other products that rely on this technology, or to register as a pill press owner or seller, and provide the business access to Paprika using the Business BCeID username and password. Note that the business accessing the portal will be required to be registered as a business in BC to apply.

The authentication standards for a person to which the project is held is the Canadian Police Information Centre (CPIC) standards which requires an individual provides two valid pieces of ID, one of which must be government-issued and include the applicant's name, date of birth, signature and photo. The ID must be physically verified by a "trusted agent" of the CPIC agency, the Security Program Division (SPD) of the Policing and Security Branch of the Ministry of Public Safety and Solicitor General. For BC residents with a BC Services Card, this is the gold standard for ID verification.

The BC Services Card will be only used as part of the application for the Registered Sellers' owner category. Using Paprika, businesses will be required to provide the names and contact information of the owners and managers of the business that intend to sell controlled equipment. Individuals who are owners or managers, and who are eligible BC residents, will be required to use their BC Services Card to authenticate their identity as part of the Registered Seller application process.

If these individuals are in BC but do not meet the BC residency requirements for the BC Services Card (i.e. new resident to BC or visiting), authentication will be achieved by the individuals requesting authentication from Service BC. That process will be assessed as part of another PIA. If these individuals are from another province and they are not currently in BC, authentication will be achieved by the individuals providing to SPD (by mail) a copy of two valid pieces of identification (one which will be government issued and which will include name, date of birth, signature and photo) authenticated by their local police agency. They will also request a Police Information Check from their local police agency and provide the unopened document to SPD with the completed and signed Consent for Security Screening Form, and the Identity Verification Attestation and Witness of Signature Forms.

In cases where the individuals involved are not eligible to receive a BC Services Card, do not reside in Canada, and are not currently in BC, authentication will be achieved, as per section 8 of the Royal Canadian Mountain Police (RCMP) Dissemination of Criminal Record Information Policy, by the individuals attending their local police department for verification of identity. SPD will require the individual to provide them with a copy of two pieces of valid international identification (one which will be a valid passport and a secondary piece of government-issued identification with a signature and imprinted name that matches that on the passport).

SPD will also require these individuals to provide a copy of a local criminal record check, authenticated and translated, if applicable, the Security Screening form, and signed copies of the Identity Verification Attestation and Witness of Signature Attestation Forms.

Security Screening

PPRECA will require those who want to sell controlled equipment (i.e. business applying for a Registered Seller registration) to register and agree to prescribed checks which will disclose the criminal charges and convictions, involvement with law enforcement, and involvement with correctional services of owners and managers of business applicants.

Only owners and managers of a business applying for the Registered Seller registration will be required to agree to the prescribed checks. The terms owner and manager are used in PPRECA and will be defined in policy. The individuals/roles who meet these definitions changes depending on the business legal structure. For example, in a corporation the "owner" will be directors and officers of the company, whereas in a partnership the owner will be each partner.

Note that the individual is not "consenting" to the disclosure of the information as prescribed by the Freedom of Information and Protection of Privacy Regulation but to fulfill a RCMP Canadian Police Information Centre (CPIC) requirement.

The background investigations and the specified checks will include criminal record checks, police information checks, checks of records in the Justice Information System of the Ministry of Attorney General and checks of records in the corrections information system of the Ministry of Public Safety and Solicitor General. In rare circumstances, fingerprint-based criminal record verification may also be included as part of the checks and would only be done by a law enforcement agency. Fingerprints would not be collected by SPD.

The security screening for a prospective Registered Seller applicant will mitigate risks including but not limited to the following:

- Adverse activity involving illegal drugs
- Associations with criminal elements, interests and activities

The collection of the personal information will be necessary for the Deputy Registrar to determine whether the individual is suitable to hold a Registered Seller certificate based on: charges and convictions; conduct, character and repute of the applicant; and, public interest. PPRECA will provide an opportunity for reconsideration of the Deputy Registrar's decision.

2. Scope of this PIA

The PIA will assess the privacy implications of the development and implementation of the Pill Press and Related Equipment Control Program, including the use of the Paprika, its portal, and the information exchange with IDIM.

Note that the alternative process for individuals authenticating through Service BC will be assessed in a separate PIA and that the information exchange with the RCMP was assessed in a previous PIA.

3. Related Privacy Impact Assessments

PSSG18013L	Pill Press Control Act LPIA
CTIZ12047	BC Services Card PIA
MTICS14007	BC Services Card Release 2 Implementation
CITZ17025	Exchange
CITZ18019	BC DevOps OpenShift Service
293-05/PIA 04-S005	FIGARO - Criminal Records Review Module

4. Elements of Information or Data

A. Authentication

As part of the authentication of a business, the IDIM will provide the following Business BCeID information to SPD:

- Business Legal Name
- Doing Business As (DBA) Name
- Business Number
- Business Type
- Name of User

As part of the authentication of a manager or an owner of a Registered Seller's applicant, IDIM will provide the following BC Services Card personal information to SPD:

- Primary Documented Surname
- Primary Documented Given Names
- Birth Date
- Sex

- Verified Email

Alternate Manual Process

The following documents and information will be provided by the owners and managers of a prospective Registered Seller to SPD by either mail or email:

- Consent for Security Screening Form
- Identity Verification Attestation Form and Witness of Signature Attestation Form
- Two pieces of government-issued picture IDs
- A Criminal Records Check or a Police Information Check

Note that the alternative process for individuals authenticating through Service BC will be assessed in a separate PIA.

B. Security Screening

The following personal information of owners and managers will be used to assess the security screening:

- Name of Individuals, including maiden names
- Alias
- Date and place of birth
- Gender
- Addresses over the past 5 years
- Driver Licence number or BCID
- Email address
- Phone number
- BC Registry number
- Relationship to applicant/business (i.e. title)

C. Application

Authorized Owner

In the case of Authorized Owners, the following information and relevant records may also be collected as part of the application:

1. Business Information

   - Business name
   - Business number
   - Business address and contact information

2. Authority to Own

   - Information to support legal authority to own, use, or possess controlled equipment under an enactment of BC or Canada to manufacture a drug or natural health product, such as:
     - Name shown on business' drug establishment licence or site licence
     - Drug establishment licence number and expiry date (issued by Health Canada)
     - Site licence number and expiry date (issued by Health Canada)
   - Whether the licence issued under an enactment to manufacture a drug or natural health product has been suspended, cancelled, or replaced

3. Use of Equipment

   - If the owner rents/leases the controlled equipment from someone else
   - Whether the controlled equipment is being used to manufacture business' own product or for someone else (i.e. contract manufacturing)

4. Purchasing Details

   - Business representative for the purposes of purchasing equipment
   - Purchaser's legal name, date of birth, civic address, contact information
   - If the controlled equipment was purchased from a Registered Seller, their legal name and registration number
   - If the controlled equipment was not acquired from a Registered Seller, the seller's legal name and civic address
   - Date on which the purchaser acquired the controlled equipment

5. Equipment (and changes to equipment)

   - Description of controlled equipment
     - Type of equipment
     - Make, model, serial number of equipment

- Civic address at which the controlled equipment will ordinarily be stored, and if it is moved:
  - The address where it is to be ordinarily stored
  - The date the equipment will be moved
- If the controlled equipment is lost, stolen, or destroyed:
  - The relevant equipment registration number
  - Description of equipment, including make, model, serial number
  - Date on which the equipment was lost, stolen, or destroyed
  - Police file number, if any

Waiver Holder

In the case of a Waiver applicant, the following information and relevant records may also be collected:

- Why business requires controlled equipment in manufacturing process
- How controlled equipment is utilized in manufacturing process
- The nature of the products being manufactured

Registered Seller

In the case of a Registered Seller applicant, the following information and relevant records may also be collected:

- Name, address, and business contact information for all owners and managers of the business.
- Whether the controlled equipment is being used to manufacture a product
- Whether the Registered Seller intends on renting or leasing controlled equipment to others (note: "selling" includes renting, leasing etc.)

D. Recording Sales Information

When a BC Registered Seller sells a piece of controlled equipment (either to a purchaser in BC or outside of BC), the Registered Seller will be required to report the sale to SPD within 10 days. SPD will collect the following information from the Registered Seller:

- Registered Seller Number
- Equipment type, make, model, serial number
- Equipment Registry Number for the piece sold

- Whether the purchaser is inside or outside of BC (to match with BC purchaser Equipment Notification)
- Name, address, contact of purchaser, ID of individual purchaser
- Verification of owner category if purchaser in BC (i.e. Waiver Number)
- Date the controlled equipment was sold
- Method of payment

E. Compliance and Enforcement

a. Sales Information:

i. Type of seller (i.e. manufacturer of controlled equipment, retailer etc.)
ii. Type of controlled equipment being sold (i.e. pill press, encapsulator, pharmaceutical mixer etc.)
iii. Prescribed records that must be kept by Registered Seller for each sale, including:
   - Completed sales form
   - Date on which the sale was made
   - If an individual, ID of the purchaser
   - Description of the controlled equipment that was sold (including type of equipment, make, model, serial number)
   - Registered Seller's registration number
   - Method of payment
   - Where purchaser will store equipment and whether a dwelling

b. Witness or complainant information
   - full name
   - address
   - home and work phone numbers
   - email address
   - details of alleged complaint/tip

c. Incidents or events (i.e. violations, seize equipment, legal actions)

d. Business information may be exchange with other agencies (i.e. Health Canada) such as contact information, site licence or drug establishment licence.

e. The following information may be exchange with Police Forces in BC :

- First Name
- Last Name
- Middle
- Maiden Names/Aliases
- Birth date
- Citizenship
- Primary Email address
- Current Address
- Business Address
- Home Phone Number
- Work Phone Number
- Cell Phone Number
- Driver's Licence # (as applicable)
- BC ID (as applicable)
- Whether the individual has ever been charged or convicted of a criminal offence
- Information resulting from criminal record check, police information check or correctional service check
- Photograph
- Government issued identity document number
- BCeID
- Site licence information
- Drug establishment licence information
- Seller registration information
- Waiver information
- Details of ownership of equipment to identify the legitimacy of the ownership

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information stored or located on Paprika and the Exchange Web Services (EWS) System will be located within the BC Government infrastructure located on Canadian data centres and will only be accessed within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	No
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	n/a
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	n/a

8. Personal Information Flow Table

Note that the confirmation process for Authorized Owners and the application process for Waiver applicants, the Notification of Equipment process, and the Reporting of Sales processes do not involve personal information and the flows of the information will not be presented here.

Personal Information Flow Table – Application for the Registered Seller			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Applicants (i.e. business representatives) will enter the Pill Press Online Registry portal from a government webpage sign-in button, where they will be redirected to the BCeID (Shared Services BC) website to authenticate using their Business BCeID (BCeID) and password. If the applicants do not have a BCeID, they will be directed to the BC Registry Services to register.	Out of Scope of FoIPPA and this PIA	n/a
2.	Once the applicant is returned to PAPRIKA, certain fields of information will be imported from BCeID and populate a client-facing Business Profile page. Shared data elements from BCeID include the following: • User GUID • Business Legal Name • Doing Business As • Business Number More detailed information about the security of the connections between the systems can be found on Security Threat Risk Assessment (STRA) for the Pill Press system. Note: There is no payment provision for this program.	No Personal Information	n/a
3.	The applicant will fill out business information, such as business type, physical address, mailing address, website, contact information, and name(s) of business representative(s).	No Personal Information	n/a
4.	The applicant will then be directed to the client Dashboard, where they will be directed to click on a specific link to apply as a Registered Seller registration.	No Personal Information	n/a

5.	The applicant will be then asked a series of questions as part of their application (see Q.4) and provide the full names, phone number, and business email address of all individuals who are either an "owner" or "manager" of the applicant business.	No Personal Information	n/a
6.	Once the applicant agrees to a declaration that the information provided in the application is complete, honest, and accurate, they will have the ability to submit the application and initiate the next phase. The application will be placed in the SPD Licensing Queue for processing.	No Personal Information	n/a
7.	The system will automatically generate and send a standardized email to all the owners/managers listed in the Registered Seller application. The email will advise the owner/manager that an application has been received for Registered Seller registration under PPRECA and provide a link which will direct them to the BC Services Card log in. As part of the authentication process, SPD will collect specific data elements from the BC Services Card about the individuals. Note that prior to login into the BC Services Card system, the individuals will be required to activate their cards. This is outside of the scope of this PIA.	Disclosure [IDIM] Collection [SPD]	33.1(5)(b) 26(c) and (h)(ii) 27(1)(b) [33.1(5)(b)]
8.	Once authenticated, the individuals (from step 7) will be redirected to Paprika to review and accept the terms of use and to fill in the required information (i.e. consent to the prescribed checks). Note that a collection notice will be provided as part of the terms of use and the individuals will be asked to authorize SPD to use their email address to communicate with them. The business representative who made the Registered Seller application will not have access to any correspondence or criminal record information of the owner(s)/manager(s).	Collection [SPD]	26(a) [ss. 7(2), (4), and 14(2) of the PPRECA] and (c)

9.	If the individual owner/manager is in BC but does not meet the BC residency requirements for the BC Services Card (i.e. new resident to BC. or residing outside of the province or country), authentication will be achieved by the individuals requesting authentication from Service BC.	Out of Scope of this PIA	n/a
10.	If the individuals are from another province and they are not currently in BC, authentication will be achieved by the individuals providing to SPD by mail a copy of two valid pieces of identification authenticated by their local police agency. The individuals will also need to request a Police Information Check from their local police agency and provide the unopened document to SPD with the signed Identity Verification Attestation Form, the completed and signed Consent for Security Screening Form, and the signed Witness of Signature Attestation Form.	Collection [SPD]	26(a) [ss. 7(2), (4), and 14(2) of the PPRECA] and (c)
11.	In cases where the individual owner/manager is not eligible to receive a BC Services Card, does not reside in Canada, and is not currently in BC, authentication will be achieved, as per section 8 of the RCMP Dissemination of Criminal Record Information Policy, by the individuals attending their local police department for verification of identity. SPD will require the individual to provide them with a copy of two pieces of valid international identification (one which will be a valid passport and a secondary piece of government-issued identification with a signature and imprinted name that matches that on the passport) and a signed Identity Verification Attestation Form. SPD will also require these individuals to provide a copy of a criminal record check, authenticated and translated, if applicable, the completed and signed Consent for Security Screening Form, and a signed Witness of Signature Attestation Form.	Collection [SPD]	26(a) [ss. 7(2), (4), and 14(2) of the PPRECA] and (c)
12.	SPD will review the Registered Seller applicant's submission for accuracy and completeness and may contact the applicant (or the relevant owner/manager) by email if it is necessary for clarification, correction, or if additional information is required.	No Personal Information	n/a

13.	SPD will gather information from other sources (i.e. CPIC, PRIMEBC, JUSTIN, CORNET, etc.) to perform the Security Screenings.	Disclosure Collection	33.2(a) 26(a) [ss. 12 and/or 14(2) of the PPRECA] and (c) 27(1)(a)(iii) [ss. 12 and/or 14(2) of the PPRECA]
14.	If an investigation has been requested by the Deputy Registrar, a SPD risk assessment investigator will contact relevant individuals to request additional information and prepare an investigative report for Deputy Registrar review.	Use Disclosure Collection	32(a) and (c) 33.2(a) 26(a) [s. 14(2) of the PPRECA] and (c)
15.	The Deputy Registrar will then decide whether security clearance will be granted after considering file information and the investigative report.	Use	32(a) and (c)
16.	If the clearance is not granted, or if there are other issues with the Registered Seller application, the Deputy Registrar will undertake a hearing process in accordance with administrative fairness and advised that the issue is specific to a denied security clearance without providing specific information.	Disclosure Collection Use Disclosure	33.2(a) 26(a) [s. 14(2) of the PPRECA] and (c) 32(a) 33.1(1)(c) [s. 9 of PPRECA] and 33.2(a)
17.	If any owner/manager is denied security clearance, then the Registered Seller application will be refused, and the applicant will be notified of the decision.	Disclosure	33.1(1)(c) [s. 9 of PPRECA]
18.	The Registered Seller applicant may apply for reconsideration.	Collection	26(a) [s. 14(2) of the PPRECA] and (c)

19.	**The reconsideration process may involve collecting additional information.**	Collection	26(a) [ss. 12 and/or 14(2) of the PPRECA] and (c) 27(1)(a)(iii) [ss. 12 and/or 14(2) of the PPRECA]
20.	Reconsideration decision will be provided to the applicant.	Disclosure	33.2(a) and 33.1(1)(c) [ss. 11(3)(c) of the PPRECA]
21.	If the application is denied, the applicant may apply for a judicial review of the decision.	Out of scope of FoIPPA	Not applicable
22.	If it has been deemed by SPD that the client's application meets criteria for approval, SPD will issue a Registered Seller registration and advise the applicant.	Disclosure	33.1(1)(c) [s. 8 of PPRECA] 33.2(a)
23.	Registered Seller will be required to report sales of controlled equipment (either to a purchaser in BC or outside of BC) to SPD and provide personal information of the individual who acquired the equipment.	Collection	26(a) [s. 14(2) of the PPRECA and s.4 of the PPREC Regulation] and (c) 27(1)(a)(iii) [s. 14(2) of the PPRECA and s.4 of the PPREC Regulation]

Note: 60-30 days before the Registered Seller registration is set to expire, the system will generate an automatic email to the business client reminding them to apply for renewal of their Registered Seller owner category. The Registered Seller renewal application will be the same process as the original Registered Seller application process.

Personal Information Flow Table – Compliance & Enforcement – Complaints and Investigations			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Tips about potential illegal use of controlled equipment will be received by SPD. Tips may come from a number of sources (i.e. public, law enforcement agencies, etc.). The information will be used to make a decision to investigate.	Collection Use	26(a) [s. 14(2) of PPRECA], (b) and (c) 27(1)(a)(iii) [s. 14(2) of PPRECA] and (c)(iv) 32(a)
2.	If the decision is made to investigate, the investigator will connect with other sources to exchange information relevant to the investigation and create a report for the Deputy Registrar.	Disclosure Collection Use	33.1(1)(d) [s. 15 of PPRECA] 33.2(a) and (i) 26(a) [s. 18 of the PRRECA] and (b) and (c) 27(1)(a)(iii) [s. 18 of PPRECA] and (c)(iv) 32(a) and (c)
3.	Deputy Registrar will review the report and make a decision in terms of next steps (i.e. seize equipment, review a registration).	Use	32(a) and (c)
4.	In some circumstances, the decision may have an impact on a business (i.e. seize equipment, education, violations) and the Deputy Registrar would notify the business of the consequences and the related process.	No Personal Information	n/a
5.	If a violation ticket is issued, the business will have the ability to dispute the ticket in court.	Out of scope of FoIPPA.	n/a

Personal Information Flow Table – Compliance & Enforcement – Inspections			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	The Deputy Registrar may order an inspection of an owner of controlled equipment, or the system may initiate a standard inspection based on a predetermined schedule.	No personal Information	n/a
2.	Inspectors may access and collect personal information as part of the inspections (i.e. ID of purchasers of controlled equipment) to assess compliance and create an inspection report.	Collection Use	26(a) [ss. 14(2) and 18 of PPRECA] and (c) 27(1)(a)(iii) [ss. 14(2) and 18 of PPRECA] and (c)(iv) 32(a)
3.	If the business is not compliant with PPRECA, based on the compliance history, cooperation of the business, and the severity of the violation, the inspector may direct progressive enforcement actions.	No Personal Information	n/a

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes	Oath of Employment Privacy Training Standards of Conducts Criminal Records Checks Enhanced Security Screenings	Low	High
2.	The security check is being done on the wrong person.	Authentication using BC Services Card and supporting document identifying the owner(s) and manager(s) of the business applicant.	Low	High

3.	The personal information is compromised when transferred between PSSG and the Police Forces in BC.	s.15		

10. Collection Notice

The following collection notice will be provided to all individuals when they log into the portal, as part of the security checks, and when authenticating by an alternative measure on the associated form:

The Security Programs Division will collect your personal information for the purpose of fulfilling the requirements of the Pill Press and Related Equipment Control Act (PPRECA) and associated regulations in Pill Press registration, compliance and enforcement matters in accordance with Sections 26 (a) and (c) of the Freedom of Information and Protection of Privacy Act. Should you have any questions about the collection, use, or disclosure of personal information, please contact the Senior Policy Analyst, Security Programs Division via mail to PO Box 9217 Stn Prov Govt Victoria, BC V8W 9J1; email to securitylicensing@gov.bc.ca; or by telephone at 1-855-587-0185.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

s.15

s.15

12. Please describe the technical security measures related to the initiative (if applicable).

s.15

s.15

13. Does your branch rely on security policies other than the Information Security Policy?

No.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

s.15

15. Please describe how you track who has access to the personal information.

s.15

In terms of the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.

- Message Transport logs include message tracking (Exchange server to Exchange server internal only) which provides a detailed record of message activity, such as sent, received date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.

- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

An individual may request that they personal information be corrected or updated in PAPRIKA. If the information is not corrected, an annotation will be made to the file and if the information has been provided to another party in the last 12 months, SPD will advise the party of the request.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

The information will be used to assess whether a client will have the ability to own or sell the controlled equipment.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

The identity of all owners and managers for the Registered Seller application will be authenticated either using the BC Services Card or the alternative measures.

Additionally, SPD staff will contact the applicants to determine whether the information is correct. They will also review any official documents that have been provided to them, including corporate records, to confirm validity of the collected information.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

SPD is currently working with the Corporate Information and Records Management Office to develop an approved records retention and disposition schedule for the personal information collected. In the interim, the personal information collected will be retained for at least two years after it was used to make the decision.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

There will be an information sharing agreement with the Police Forces in BC as information will be shared between parties.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.	X

Information Sharing Agreement – Required Information	
Description	Information sharing between the Ministry of Public Safety and Solicitor General, Policing and Security Branch and Police Forces in BC in the context of the Pill Press and Related Equipment Control program.
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General, Policing and Security Branch
All other ministries/government agencies and public bodies involved	Police Forces in BC
Business contact title	Senior Policy Analyst, Security Programs Division
Business contact telephone number	1-855-587-0185
Indication of whether or not personal information is involved	Yes
Start date	Winter 2019
End date (if applicable)	n/a

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

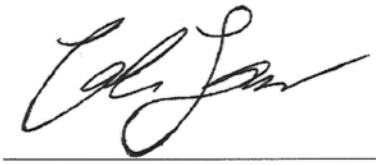
22. Will a personal information bank (PIB) result from this initiative?

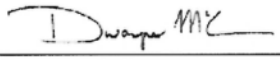
Yes. The new case management system, Paprika will be a new PIB.

Personal Information Bank – Required Information	
Description	Pill Press and related control equipment case files.
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General, Policing and Security Branch, Security Program Division
All other ministries/government agencies and public bodies involved	None
Business contact title	Senior Policy Analyst, Security Programs Division
Business contact telephone number	1-855-587-0185

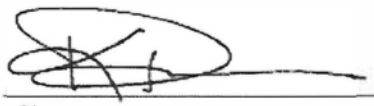
Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Cole Lance		January 14, 2019
Privacy Advisor Privacy, Compliance and Training Branch Corporate Information and Records Management Officer Ministry of Citizens` Services	Signature	Date

Dwayne McCowan		January 14, 2019
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens` Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	 Signature	January 14, 2019 Date
Ian Bailey Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	 Signature	January 14, 2019 Date
Heather Stewart Director, Security Services, Security Programs Division Policing and Security Branch Ministry of Public Safety and Solicitor General	H Stewart Signature	Jan. 14, 2019 Date
Clayton Pecknold Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	 Signature	January 18, 2019 Date

Privacy Impact Assessment for

BC Witness Security Program

PIA# PSSG19015

Part 1 – General

Name of Ministry:	Ministry of Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter:	s.15; s.19		
Email:	s.15; s.19	Phone:	s.15; s.19
Program Manager:	Tom Steenvoorden, Director - Public Safety Initiatives		
Email:	Tom.Steenvoorden@gov.bc.ca	Phone:	s.15; s.19

1. Description of the Initiative

The purpose of the project is to develop and implement a provincial *Witness Security Act* (BC WSA) and corresponding Witness Security program (WSP) to enhance management and protection services to witnesses and associated persons at risk of threats or violence.

s.16

Initial policy work has identified the opportunity to create a WSP which will result in a unique and comprehensive program tailored to support current efforts to combat organized crime, gangs, gun violence, and achieve provincial crime reduction goals. Building and maintaining a flexible and reputable program is critical to combat organized crime, as recruiting and retaining cooperating witnesses who can testify in court to secure convictions is critical for the prosecution to be successful and maintain public safety and confidence in the administration of justice. s.16

s.16

s.16 The management of witnesses for these often-lengthy prosecutions is time consuming, requires significant effort and resourcing, and is fraught with risks to the witnesses and the successful prosecution of a case.

A provincial witness security statute and program will provide a consistent approach to complex witness recruitment and management. This will result in reduced wait times for confirmation of witness admittance into the program, leading to a timelier charge approval, and ideally result in the successful prosecution of organized crime due to the willing participation of well-managed and safe witnesses.

The formal participation of a witness in the program is done through a Statement of Obligations and a Service Plan, whereby the witness signs a contract agreeing to the terms set out and is notified that a breach in the agreement may result in termination from the program. Where the Director finds appropriate, they may refer any witness application to a volunteer Assessment Committee and Panel for determination. The Committee and Panel will be made up of experienced members from law enforcement and other relevant areas, and members will be appointed by Ministerial Order.

The purpose of the project is to develop and implement a legislative framework for a WSP to enhance protection services to witnesses and cooperating co-accused, those sharing information with police, and associated persons-at-risk. It is anticipated that the Designated Agency of the WSP will be appointed by the Minister for the purpose of providing protective services and witness management.

In alignment with the Minister's mandate commitments to take action on gang and gun violence and increase support for initiatives that are proven to prevent and reduce crime, this project will enhance management and security services to witnesses and cooperating co-accused. Protection for those that share information with police results in stronger cases and prosecutions, and an increased likelihood of conviction.

2. Scope of this PIA

The PIA will assess the privacy implications of the new BC WSP.

3. Related Privacy Impact Assessments

PSSG18001L – Witness Security Act

4. Elements of Information or Data

The following information may be provided to WSP as part of a referral from a Law Enforcement Agency (the Sponsor):

s.13

- s.13
- Physical Information (s.13
  s.13
- s.13 religious
- s.13
- s.13
- s.13
- s.13
- s.13
- s.13 financial, criminal s.13
  s.13
- s.13
- Description of their risk situation s.13
- s.13 mental health s.13
- Personal information of relevant associated person's s.13
  s.13
- s.13
-

Note that this list is not comprehensive.

The above information may also be collected directly from the individuals if the Sponsor does not have this information available at the time of the referral.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The personal information will be stored in Canada on BC Government's infrastructure on Canadian data centers and the information will only be accessible within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	An individual informs a law enforcement agency (the Sponsor) that they would like to apply to the program.	Out of scope of the PIA	n/a
2.	The Sponsor contacts the Designated Agency and advises of the individual's interest. The Sponsor secures the applicant and assists them with application.	Out of scope of the PIA	n/a
3.	The Director receives the application from the Sponsor on behalf of the applicant for the purpose of determining if the individual satisfies the eligibility threshold.	Collection	26(a), (b), and (c) 27(1)(a)(iii) [section 34(1) of the BC WSA]
4.	The Director may collect from a person or a witness any information or records that the Director, Committee, or Panel considers necessary for the purpose of exercising a power or performing a duty of the Director, Committee, or Panel.	Collection	26(a), (b), and (c) 27(1)(a)(iii) [section 34(1) of the BC WSA]
5.	If the Director finds that the witness meets the eligibility threshold, they will refer the application to the chair of the Committee.	Use Disclosure	32(a) and (c) 33.1(1)(c) [sections 18(1)(b) and 18(2) of the BC WSA] and 33.2(a)
6.	If the Director finds that the witness does not meet the eligibility threshold, they will reject the application and advise the Sponsor of the decision.	Use Disclosure	32(a) and (c) 33.1(1)(c) [section 18(1)(a) of the BC WSA] and 33.2(a)

7.	The chair of the Committee receives the application and assembles the Panel for the assessment of the application.	Collection Disclosure	26(c) 27(1)(b) 33.2(a)
8.	If eligibility is confirmed as part of the assessment, the Panel will draft a Service Plan and cost estimate. If the Panel requires additional information to draft the plan, they may request that the Director provides them with additional information.	Use Disclosure Collection	32(a) and (c) 33.1(1)(c) and 33.2(a) 26(a) and (c) 27(1)(a)(i) and iii) [sections 19(1)(c)(ii), 34(1) and 34(2) of the BC WSA]
9.	Once the Plan is drafted, the Director will provide the Plan to the Designated Agency, and a high-level summary the Sponsor.	Disclosure	33.1(1)(c) [sections 20(b) and 21(1)(b) of BC WSA] and 33.2(a)
10.	The Designated Agency may disclose personal information to another agency in the context of implementing the Service Plan or to support the witness transition out of the program.	Disclosure	33.1(1)(c) [sections 39(1)(b), (2)(g), 47(1) and (2) of the BC WSA] 33.2(a)
11.	The Director may collect information from those same agencies to assist in the management of the protective services and witness management.	Collection	26(a) and (c) 27(1)(a)(iii) [section 34(1) of the BC WSA]

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes.	• Oath of Employment • Privacy Training • Standards of Conduct • Criminal Background check • Enhanced Security Screening Offence under the *Witness Security Act* to inappropriately share personal information of witness.	Low	High
2.	s.13	• s.13	Low	High
3.	s.13	s.13	Low	High

10. Collection Notice

A Collection Notice is not required as per section 27(3)(c) of the *Freedom of Information and Protection of Privacy Act* (FoIPPA) as the personal information will not be collected directly from the individual and the indirect collection is authorized as per section 27(1)(a)(i) and (iii) of FoIPPA.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

s.13

s.15

s.13

12. Please describe the technical security measures related to the initiative (if applicable).

s.13

13. Does your branch rely on security policies other than the Information Security Policy?

s.13

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

s.15

s.13

15. Please describe how you track who has access to the personal information.

s.15

s.13

In terms of the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.
- Message Transport logs include message tracking (Exchange server to Exchange server - internal only) which provides a detailed record of message activity, such as sent, received, date/time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.
- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?**

    If a participant identifies that their information needs to be revised or corrected, the Director will make an annotation or correction to the participant's file.

    If participants request a correction to their personal information and the information has already been shared with another party or stakeholders within the last year, the Director will notify the receiving organization.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

    Yes, personal information will be used to determine if the individual or family members are eligible to participate in the program, and if so, the level of protective services they require.

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

    Personal information received by the Director as part of the initial application will be coming from Sponsor who has interviewed the witness directly.

    Personal information received by the Director as part of the information gathering process for eligibility and/or the determination of the level of protection required will be confirmed with witness as part of the application process.

19. **If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

    PSB has connected with the Corporate Information and Records Management Office who have advised that there is currently no suitable retention and disposition schedule available for the WSP. As such, the WSP is currently on the list for future schedule development but has not been advised of a timeline for commencement or completion.

Until a schedule has been developed and implemented, all documentation will be kept as long as the individual/family is enrolled in the program and any ongoing legal proceedings are underway or retained for at least one year after it was used to make the decision, whichever is the longest.

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No, the initiative will not involve systematic disclosures of personal information as the information will be shared on a case-by-case basis.

Part 5 – Further Information

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative?

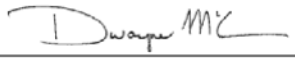
Yes, a new PIB will be developed in the LAN.

Personal Information Bank – Required Information	
Description	Personal information collected as part of the BC Witness Security Program.
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General, Policing and Security Branch
All other ministries/government agencies and public bodies involved	none
Business contact title	Director, Witness Security Program
Business contact telephone number	250-387-1751

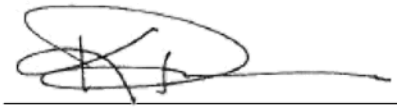
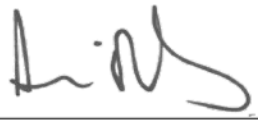
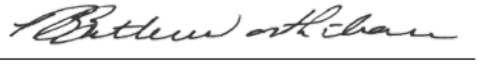
Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Tim Perry		May 22, 2019
Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Officer Ministry of Citizens` Services	Signature	Date

Dwayne McCowan		May 30, 2019
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens` Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua		May 31, 2019
Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Ian Bailey		June 4, 2019
Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Tom Steenvoorden		June 4, 2019
Executive Director Public Safety & Policing Support Units Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date
Brenda Butterworth-Carr		2019-06-11
Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date

Privacy Impact Assessment for Community Safety Unit Video Surveillance

PIA# PSSG19048

Part 1 – General

Name of Ministry:	Ministry of Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter:	Deputy Director, Community Safety Unit		
Email:	Katelyn.mackellen@gov.bc.ca	Phone:	250-387-1751
Program Manager:	Jamie Lipp, Executive Director, Community Safety Unit		
Email:	Jamie.lipp@gov.bc.ca	Phone:	250-387-1751

1. Description of the Initiative

The Community Safety Unit (CSU), under the Policing and Security Branch of the Ministry of Public Safety and Solicitor General, is responsible for compliance and enforcement under the *Cannabis Control and Licensing Act* (CCLA), in regard to those who do not hold a retail licence under the Act. Community Safety Unit officers focus on carrying out compliance and enforcement activities against unlicensed non-medical cannabis retailers and suppliers.

The Community Safety Unit (CSU) can undertake a range of enforcement activities, including conducting inspections, issuing violation tickets, obtaining warrants and issuing demands for information, summoning witnesses, conducting hearings, seizing cannabis, and issuing administrative monetary penalties.

s.15

Page 099 of 195

Withheld pursuant to/removed as

s.15

s.15

2. Scope of this PIA

This PIA will assess the privacy implications of the surveillance system installed at CSU's secure storage containers. A separate PIA has been done on the implementation of the CSU.

3. Related Privacy Impact Assessments

PSSG18057 – Community Safety Unit

4. Elements of Information or Data

s.15

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information will be stored locally on the DVMS, CSU Drive LAN, the BC Government secure File Transfer Service (sFTS), or the Exchange Web Services (EWS) system, and the information will only be accessible within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	Yes

3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	s.15	Collection	26(c)
2.	s.15	Disclosure Collection Use	33.2(a) and (c)_ 26(c) 27(1)(b) 32(a)
3.	s.15	Disclosure Collection Use	33.2(a) and (c) 26(c) 27(1)(b) 32(a)
4.	Archived video recordings or screenshots may be disclosed to CSU management for incident response reviews.	Disclosure Collection Use	33.2(a) and (c) 26(c) 27(1)(b) 32(a)
5.	Archived video recordings or screenshots may be disclosed to PSSG legal counsel to gather legal advice.	Disclosure	33.1(1)(g)

6.	Archived video recordings or screenshots may be disclosed to the British Columbia Prosecution Service (BCPS) for use in legal proceedings.	Out of Scope of FoIPPA	3(1)(h)
7.	Archived video recordings or screenshots may be disclosed to law enforcement agencies to support an active police investigation into an incident. Note that unless the incident being investigated occurred within the storage container, all law enforcement agencies will be required to provide a court order to access the video recordings or screen shots.	Disclosure	33.1(1)(t) or 33.2(i)
8.	Archived video recordings or screenshots may be disclosed to WorkSafeBC if they are investigating a workplace incident s.15 s.15	Disclosure	33.1(1)(c) [s. 175 of the *Workers Compensation Act*] and 33.2(i)
9.	Archived video recordings may be disclosed to the Public Service Agency as part of a labour relation investigation.	Disclosure	33.2(a) and (i)
10.	Video storage array archivers and DVMS work stations are maintained by the Status Systems Division of Status Electrical Corporation ("Status Systems"). Note that there is no need for archived or retained video to be viewed as part of the maintenance process.	No Disclosure	N/A
11.	Archived video recordings or screenshots may be disclosed to LCRB if an incident occurs that involves their staff or exhibits.	Disclosure	33.2(a) and (i)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and could use or disclose it for personal purposes.	Oath of Employment Privacy Training Enhanced Criminal Records Check Standards of Conduct	Low	High
2.	Personal information captured by the video recording is compromised when transferred within BC Government.	Personal information will be transferred in person, by phone, by email or for large files (i.e. video and audio recordings), through secure File Transfer Services (sFTS). Both LSB and CSU are using the BC Government Exchange Web Services (EWS) system and the information will be encrypted at rest and in transfer.	Low	High
3.	Personal information captured by the video recording is compromised when transferred to law enforcement agencies.	The personal information would be transferred through sFTS.	Low	High
4.	Personal information captured by the video recording is compromised when transferred to BCPS.	Personal information will be transferred by email or for large files (i.e. video and audio recordings), through sFTS. Both BCPS and CSU are using the EWS system and the information will be encrypted at rest and in transfer.	Low	High

10. Collection Notice

A Collection Notice is not required as per section 27(3)(a) and (c) of the *Freedom of Information and Protection of Privacy Act* (FoIPPA) as the personal information, which will be collected directly from the individual, will be collected in the context of law enforcement.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

s.15

12. Please describe the technical security measures related to the initiative (if applicable).

The Avigilon software that will run the DVMS is a desktop application which is loaded onto a windows PC.

The application will only be accessible to authorized staff of CSU and Status Systems. Each authorized user is issued a password by the site system administrator/s and each user's privilege levels for the system are based on their job functions.s.15

s.15

Personal information will be transferred to BCPS and LCRB by email using the EWS system or sFTS for large video file.

Personal information will be transferred to BC law enforcement agencies using sFTS or by providing a USB Flash Drive encrypted with a password. The encryption meets the Government's Cryptographic Standards for Information Protection. A policy will identify that a unique complex password will be required for each file.

The password will be sent to the third party by email or provided by telephone independently from the files and the disk.

The access to the EWS system, sFTS, and the CSU LAN Drive are only accessible through a valid BC Government user ID and password.

BC Government firewalls as well as additional intrusion prevention mechanisms will be used to protect the personal information that will be stored on the LAN Drive, sFTS, and EWS system as the information will be located within the secure BC Government infrastructure.

13. Does your branch rely on security policies other than the Information Security Policy?

- Policies prohibiting the sharing of passwords and user ID's
- Policies prohibiting users from posting passwords
- Policies requiring screens to be locked when not in use
- Security incidents must be reported immediately

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

s.15

Page 107 of 195

Withheld pursuant to/removed as

s.15

s.15

In terms of the sFTS, access and attempted access are logged.

As for the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.
- Message Transport logs include message tracking (Exchange server to Exchange server - internal only) which provides a detailed record of message activity, such as sent, received, date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.
- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

The Avigilon recording format is a proprietary format that uses a security seal that prevents images from being tampered, manipulated or edited in any way.

No personal information in the form of live or archived video can be updated or corrected but time stamps could potentially be updated if an error was made.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Yes, video s.15 are archived and/or exported for use in disciplinary procedures, criminal investigations, and labor relations investigations.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Access to the video clips is limited to mitigate the possibility of the video clips being altered. Additionally, CSU staff will their investigative skills to confirm the identity of the individuals shown on the clips.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

CSU is currently working with the Corporate Information and Records Management Office to develop an approved records retention and disposition schedule for the program. In the interim, the personal information collected and used in making a decision directly affecting an individual will be retained for at least one year after it was used to make the decision.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No. The personal information will only be disclosed to on a case by case basis when an incident that took place s.15 is being investigated.

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

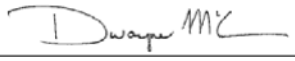
22. Will a personal information bank (PIB) result from this initiative?

No, a PIB will not be developed as part of this initiative. The archived video clips will not be saved under a person's name or any other identifiable number.

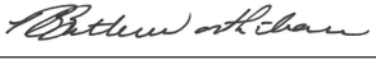
Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Tim Perry		2019-12-09
Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Officer Ministry of Citizens` Services	Signature	Date

Dwayne McCowan		December 11, 2019
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens` Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua		December 11, 2019
Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Ian Bailey		December 12, 2019
Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Jamie Lipp		December 16, 2019
Executive Director of the Community Safety Unit Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date
Brenda Butterworth-Carr		December 20, 2019
Tr'injà shär njit dintlät Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date

Page 112 of 195 to/à Page 124 of 195

Withheld pursuant to/removed as

s.12

Page 125 of 195

Withheld pursuant to/removed as

s.15; s.12

Page 126 of 195 to/à Page 133 of 195

Withheld pursuant to/removed as

s.12

Privacy Impact Assessment for

Building and Enhancing Law Enforcement Capacity in BC to Address Drug-Impaired Driving in Canada Project
PIA# PSSG19052

Part 1 - General

Name of Ministry:	Ministry of Public Safety Solicitor General, Policing and Security Branch		
PIA Drafter:	Shannon Oberholtzer, A/Senior Program Analyst		
Email:	Shannon.oberholtzer@gov.bc.ca	Phone:	778-698-2810
Program Manager:	Wendy Sutherland, A/Senior Program Manager		
Email:	Wendy.sutherland@gov.bc.ca	Phone:	778-572-3413

1. Description of the Initiative

Public Safety Canada (PSC) will allocate $81 million of federal funding to provinces and territories over five fiscal years, starting 2018-2019, for a project entitled: Building and Enhancing Law Enforcement Capacity in British Columbia to Address Drug-Impaired Driving in Canada (the Project).

The purpose of this Project is to build and enhance law enforcement capacity in British Columbia to address drug-impaired driving. The Project has two elements:

1. To provide federal funding to support law enforcement training and access to particular resources.

2. To assess and evaluate law enforcement efforts by collecting data.

The funds will be used to support the following training and access to equipment:

1. Police training in Standardized Field Sobriety Testing (SFST),
2. Drug Recognition Expert training (DRE),
3. Access to Approved Drug Screening Equipment (ADSE), and
4. Build capacity to enforce new laws related to drug-impaired driving.

British Columbia entered into a Contribution Agreement with Canada in respect of the Project ("the Agreement"). Under the terms of the Agreement, the Policing and Security Branch (PSB) of the Ministry of Public Safety and Solicitor General (PSSG) will grant funds for related training to JIBC, VPD, and RCMP and will provide aggregate information to PSC that will include a comprehensive trend analysis that will be utilized to examine the implications of the legalization of cannabis and the new drug-impaired driving legislative regime on road safety at a provincial and federal level. It will also be utilized to examine the effectiveness of the ADSE(s) as an enforcement tool to detect drug-impaired driving.

2. Scope of this PIA

s.15; s.16

3. Related Privacy Impact Assessments

There are no related PIAs.

4. Elements of Information or Data

A. <u>The following aggregate data elements will be provided to PSC by PSB:</u>

Training and certification: the number of officers trained per year (in Drugs that Impair; SFST; DRE), the number of officers newly certified per year (as DREs); the total number of certified DRE officers in a given year; and the method of training in respect of each of the above (in class; computer)

Incidents: the number of vehicles stopped, and signs of impairment detected; the type of intervention (SFST; ADSE; DRE; blood sample); the number and type of charges laid (operation while impaired: drugs only, drugs and alcohol, alcohol only; causing bodily harm, death, damage)and characteristics of accused (age, gender); toxicological analysis results (type of substance).

Detection and investigation: the number of vehicles stopped, and signs of impairment detected; the type of intervention (SFST; ADSE; DRE; blood sample); the number and type of charges laid (operation while impaired: drugs only, drugs and alcohol, alcohol only; causing bodily harm, death, damage) and characteristics of accused (age, gender); toxicological analysis results (type of substance).

Prosecution and court outcome: cases resulting in conviction (guilty plea or verdict); the type of sentence imposed (fine, community, prison) by type of incident; offender characteristics (age, gender).

General preventative interventions: descriptions of media campaigns, targeted information and educational campaigns.

<u>B.</u>

Information collected by PSB:

1. Training and Certification.

PSB will collect the training and certification information from the following training institutions:

- RCMP Pacific Region Training Center (PRTC),
- RCMP Provincial DRE Program,
- Justice Institute of British Columbia (JIBC), and
- Vancouver Police Department (VPD).

The information collected will include:

- Names and detachment/department of officers who attended training
- Number of officers trained in each course
- Number of courses offered
- Associated costs and invoices

The personal information collected by PSB in respect of the officers who attend the training will be used by PSB for billing/invoice reconciliation purposes and will not be shared with PSC.

2. Incidents:

PSB will collect the details of police-attended motor vehicle incidents information from RoadSafetyBC and the Insurance Corporation of British Columbia (ICBC) including:

- Number and type of incidents involving drugs and/or alcohol;
- Whether there are associated injuries or death with the motor vehicle incident;
- Gender and age of the driver;
- Date and time of the motor vehicle incident; and
- If the driver has a previous drug or alcohol related motor vehicle incident.

No personal information will be collected.

3. Detection and Investigation:

PSB will collect the following from the police-run Drinking and Driving CounterAttack program (CounterAttack):

- Number of impaired driving investigations;
- Number of times SFST was used;
- Number of times DRE was used;
- Signs of impairment detected; and
- Number and type of sanctions issued.

PSB will collect the following data from the RCMP Forensic Labs:

- Number of blood samples from BC per month; and
- Toxicological analysis results.

PSB will collect the following data from the police-run Integrated Road Safety Unit:

- agency or detachment name;
- date of the stop;
- the circumstances that lead to the stop (traffic stop, collision, checkpoint or other);
- time of the use of the device;
- outcome of the test (positive for THC, positive for cocaine, positive for both, negative);
- if a DRE evaluation was requested;
- the results of the DRE evaluation, including if the evaluation confirms results of device; and
- time of the DRE evaluation; and if a blood or urine sample was demanded, the result of blood or urine sample (including consistency with the results of the device).

No personal information will be collected.

4. Prosecutions and Court Outcomes:

PSB will collect the following information from the Court Services Branch (CSB) of the Ministry of Attorney General through JUSTIN, CSB's integrated case management system:

- Number of offences charged under new federal legislation, C-46;
- Dispositions of these cases (guilty plea, verdict, type of sentencing); and
- Offender characteristics (age, gender etc.).

The collected personal information will be outside of the scope of the *Freedom of Information and Protection of Privacy Act* (FoIPPA) as per section 3(1)(a) of FoIPPA.

5. General Preventative Interventions

PSB will collect the following information from Government Communications and Public Engagement (GCPE):

- Dates of public education campaigns;
- Who sponsored the campaign (i.e. federal or provincial government); and
- What the education campaign referred to (drug impaired driving, cannabis generally etc.).

No personal information will be collected by PSB, only general descriptions of campaigns run.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The personal information collected by PSB, will be located and stored in Canada on BC Government infrastructure on Canadian servers located in BC and in Alberta.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	No

2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	N/A
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	No
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	PSB will collect the training and certification information from the RCMP, VPD, and JIBC training institutions for billing purposes (i.e. to reconcile the accounts and invoices) and to evaluate whether the police forces are meeting PSB's quality and standard of policing.	Collection Use	26(a) [s.40(1)(a) of the *Police Act*], (c) and (e) 27(1)(a)(iii) and (c)(iii) 32(a) and (c)

2.	PSB collects incident information from RoadSafetyBC and ICBC for the purpose of evaluating police services.	No Personal Information	n/a
3.	BC collects aggregate information from CounterAttack, the RCMP Forensic Labs, and IRSU to assess the quality of the law enforcement service.	No Personal Information	n/a
4.	PSB collects prosecution and court outcome information from CSB.	Out of scope of FoIPPA	n/a
5.	PSB collects information from GCPE about public education campaigns about drug impaired driving and cannabis generally.	No Personal Information	n/a
6.	The collected information will be analyzed to inform trends and patterns and the analysis will be sent to PSC on a quarterly basis. There will be no individual data in these reports, only trends, averages, etc.	Use	32(a) and (c)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes	• Oath of Employment • Privacy Training • Standards of Conduct • Criminal Background check • Enhanced Security Screening	Low	High
2.	Personal information is compromised when transferred to PSC.	No personal information will be shared with PSC, only aggregate data.	Low	High

10. Collection Notice

A Collection Notice is not required as per section 27(3)(c) of the *Freedom of Information and Protection of Privacy Act* (FoIPPA) as the personal information will not be collected directly from the individual and the indirect collection is authorized as per sections 27(1)(a)(iii) and (c)(iii) of FoIPPA.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

The collected information will be stored on secure folders on the PSB LAN. Police Agencies may provide personal information by email and the information may be stored temporarily in the BC Government Exchange Web Services (EWS) system.

s.15

12. Please describe the technical security measures related to the initiative (if applicable).

s.15

13. Does your branch rely on security policies other than the Information Security Policy?

No.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

The Police Services Division LAN and emails will only be accessible through a valid BC Government user ID and password and the access will be based on roles and responsibilities.

15. Please describe how you track who has access to the personal information.

In terms of the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for seven days.
- Message Transport logs include message tracking (Exchange server to Exchange server internal only) which provides a detailed record of message activity, such as sent, received date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.

Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires

LAN has complete, real-time audit logs of all system activities. The logging capabilities are being integrated into the Hosting Services Log Aggregation service (ArcSight logger) and will be monitored for irregularities. Log analysis is under the control of the Ministry of Citizen's Services and is outside the scope of this PIA.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

If an individual were to contact PSB to have their information updated or corrected, PSB would redirect the individual to the appropriate agency.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No, the information will only be used to show trends, averages etc. The data will not be used to make decisions that will directly affect an individual.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

There will be no systematic sharing of personal information between PSB and the police agencies. The exchange will only occur on a few occasions.

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

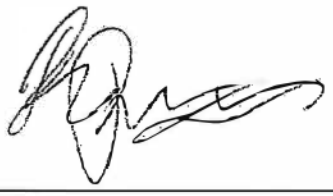
No.

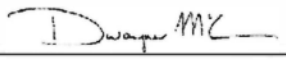
22. Will a personal information bank (PIB) result from this initiative?

No as the information will not be searchable by name.

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Tim Perry		2020-01-08
Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Dwayne McCowan		January 9, 2020
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	January 09, 2020 Date
Ian Bailey Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	January 09, 2020 Date
Wendy Sutherland Senior Program Manager Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	January 9, 2020 Date
Sandra Sajko Executive Director, Police Services Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	January 13, 2020 Date
Brenda Butterworth-Carr Tr'injà shär njit dintlät Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	January 17, 2020 Date

Privacy Impact Assessment for

Provincial Review of Police Detention Facilities, and Evaluation of Compliance with BC Policing Standards regarding Use-of-Force Training

PIA# PSSG20007

Part 1 – General

Name of Ministry:	Ministry of Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter:	Benjamin Woolsey, Research Officer		
Email:	benjamin.woolsey@gov.bc.ca	Phone:	778-572-3389
Program Manager:	Mike Massine, Senior Program Manager		
Email:	Mike.Massine@gov.bc.ca	Phone:	778-572-3407

1. Description of the Initiative

The Policing and Security Branch of the Ministry of Public Safety and Solicitor is conducting a Provincial Review including both evaluating compliance with various use-of-force related British Columbia Provincial Policing Standards and gathering information about police detention facilities and related policies, procedures and practices to inform the development of new standards.

The Director's authority for the Review is set out in Part 8 of the *Police Act*. The Review will involve site visits to all municipal police departments in BC, a sample of approximately 14 RCMP detachments with detention facilities throughout BC, and the RCMP's Pacific Region Training Centre (PRTC) in Chilliwack. All site visits will include open-ended interviews with staff associated with the detention facility as well as reviewing training records related to use-of-force training. Any notes taken to substantiate the resulting compliance rate will not include any identifying information. The review will be focused on policies, roles and responsibilities, training, equipment, supervision and accountability structures, challenges, recommendations for provincial standards, and the like.

The review will include the examination of personnel lists (including officer ID numbers and/or names, hire date and type of assignment) and training records as required to evaluate compliance with the use-of-force training requirements in the BCPPS (i.e., to ensure officers have completed the training required for their length of service and type of role held).

2. Scope of this PIA

The privacy impact assessment will assess the privacy implications of PSB doing this Provincial review.

3. Related Privacy Impact Assessments

There is no related PIA.

4. Elements of Information or Data

PSB will collect the following information about Police Officers in BC:

- Name
- Business contact information
- ID numbers
- Hire date
- Type of assignment
- Use-of-force training
- Availability (to set up interview)
- Professional Opinion

PSB will also collect a police agency's rate of compliance for various types of training standards.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The personal information collected as part of this review will be stored on a restricted-and secure PSB LAN Drive on BC Government infrastructure located on Canadian data centres and the information will not be accessible from outside Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	N/a
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	N/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	No
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	N/a
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	N/a

8. Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Police detachments will provide PSB will a list of detention-related staff within each police agency that PSB can interview to gather their professional opinions on police detention facilities. The information will be used to contact the individuals to set up the interviews.	No Personal Information	n/a
2.	The detention-related staff will identify to PSB when they are available to meet for the interview.	Collection Use	26(c) 32(a)
3.	PSB will review police agencies training information to assess compliance with use-of-force BCPPS training requirements and assess current standards requirements and to need to modify them.	Collection Use	26(a) [section 40(1)(a.2) and (3) of the *Police Act*], (c) and (e) 27(1)(a)(iii) 32(a) and (c)
3.	The findings of the evaluation will be reporting in a report to executives.	No Personal Information	n/a

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes	Oath of Employment Privacy Training Standards of Conduct Criminal Record Checks	Low	High
2.	Police Officer's personal information is compromised when transferred to PSB from the police agencies.	PSB will access the personal information of officers on site.	Low	High

3.	Interviewees may provide personal information to PSB as part of the interview.	As per section 27.1 of the *Freedom of Information and Protection and Privacy Act* the information will not be collected and may be provided to another agency if necessary.	Low	High

10. Collection Notice

The following information will be provided to the police officer being interviewed when asking for their availabilities to meet for the interview:

As part of a review of police detention facilities, practices, and standards in British Columbia, the Ministry of Public Safety and Solicitor General's Policing and Security Branch (PSB) will collect your availability to set up a time to meet for an interview to gather your professional opinion about your agencies' police detention facilities. PSB has the authority to collect your personal information as per section 26(c) of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection of this information, you may contact the Director of the Standards and Evaluation Unit at: Suite 405-815 Hornby Street, Vancouver, BC, V6Z 2E6, tel: 778-572-3397.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

s.15

12. Please describe the technical security measures related to the initiative (if applicable).

The LAN and EWS will be on the BC Government infrastructure secured by BC Government firewalls as well as a security multilayered approach, which applies multiple mitigation strategies to protect resources from external and internal threats, will be used to protect the personal information. Sometimes referred to as security-in-depth or layered security, defense-in-depth is a term used to describe the layering of security countermeasures to form a cohesive security environment. The access will be restricted based on roles and responsibilities.

13. Does your branch rely on security policies other than the Information Security Policy?

- Policies prohibiting the sharing of passwords and user ID's
- Policies prohibiting users from posting passwords
- Policies requiring screens to be locked when not in use
- Security incidents must be reported immediately.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

The LAN and EWS are only accessible through a valid BC government user ID and password. Additionally, the secure access will be based on role-and responsibilities.

15. Please describe how you track who has access to the personal information.

s.15

In terms of the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.

- Message Transport logs include message tracking (Exchange server to Exchange server - internal only) which provides a detailed record of message activity, such as sent, received, date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.

- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

Interviewee will have PSB evaluation team's contact information to provide PSB with updated information about their availability.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No. The information will be used to make a high level finding about a police agency's degree of compliance with standards.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/a.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/a.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No. the information is a one-time collection of the personal information of police officers.

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative?

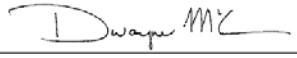
Yes, the emails communication with interviewees about their availability will be collected and stored in the PSB secure LAN Drive

Personal Information Bank – Required Information	
Description	The availability of detention-related staff within each police agency that PSB can interview to gather their professional opinions on police detention facilities.
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General's Policing and Security Branch
All other ministries/government agencies and public bodies involved	None
Business contact title	Director, Standards and Evaluation Unit
Business contact telephone number	778-572-3397

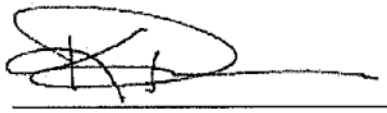
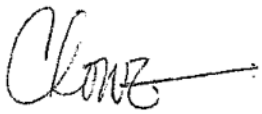
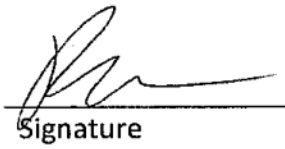
Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Tim Perry		2020-02-28
Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Officer Ministry of Citizens` Services	Signature	Date

Dwayne McCowan		March 4, 2020
Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens` Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua		March 04, 2020
Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Charmaine Lowe		March 11, 2020
A/Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Jenni Bard		Mar 13, 2020
Director Standards and Evaluation Unit Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date
Brenda Butterworth-Carr		March 24, 2020
Tr'injà shär njit dintlät Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date

Privacy Impact Assessment for
Security Programs Division
Criminal Records Review Program
PIA# PSSG20017

Part 1 – General

Name of Ministry:	Ministry of Public Safety and Solicitor General, Policing and Security Branch		
PIA Drafter:	Adriana Alvear, Director Business Transformation		
Email:	Adriana.Alvear@gov.bc.ca	Phone:	250 415-7180
Program Manager:	Michelle Milljour, Director Business Support and Protective Services		
Email:	Michelle.Milljour@gov.bc.ca	Phone:	778 974-3574

1. Description of the Initiative

The *Criminal Records Review Act* (CRRA) ensures that people who work with or may have potential for unsupervised access to children or vulnerable adults undergo a CRRA check by the Criminal Records Review Program (CRRP). The CRRA provides a regulatory framework under which the deputy registrar assesses the criminal history of applicants to identify whether the history reflects a risk of physical/ sexual abuse to children or physical/ sexual/ financial abuse to vulnerable adults

Security Programs Division (SPD) is a division of the Policing & Security Branch in the Ministry of Public Safety & Solicitor General that manages the CRRP and through that program undertakes CRRA checks for people who work, volunteer with, or may have the potential for unsupervised access to children or vulnerable adults.

CRRA requires that organizations in BC ensure that employees working with children and/or vulnerable adults complete a CRRA check through the CRRP every five years. Employer, as defined in the CRRA, includes any organization that is partially provincially funded, licensed, or contracted. The following employers are required to screen their employees through the CRRP:

A. Licensed and Unlicensed Childcare and Licenced Adult Care Facilities

Owners, operators, and managers of a licensed family-run childcare, or a licensed or registered adult care facility, must undergo a CRRA check by the CRRP. The local Health Authority responsible for governing licensed childcare facilities or adult care facilities will inform the proposed owners, operators, or managers of the CRRA check requirement. Employees and volunteers of licensed childcare or adult care facilities or a license-not-required childcare facility must also undergo a CRRA check.

Additionally, individuals that are 12 years old or over and are ordinarily present on the premises of a licensed childcare or licensed or registered adult care facility must also undergo a CRRA check. This includes:

- Exchange students
- Tenants
- Spouses
- Any other individual that may be ordinarily present on the premises of the child care or adult care facility

B. Companies Contracted by Provincially Operated or Funded Organizations

Provincially funded, operated, or licensed facilities that hire contractors must also ensure all contractors who work with or have potential unsupervised access to children and/or vulnerable adults are screened by the CRRP. An Authorized Contact at the provincial entity is responsible for facilitating the CRRA checks for contractors.

C. Teacher Certification Branch

Teachers in BC are required to undergo a CRRA check prior to being licensed.

D. Post-Secondary Institutions

Post-secondary students working with children and/or vulnerable adults as part of a practicum must also undergo a CRRA check.

E. Governing Bodies and Regulated Professions

Members of the following governing bodies are required to undergo a CRRA check for licensing purposes at least once every 5 years:

- British Columbia College of Social Workers
- British Columbia College of Nursing Professionals
- College of Chiropractors of British Columbia
- College of Dental Hygienists of British Columbia
- College of Dental Surgeons of British Columbia
- College of Dental Technicians of British Columbia
- College of Denturists of British Columbia
- College of Dietitians of British Columbia

- College of Massage Therapists of British Columbia
- College of Midwives of British Columbia
- College of Naturopathic Physicians of British Columbia
- College of Occupational Therapists of British Columbia
- College of Opticians of British Columbia
- College of Optometrists of British Columbia
- College of Pharmacists of British Columbia
- College of Physical Therapists of British Columbia
- College of Physicians and Surgeons of British Columbia
- College of Podiatric Surgeons of British Columbia
- College of Psychologists of British Columbia
- College of Speech and Hearing Health Professionals
- College of Traditional Chinese Medicine Practitioners Acupuncturists of British Columbia and
- Teacher Certification Branch

The CRRA also allows for specified organizations in BC to apply to screen volunteers for free through the CRRP. Specified organizations, as defined in the CRRA, generally includes any non-profit organization or any organization that is partially provincially funded, licensed, or contracted. Volunteers must be providing a free service involving direct or potential unsupervised access to children and/or vulnerable adults. Organizations do not qualify for the CRRP's volunteer CRRA check service if any form of monetary compensation is provided to volunteers.

Examples of organizations that commonly qualify to use the CRRP for screening volunteers are:

- Sports clubs
- Adult care facilities
- Child care facilities
- Hospitals, and
- School districts.

Additionally, organizations that are enrolled or registered with the CRRP are required to submit CRRA checks for each independent contractor and subcontractor that may have direct access or potential for unsupervised access to children and/or vulnerable adults. The CRRA check must be processed under the organization that is enrolled or registered with the CRRP.

Organization Registration Process

If an organization that falls under the categories mentioned above needs to have prospective volunteers/ employees apply for a CRRA check, the organization must first register with the CRRP. To apply for an account, organizations must complete the Organization Registration Process which involves a manual registration process.

A. To screen employees through the CRRP, the organization must first fill in an employer enrollment form and questionnaire to assess whether the organization meets the CRRP requirements (i.e. organization falls within the definition of "employer" as per the CRRA and involves working with children or vulnerable adults). The organization will also be required to provide license agreement, contract, and an attestation that the organization is partially provincially funded. Note that CRRA checks for contractors and subcontractor will follow the employees' process.

B. To screen volunteers through the CRRP, the organization must first fill in a volunteer organization registration form and questionnaire. The document will assist the organization with identifying whether the organization meets the requirements and is eligible to participate in the CRRP.

As part of the registration processes, the organization must provide a Primary Authorized Contact who will be responsible for facilitating the CRRA check process for their organization. The CRRP will also allow a Secondary Authorized Contact. To ensure the suitability of an Authorized Contact, the CRRP will require a CRRA check to be conducted for the Authorized contact(s). Currently, SPD performs this process manually. The authorized contact(s) is/are required to submit the CRRA check form along with the organization registration form and questionnaire. Note that if the authorized contact is/will be working with the children or vulnerable adults, they may be required to do a certified criminal record check. For more information see the CRRA Check Risk Assessment section of the PIA below.

Upon completion of the organization registration process, including the CRRA check of the authorized contact(s), the CRRP will confirm registration of the organization in writing and will assign a Party ID number (an account number) for their manual submission process. If the organization requests to enroll in the online service, the organization will also be provided with a unique access code. The unique access code will be required by volunteers, contractors and employees to submit their CRRA check requests online.

If the organization has volunteers and employees covered under the CRRA, they will be required to enroll two separate profiles, one for "volunteers" and one for "employees" (also includes contractors). Should the organization use the online service, the organization will have one unique access code for employees and one for volunteers.

Manual CRRA Check Process

Organizations will have the ability to request that their contractors, volunteers, or employees fill in a physical/ paper CRRA check application form. As part of this process, the organization's authorized contact will be responsible for confirming that the applicant's identification has been verified and will be required to sign the Consent Cover Letter. They will also be submitting on behalf of the applicant the applicant's consent form signed by the applicant.

For payment, the majority of applicants will provide their personal email and the CRRP will send a payment link to the email. The applicant may also forward this email to their organization to pay should the organization pay the fee for the CRRA check. Alternatively, the applicant and organization will have the ability to submit a pre-authorized credit card form with their application. This is received by mail. Lastly, the application can be submitted (via mail) with cheque or money order.

CRRP Online Services

There are two online service streams available through the CRRP:

- Applicant-Based Online Service (eCRC)
- Organization-Based Online Service (BCeID)

These services provide organizations a convenient option for facilitating the CRRA check process. Both online services are available 24 hours a day, seven days a week.

A. Applicant-Based Online Service (eCRC)

The eCRC online service is available for employer and volunteer organizations that have registered with the CRRP. Enrollment into the eCRC may be selected while enrolling an organization or at a later date through the Organization Account Information Update Process.

Once an organization receives confirmation of their enrollment in the eCRC online service, a unique access code will be issued to the organization.

The access code is given to applicants and enables them to access the online service portal to submit their CRRA check requests online. The access code never expires and also allows for the sharing of CRRA check findings. However, the code can be changed at any time upon the request of the organization. The access code is not to be posted publicly. This will prevent members of the public from applying to the organization without any initial contact with an Authorized Contact person.

B. Organization-Based Online Service (BCeID)

The BCeID online service is for organizations that have a Business BCeID account or an IDIR ID (internal government) account.

The organization generates an individual code for each applicant which may only be used once within a two-week period and does not allow for the sharing of CRRA check findings.

Whether the organizations are using Business BCeID or IDIR to access the online system, the 'identification' needs to be 'authorized' by the CRRP to enter the system.

To get started, the organization must name a 'Primary User' (also referred to as the Business Account Manager) and if applicable Secondary users to act on the organization's behalf. These individuals are responsible for administering and monitoring access to the online service for the organization.

The organization's primary user must complete, sign, and send the CRRP Online Service Agreement to SPD to be authorized to use this online system. The Online Service Agreement outlines the responsibilities of the organization and the organization's primary user. The agreement also outlines the responsibilities of CRRP when CRRA checks are processed through the online service. An organization's profile (name, address and payment type/method) will be provided to SPD and the profile will be displayed on the online service main screen once the primary user has signed in.

To use an IDIR to access the services, the organization submits their completed Online Service Agreement to the CRRP and once they have received confirmation, the IDIR user ID is linked to the organization. The organization will be required to sign in using their IDIR to finalize the on-boarding process.

For organizations outside of government, a Business BCeID will be used to authenticate an organization that is applying for registration for a CRRP account and to provide the business access to the relevant SPD programs.

The BCeID is an online system (separate from the SPD online service) that makes it possible for an 'authorized user' of an organization outside of government to participate in government online services via a log-in ID and secure password. Note that the business accessing the portal will be required to be registered as a business in BC to receive a Business BCeID. The CRRP does not manage BCeID; it is a separate process that organizations must complete prior to accessing the SPD online service.

As part of improving SPD's digital platform, the organization registration process for authorized contacts will develop an online process where the authorized contact(s) of an organization that has yet to be registered will have the ability to do their CRRA check online using their BC Services Card.

IM/IT Solutions

SPD will develop a Security Program Services (SPS) portal to manage its online services. The portal will utilize an OpenShift Online application which will be integrated with a Customer Relationship Management (CRM) Service application, currently the SPD Criminal Record Review (CRR) Module of FIGARO, for document management and case management. The portal will be installed and run on the BC Government Information Technology Infrastructure.

The SPS portal will support the following processes:

- Organization Authorized Contact authentication (using the BC Services Card)
- Applicant authentication (using the BC Services Card)
- Application for a CRRA check
- Payment for a CRRA check

The SPS portal will eventually also assist with the Organization authentication (Through Business BCeID or a manual process) and the organization registration with SPD to access security program services which will be assessed in a future PIA.

Personal information submitted through the application portal will only persist within the case management system. The portal will have multiple screens to guide users to their desired destination.

Electronic Identity Verification (EIV)

The applicant based online service, known as the eCRC, verifies an applicant's identity using Electronic Identity Verification (EIV). EIV meets the RCMP's standard for electronically verifying an applicant's identity with an online process that confirms an individual's identity. For BC residents with a BC Services Card, this will be the gold standard for ID verification.

The Provincial Identity Information Management (IDIM) program will support SPD authentication of a person using the BC Services Card. Individuals will be enabled to use their BC Services Card to authenticate their identity and to access the CRRP online services.

Individuals, who are eligible B.C. residents, will be required to use their BC Services Card to authenticate their identity as part of the online CRRA check application process. If the individuals do not meet the BC residency requirements for the BC Services Card (i.e. new resident to B.C. or visiting), they will not be able to use the SPS portal and will have to follow the manual process.

Payment

CRRA checks are offered free of charge to volunteers who work with organizations registered with the CRRP, and to authorized contacts of those organizations that do not work directly with children or vulnerable adults. For all other individuals, there is a processing fee. There is also no fee for a volunteer or employee to request to share a CRRA check findings.

Payments can be done manually as part of CRRA check manual process (i.e. physical forms) where financial information (e.g. credit card, money order, etc.) is manually collected by SPD. However, the majority of payments from manually submitted applications are processed through links emailed to the applicants that direct them to a one time use link through Bambora/BC Express Pay.

Organizations also have the option of using pre-established draw-down account withdrawal or credit card.

For the organization-based online service, the preferred payment option is established in the online service agreement. Organizations also have the option to generate a one-time access code so applicants can submit their own CRRA check online using the organization-based online service. The organization will generate a single use access code and URL and will provide it to the applicant – this allows the organization to pay for the CRC.

A. Draw Down Account

The draw-down account option allows organizations to keep funds in a secure account, pre-authorizing the CRRP to withdraw fees per CRRA check request submitted online. The CRRP will provide the organization with a monthly statement to assist in monitoring the account.

In a future iteration, the SPD online service main page will provide the ability for organizations to access their draw-down account balance so it may be easily monitored. If funds are low, the organization may provide CRRP with a certified cheque or money order (made payable to the Minister of Finance) to replenish the account or the account may be replenished through the organization's VISA or MasterCard by faxing or mailing the CRRP a completed Application for Pre-Authorized Credit Card Usage form. The organization's financial information is collected by SPD. If the organization's draw-down account balance is zero, but the organization has CRRA check requests in pending that require payment, the SPD online service will allow the organization to opt to pay for the currently outstanding CRRA check requests using the organization's credit card.

B. Credit Card Payment

The credit card option allows organizations to enter VISA, MasterCard, American Express, Mastercard Debit, Visa Debit, and in a future iteraction will also accept Online Debit information when paying for submitted CRRA check requests. The organization may provide a single use access code and URL to the applicant to submit their own CRRA check online using the organization-based online service – this allows the organization to pay for the CRC. A credit card information entry is required each time the organization is ready to provide payment for CRRA check request(s). After paying, either a receipt will be generated if the payment was successful, or a declined message if there was a problem with the transaction. If there was a problem, there is the option to try again so you may enter new or correct credit card information.

Applicants will enter their financial information separately from the personal information provided for the CRRA check, through a government-approved online payment portal (BC Express Pay 2.0/Bambora). Payment info will be collected on a separate webpage (which will look seamless to the user) than the order page and all payment information (i.e. credit card information) will be sent to the Ministry of Finance through the BC Express Pay 2.0/Bambora.

CRRA Check Risk Assessment

As per current RCMP Canadian Police Information Centre (CPIC) policy, the individuals are required to consent to the CRRA checks. Specified checks are based on the program and may include CRRA checks or fingerprint-based criminal record verification by searching the CPIC database, police information checks, checks of records in the Justice Information System of the Ministry of Attorney General and checks of records in the corrections information system of the Ministry of Public Safety and Solicitor General.

Collection of the personal information will be necessary for the CRRP to carry out the applicant's CRRA check. The Criminal Records Review Unit (CRRU), which is embedded within the Combined Forces Special Enforcement Unit, supports the CRRP by conducting checks of CPIC and, in some instances, Police Records Information Management Environment (PRIME) to assist SPD in fulfilling its statutory functions. The *Privacy Act* applies to CRRU.

The information will be disclosed by SPD to CRRU through direct access to the CRR Module in FIGARO. CRRU will confirm the identity of individuals who are requiring or requesting a CRRA check or screening from SPD and they will then cross-check this information against data in CPIC. They will only access PRIME where there is a relevant/ specified offence (as defined in the CRRA) in CPIC. CRRU will input applicant's CRRA checks and tombstone data about pertinent police information check records into FIGARO or email it to SPD. Note that CRRU employees will have and use BC Government IDIR and email addresses.

When name-based CRRA checks will not provide a definite way of confirming a person's identity, CRRU will inform SPD, who will mail out a letter to the applicant requesting that they get a "certified criminal record check" done at their local law enforcement agencies/detachment. The local law enforcement agency or RCMP detachment will collect the applicants' fingerprints and provide the fingerprints to the RCMP's Canadian Criminal Real Time Identification Services (CCRTIS), who will conduct a search of the National Repository of Criminal Records.

The use of fingerprints for criminal record checks is based on informed consent and the applicant will be asked to consent to the disclosure of the results of the check to SPD on the application form.

The fingerprints submitted to CCRTIS for criminal record checks will only be used to confirm the applicants' identity. At no time will the fingerprints be added to a database where they could be subject to search and the fingerprints will not be provided to SPD.

As part of the CRRA check, SPD will also conduct a CORNET check through a CORNET-FIGARO API and may undertake JUSTIN check through direct access to that database when the CRRU check returns a relevant/ specified offence. CORNET is the BC Corrections Offender management system and JUSTIN is the Province's computerized criminal justice system which are hosted on BC Government infrastructure in Canada.

All of the collected information will inform the risk/ no risk finding of the CRRA checks which will be provided to the organization.

Reconsideration

If the deputy registrar (i.e. SPD) makes a determination that the applicant presents a risk of physical or sexual abuse to children or a risk of physical, sexual or financial abuse to vulnerable adults, the individual may request a reconsideration of the determination by serving SPD with written notice within 30 days after the day on which SPD notified the individual of the determination. SPD may request additional information from the organization or the individual and convene a hearing. For the purposes of a hearing the registrar, by summons, may require a person to attend as a witness and to bring and produce all relevant documents in the person's possession.

After conducting a review, the registrar will either confirm or overturn the determination and direct that the individual does not present a risk of physical or sexual abuse to children or does not pose a threat of physical, sexual or financial abuse to vulnerable adults; and promptly provide notification of a decision to the individual who is the subject of the decision and to the persons or entities that were provided with the original notification. The registrar will be required to provide written reasons for the decision to the individual who is the subject of the decision, if the individual so requests, and to the organization, if requested.

Sharing a CRRA Check

If a CRRA check has been completed within the last 5 years through the SPD CRRP; the request was for the same type of check as previously completed, either for children, vulnerable adults, or both children and vulnerable adults; and there was no risk identified, an individual may share a previous CRRA check. The individual will utilize the organization's unique access code provided by the new organization to request that the previous CRRA check be provided to the organization. The process will require the individual to review the new organization's profile to confirm that it is the correct organization. The individual will then perform the EIV using the BC Services card following the process mentioned above. Once the individual confirms the information, the request to share a CRRA check findings is complete and the organization will receive the findings.

If no CRRA check was done in the last 5 years or that the finding of the check identified that the individual who authorized the CRRA check presented a risk of physical or sexual abuse to children or a risk of physical, sexual or financial abuse to vulnerable adults, the new organization will be notified.

2. Scope of this PIA

The PIA will assess the privacy implications of the overall CRRP, including the development of the SPS portal and the onboarding of the IDIM services (i.e. BC Services Card and Business BCeID) to authenticate organizations and verify individuals' identity. Note that the current EIV through Equifax is out of scope of this assessment as it will be phased out as programs are being onboarded into the BC Services Card. Additionally, the real time identification and the information collected by BC Express Pay/Bambora are also out of scope of the PIA as they have previously been assessed (see below).

3. Related Privacy Impact Assessments

PSSG18029	Cannabis Licensing Security Checks
AG18029	Cannabis Integration Initiative
PSSG17008	Real Time Identification
JUST-13109	Volunteers under the CRRA
FIN15017	BC Express Pay (BCEP) 2.0 Lite-Banking and Cash Management
FIN12020	BC Express Pay-Banking and Cash Management
CTIZ12047	BC Services Card PIA
MTICS14007	BC Services Card Release 2 Implementation
CITZ17025	Exchange
CITZ18019	BC DevOps OpenShift Service

4. Elements of Information or Data

A. <u>Registration of Organizations</u>

SPD will collect the following information from the organization as part of an organization's enrollment process:

- Organization Name
- Organization general email and phone

- Email for CRRA Check Findings
- Mailing and physical addresses
- Authorized primary contact and title
- Authorized secondary contact and title
- The default category of CRRA Check to be performed for the organization (i.e. works with children, works with vulnerable adults, or both)
- Schedule Type
- Whether the organization fall under the “employer” definition of the CCRA

The organization will also be required to provide license agreement, contract, funding arrangement, and attestation, to identified whether the organization is partially provincially funded.

In the context of registering an organization for screening volunteers through the CRRP, the following additional information will be provided to SPD:

- Whether volunteers receive any monetary compensation as part of their volunteering
- Whether the volunteering provides a benefit to children or vulnerable adults and whether there is direct contact with these populations
- Whether the organization falls under the definition of "specified organization" as per the CRRA
- Whether the organization is a registered charity, or a non-profit organization registered with BC Corporate Registries

The registration may also include the organization providing the organization’s Bylaws, Constitution, or other supporting documentation that confirm the non-profit registration status. These documents do not include personal information.

Once registered, SPD will provide the organization a unique access code.

SPD will also collect the following information from the organization when the application is done manually to ensure the suitability of an Authorized Contact. The application will require a CRRA check of the Authorized Comtact to be conducted and ID to be verified:

- Name of Individuals including maiden names
- Alias
- Date of Birth
- Gender

- Place of birth
- Mailing Address
- Residential Address
- Phone number
- Driver Licence number or BCID
- Email address
- Job Title with Organization

In the context of the alternate online process, the organization's authorized contact(s) will use their BC Services Card to do their CRRA check online (see below the BC Services Card section).

B. Organization-Based Online Service (BCeID)

As part of requesting authorization to use the Organization-Based online service using the Business BCeID or a BC Government IDIR, the organization fill in an Online Service Agreement for Online Submissions of Requests for Criminal Record Checks and the following information will be provided by the organization to CPPR:

- Name of organization,
- Address of organization
- Contact name
- Phone number of the organization
- Fax number of the organization
- The category of CRRA check to be performed for the organization
- The organization's primary user method of access to the Online System (i.e. BCeID or IDIR)
- Primary user's name and contact information
- Method of payment
- Schedule Type
- Name and email of the person who will receive the risk/ no risk findings of the CRRA checks (i.e. Findings Contact)

The organization's online service profile will be displayed on SPD online service main screen once the primary user has signed in.

C. Payment

The organization may provide the following information to SPD:

- Name of organization
- Contact name
- Mailing address
- Area code and phone number
- Payment (i.e. money order, cheque, credit card information, etc.)

The following information will be provided by FIN to SPD as part of the BC Express Pay 2.0/Bambora payment process:

- date of payment,
- IP of payer, and
- success or failure code

D. Business BCeID will provide the following information to SPD:

- Name of Business
- Name of the organization's Authorized Contact

E. BC Services Card:

Once the organization's Authorized Contact, the volunteers, contractors, or employees identify have been verified using their BC Services Card in the SPS portal, the following information will be provided to SPD and will pre-populate the CRRA check application:

- Primary Documented Surname
- Primary Documented Given Name
- Primary Documented Given Names
- User Display Name - The individual's name which is their preferred name if available or composed of their documented name.
- Birth Date
- Sex
- Street Address
- Locality
- Province
- Postal Code
- Country

F. CRRA Check

Once the authorized contact(s), the volunteers, contractors, or employees identify has been verified using their BC Services Card, the individuals will be prompted to enter their birth place, driver's licence number, the previous name, maiden names, aliases, city, country, personal email address, and position/title within the organization, organization type (e.g. division within the organization), and contact phone number. The portal also provides the opportunity for the applicant to provide a mailing address if the address is different than the address provided by the BC Services Card.

a) BC Corrections

The following information will be collected from BC Corrections through the FIGARO-CORNET integration:

- Names and any alias
- Correctional Service # (CS#),
- History of contact with BC Corrections, and
- Date of birth.

b) CRRU

The element of information provided by SPD to CRRU:

CRRU will have direct access to FIGARO and through that the following information will be provided:

- Names (i.e. first, last, and middle name)
- Alias
- Date of Birth
- Gender
- History of contact with BC Corrections
- CS#

The following information may be provided, if available:

- Current address
- Driver's license or BC ID number.

CRRU will let SPD know through access to FIGARO whether an applicant has charges, convictions and outstanding warrants and a record of contact with police that the CRRU determines more likely than not to apply to the applicant; and that are explicitly stated in the schedules of the CRRA as relevant/ specified.

This can include complaints, ongoing or closed investigations, driver interactions, victims of crime, children at risk, and intoxication. If there are no charges or records that potentially applies to this applicant, a clearance is issued.

c) Court Services Branch

The following information may be collected by SPD from direct access to JUSTIN:

- Identifying information (i.e. name);
- charges, convictions and outstanding warrants;
- a record of contact with police, BC corrections, and the judicial system; and
- data of birth.

d) Risk Findings and Communication

The risk/ no risk findings of the CRRA check will be sent directly to the relevant organization once completed. Note: A CRRA check is considered complete once the risk/ no risk findings of the check has been issued to an organization

e) Sharing a CRRA Check

If the CRRA check has been completed within the last 5 years through the SPD CRRP and the request was for the same type of check as previously completed, either for children, vulnerable adults, or both, an individual may share a previous CRRA check. The individual will utilize the organization's unique access code provided to the individual to access the SPS portal.

The individuals will be required to review the organization's profile, including name and address and confirm that organization type (Employee or Volunteer account) and working category (e.g. working with children).

The individual will then perform the EIV using the BC Services card, confirm the validity of the information prepopulated by the BC Services Card, provide additional information, if needed such as a different mailing address, and enter their birth place, driver's licence number, the previous name, maiden names, alias, city, country, personal email address, and position/title within the organization, organization type (e.g. division within the organization), and contact phone number. Note that if the applicant identifies that the information collected from the BC Services Card is inaccurate, they will be redirected to contact ICBC to make the changes.

FIGARO will confirm whether the applicant has a valid CRRA check on file and if there is one, it will provide the ability for the applicant to share the CRRA check with the new organization.

Once the individual confirms the information, the request to share the findings of the CRRA check will be complete and the organization will receive the findings. If there are no CRRA check, the applicant and organization will be notified.

G. Certified Criminal Record Check

In some circumstances, the findings of a CRRA check may require an applicant to submit their fingerprints to a police agency as a definite way of confirming their identity. The police detachment will send the fingerprints to CCRTIS to verify if an individual has a record for pardoned sex offences. CCRTIS will provide the result of the check to SPD.

H. Audit

FIGARO Audit Logs will identify which users have made edits to a case and what changes have been made.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The personal information will be stored on BC Government infrastructure in Canadian servers and the information will only be accessed within Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act.	
1. Personal information from one database is linked or combined with personal information from another database;	yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	n/a

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes

3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPPA regulation.	no

8. Personal Information Flow Table

Personal Information Flow Table - Registration of Organization			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	To apply for an SPD CRRP account, an organization must register and may fill in a physical enrollment form and questionnaire.	No Personal Information involved	Not Applicable
2.	To apply for a CRRP account, the organization may also use the SPD online services and click on the SPD online portal (SPS) sign-in button where they will be redirected to the BCeID (Shared Services BC) website to authenticate themselves using their Business BCeID (BBCeID) and password or their BC Government IDIR and password. If the applicants do not have a BBCeID, they will be directed to the BC Registry Services to register. This process is out of scope of this initiative. Once authenticated, the organization will be redirected back to SPS portal. Once identified, the organization's primary user must complete, sign, and send the CRRP Online Service Agreement to SPD to be authorized to use the SPD online system. The agreement will also include the organization's online profile. A unique code will be provided to the organization.	No Personal Information involved	Not Applicable
3.	As part of the registration process, the organization will also make decision around payment methods. If the organization decides to use a Draw Down Account, the organization will provide its financial information (i.e. credit card) to the CRRP.	No Personal Information involved	Not Applicable

4.	The organization may also enroll in the CRRP eCRC process.	No Personal Information involved	Not Applicable
5.	As part of the registration process, a CRRA check must be completed on the organization's authorized contact(s). First the organization may use the manual process and as part of this process verify the identity of the authorized contact(s) and provide the authorized contacts' confirmation of identity verification, CRRA check form and consent to SPD; and, if necessary, their credit card information to pay for the associated fee.	Collection	26(c) and (e) 27(1)(a)(i)
6.	The collected personal information will be manually entered in FIGARO	Use	32(a)
7.	The organization may also direct the authorized contact(s) to use the SPD online services. The authorized contact(s) will click on the SPS portal where they will be redirected to the BC Services Card log in. As part of the authentication process, SPD will collect specific data elements from the BC Services Card about the authorized contact that is applying for the CRRA check and the information will prepopulate the SPD CRRA check request form. Note that prior to login into the BC Services Card system, the individuals will be required to activate their cards. This is outside of the scope of this PIA.	Collection	26(c), (e) and (h)(ii) 27(1)(b) [33.1(5)(b)]
8.	Once authenticated, the individuals will be redirected to the SPS portal to fill in the required information which will be inputted in FIGARO.	Collection	26(c) and (e)

9.	Once the required information has been provided in the SPS portal, the applicant will be redirected to Express Pay 2.0/Bambora to pay the required fee, if required. Express Pay 2.0/Bambora will identify to SPD that the fee is paid. The transactions will be done anonymously. Payment info will be collected on a separate webpage (which will look seamless to the user) than the order page and all payment information (i.e. credit card information) will be sent to the Ministry of Finance through the BC Express Pay 2.0/Bambora. The contact will be redirected back to SPS once the payment has been made.	Outside of the scope of this PIA.	Not applicable
10.	SPD will review the applicant's submission for accuracy and may contact the organization authorized contact(s) if it is necessary for clarification or correction. Additional information may be gathered.	Use Disclosure Collection	32(a) 33.2(a) 26(c) and (e)
11.	As part of the CRRA check, SPD will access relevant information in the corrections information system of the Ministry of Public Safety and Solicitor General (i.e. CORNET) through system integration between CORNET and FIGARO to inform the adjudication.	Collection	26(c) and (e) 27(1)(a)(i) and (b) [33.2(a)]
12.	The personal information in FIGARO will be accessed by CRRU to affirm the identify of the relevant person and to do a police check on that person. The disclosure of the information is through CRRU's access to the FIGARO system.	Use Disclosure	32(a) and (c) 33.1(1)(b) and 33.2(a)
13.	Once CRRU has completed their search and analysis, CRRU will provide SPD with relevant information about the applicant. For example, if there are no risks identified, CRRU will update the status in FIGARO.	Collection	26(c) and (e) 27(1)(a)(i)

14.	When CRRU searches CPIC, they will determine if there is vulnerable sector hit and will inform SPD. SPD will mail out a letter to the applicant identifying to the applicant that they will be require to get a "certified criminal record check".	Collection Use	26(c) and (e) 27(1)(a)(i) 32(a) and (c)
15.	The use of fingerprints for criminal record checks is based on informed consent and the applicant will be asked by the local law enforcement agency to consent to the disclosure of the results of the check to SPD on the application form. SPD will only collect the result of the fingerprints check, not the actual fingerprints.	Collection	26(c) and (e) 27(1)(a)(i)
16.	If there are risks identified by CRRU, SPD may access the justice information system of the Ministry of Attorney General (i.e. JUSTIN) to inform the adjudication.	Outside of the scope of FoIPPA Collection	s.3(a) 26(c) 27(1)(a)(i)
17.	SPD will review all of the information provided to assess whether the organization is eligible to participate in the CRRP and, if the organization has been identified as eligible, SPD will advice the organization and provide them with a unique access code	Use Disclosure	32(a) 33.2(a)

Personal Information Flow Table – CRRA Checks			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	In the manual process, the organization's authorized contact(s) verify the identity of the volunteer, contractor, or employee that requires a CRRA check and once the volunteer, contractor, or employee has filled out the CRRA check application form, the authorized contact send SPD the requested information/forms, and payment information.	Collection	26(c) and (e) 27(1)(a)(i)

2.	As part of the online eCRC process, the organization will provide to its volunteers, contractors, and employees its unique SPD access code. The volunteers, contractors, or employees of organizations who are needing to complete a CRRA check will input the organization's unique access code into the SPS portal to confirm the organization that they will be working or volunteering for and their role (i.e. volunteer, employee) and the work with category (i.e. children, vulnerable adults) .	No Personal Information involved	Not Applicable
3.	Once applicants confirm the organization and the relevant information, they be redirected to the BC Services Card log in to verify their identity. As part of this authentication process, SPD will collect specific data elements from the BC Services Card about the individuals. Note that prior to login into the BC Services Card system, the individuals will be required to activate their cards. This is outside of the scope of this PIA.	Collection	26(c), (e) and (h)(ii) 27(1)(b) [33.1(5)(b)]
4.	Once authenticated, the individuals will be redirected to the SPS portal to fill in the required information and provide the organization's unique access code which will be inputted in FIGARO.	Collection	26(c) and (e)

5.	Once the required information has been provided, the applicant will be redirected to Express Pay 2.0/Bambora to pay the required fee, if required. Express Pay 2.0/Bambora will identify to SPD that the fee is paid. The transactions will be done anonymously. Payment info will be collected on a separate webpage (which will look seamless to the user) than the order page and all payment information (i.e. credit card information) will be sent to the Ministry of Finance through the BC Express Pay 2.0/Bambora. The contact will be redirected back to SPS once the payment has been made.	Outside of the scope of this PIA.	Not applicable
6.	Individuals applicants will have the ability to access and change their personal information stored via the SPS portal until the application is submitted. Note that in a future iteration, the applicants will also have the ability to make additions or changes to their personal information (where the information is not provided from the BCSC) once the application has been submitted. The information provided from the BCSC would need to be changed through the normal BCSC processes as opposed to being edited in the portal.	Disclosure Collection	33.2(a) 26(c) and (e)
7.	Through a system integration, a check of the corrections information system of the Ministry of Public Safety and Solicitor General (i.e. CORNET) will inform the adjudication.	Collection	26(c) and (e) 27(1)(a)(i) and (b) [33.2(a)]
8.	CRRU will access the personal information in FIGARO to affirm the identify of the relevant person and to do a police-check on that individual. This is consented to via the Criminal Records Review Application.	Disclosure	33.1(1)(b) 33.2(a)
9.	Once CRRU has completed their search and analysis, CRRU will provide SPD with relevant information about the applicant.	Collection	26(c) and (e) 27(1)(a)(i)

10.	If CRRU identifies relevant/ specified offences in CPIC in accordance with the CRRA, SPD may access the justice information system of the Ministry of Attorney General (i.e. JUSTIN) to inform the adjudication.	Outside of scope of FoIPPA Collection	s.3(a) 26(c) 27(1)(a)(i)
11.	When CRRU searches CPIC, they will determine if there is vulnerable sector hit and will inform SPD. SPD will mail out a letter to the applicant identifying to the applicant that they will be required to get a "certified criminal record check".	Collection Use	26(c) and (e) 27(1)(a)(i) 32(a) and (c)
12.	The use of fingerprints for criminal record checks is based on informed consent and the applicant will be asked by the local law enforcement agency to consent to the disclosure of the results of the check to SPD on the application form. SPD will only collect the result of the fingerprints check, not the actual fingerprints.	Collection	26(c) and (e) 27(1)(a)(i)
13.	SPD will use all of the information collected to inform their adjudication, which will eventually conclude with either a risk/no risk decision and will be provided to the organization. Note that in a future iteration, organizations may be able to review their employees, volunteers, and contractors CRRA check status through the SPS portal.	Use Disclosure	32(a) and (c) 33.1(1)(c) [s. 4(2) and (4) of the CRRA] 33.2(a)
14.	If the findings of the check identified that the individual who authorized the CRRA check presents a risk of physical or sexual abuse to children or a risk of physical, sexual or financial abuse to vulnerable adults, SPD will determine if another person or entity, within 5 years of the date of the CRRA check authorization was identified in a CRRA check authorization or a CRRA check verification authorization in respect of the individual.	Use	32(a) and (c)

15.	If there is a person or entity described above, SPD will take reasonable steps to determine if the individual continues to work with children or work with vulnerable adults for the person or entity.	Disclosure Collection Use	33.2(a) 26(a) [s.4(4.2) of the CRRA] (c), and (e) 27(1)(a)(iii) 32(a) and (c)
16.	If SPD determines that the individual continues to work with children or work with vulnerable adults for the person or entity, SPD will provide notification to that organization that the individual presents a risk.	Disclosure	33.1(1)(c) [s.4(4.2) of the CRRA]

Personal Information Flow Table – Reconsideration			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	If the deputy registrar (i.e. SPD) makes a determination that the applicant presents a risk of physical or sexual abuse to children or a risk of physical, sexual or financial abuse to vulnerable adults, the individual may request a reconsideration of the determination by serving SPD with written notice within 30 days after the day on which SPD notified the individual of the determination.	Collection	26(c) and (e)
2.	The registrar may request additional information from the organization or the individual and convene a hearing. For the purposes of a hearing SPD, by summons, may require a person to attend as a witness and to bring and produce all relevant documents in the person's possession.	Disclosure Collection	33.1(1)(c) [s. 5(2) of the CRRA] 26(a) [s. 5(2),(3) of the CRRA], (c), and (e) 27(1)(a)(iii)

3.	After conducting a review, the registrar will either confirm or overturn the determination and direct that the individual does not present a risk of physical or sexual abuse to children or does not pose a threat of physical, sexual or financial abuse to vulnerable adults; and promptly provide notification of a decision to the individual who is the subject of the decision and to the persons or entities that were provided with the original notification. The registrar will be required to provide written reasons for the decision to the individual who is the subject of the decision, if the individual so requests, and to the organization, if requested.	Use Disclosure	32(a) and (c) 33.1(1)(c) [s.5(7) of the CRRA]
4.	If the clearance is not granted, the individual may apply for a judicial review of the decision.	Out of scope of FoIPPA	Not applicable

Personal Information Flow Table – Sharing of CRRA Checks			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	If a CRRA check has been completed within the last 5 years through the SPD CRRP and the request was for the same type of check as previously completed, either for children, vulnerable adults, or both children and vulnerable adults, an individual may request for the CRRA check to be shared with another CRRP registered organization.	Collection	26(c) and (e)
2.	If the CRRA check is portable, meaning that the authorization for the CRRA check was signed by the individual within 5 years of the date of a CRRA check verification authorization; and the CRRA check did not findings in a determination that the individual who authorized the CRRA check presents a risk of physical or sexual abuse to children or a risk of physical, sexual or financial abuse to vulnerable adults; the findings of the check will be provided to the new organization.	Use Disclosure	32(a) 33.1(1)(c) [6.1(2) of the CRRA]

3.	If no CRRA check was done in the last 5 years or that the findings of the check identified that the individual who authorized the CRRA check presented a risk of physical or sexual abuse to children or a risk of physical, sexual or financial abuse to vulnerable adults, the applicant and the new organization will be notified.	Use Disclosure	32(a) 33.1(1)(c) [6.1(3) and (4) of the CRRA]
4.	At the request of the relevant organization or applicant, SPD is required to provide the reason for the determination.	Collection Use Disclosure	26(a) [s.4(5) of the CRRA], (c), and (e) 27(1)(a)(iii) 32(a) 33.1(1)(c) [s.4(5) of the CRRA]
5.	The Information System Branch of the Ministry of Attorney General may access the personal information in FIGARO for maintaining, repairing, troubleshooting or upgrading the application. The access will be localized.	Disclosure [SPD] Collection [ISB] Use [ISB]	33.1(1)(p)(i) 26(c) and (e) 27(1)(b) 32(a) and (c)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes	Privacy Training Standards of Conduct Criminal Records Check	Low	High
2.	Request may not actually be from applicant.	The individual identity verification will be done using the BC Services Card or by the organization.	Low	High

3.	Applicants' personal information is compromised when transferred to and from the CRRU.	s.15	Low	High
4.	Applicants' personal information is compromised when provided to the organizations.	The findings of the check (i.e. whether a risk has been identified) is provided to the relevant organization by email. As part of the registration process, SPD creates a unique access code for the new organization that is linked to the organization's SPD profile and contact email. In the context of the manual process, SPD provides the organization with a CRRA check application form which is prepopulated with the organization's unique access code. With the online services, the applicant will be required to provide the organization's unique access code as part of the application to link their application to the organization's profile but also to provide the applicant with the opportunity to review the organization's profile and contact information to confirm that this is indeed the organization that should receive the findings of the applicant's CRRA check.	Low	High

10. Collection Notice

The following collection notice will be provided to individuals participating in the CRRP as part of the terms of use of the SPS and in the case of the manual process on the physical forms:

> "The Security Programs Division will collect your personal information for the purpose of fulfilling the criminal record check requirements of the *Criminal Records Review Act* and in accordance with section 26 (c) of the *Freedom of Information and Protection of Privacy Act* (FoIPPA). Additionally, SPD may collect personal information under section 26(e) of FoIPPA for the purpose of evaluating the Criminal Records Review Program and activities to better serve you. Should you have any questions about the collection, use, or disclosure of your personal information, please contact the Policy Analyst of the Criminal Records Review Program, Security Programs Division via mail to PO Box 9217 Stn Prov Govt Victoria, BC V8W 9J1; email to criminalrecords@gov.bc.ca; or by telephone at 1- 855-587-0185 (option 2)."

In the context of the information sharing with CRRU, a Collection Notice will not be required as per section 27(3)(c) of the FoIPPA as the information will not collected directly from the individual and the indirect collection is authorized as per section 27(1)(a)(i) or (iii) of FoIPPA.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

s.15

12. Please describe the technical security measures related to the initiative (if applicable).

With regard to information located in FIGARO, users access the application from a government workstation by logging into their workstations and local network using their government provided IDIR user ID and password, and then must log into the application with their FIGARO Oracle user ID and password. The access will be restricted based on roles and responsibilities.

As for the SPS portal, there will be two levels of access control:

s.15

In the context of email, the EWS system is only accessible through a valid BC government user ID and password.

s.15

13. Does your branch rely on security policies other than the Information Security Policy?

No.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

In the context of email, the EWS system is only accessible through a valid BC government user ID and password.

The access to FIGARO will only be accessible through valid user ID and password, and access restriction will be a combination of role-based, record-level, and field-level security to define the overall security rights that users will have within FIGARO.

15. Please describe how you track who has access to the personal information.

FIGARO will log which users have edited a case and what changes have been made.

s.15

Auditing will be undertaken on receipt of a credible complaint, information incident, data quality concerns, criminal or operational intelligence (with data security implications).

In terms of the EWS, Microsoft Exchange generates a number of logs:

- EWS is hosted in Internet Information Services (IIS) on the Exchange server which records activity in the IIS logs. These logs are archived and retained for 13 months unless there is a litigation hold.
    - The EWS client protocol can be used both by internal and external clients through the Reverse Proxy service, Threat Management Gateway (TMG). Connections through TMG are logged with client IP address and these logs are retained for 7 days.

- Message Transport logs include message tracking (Exchange server to Exchange server - internal only) which provides a detailed record of message activity, such as sent, received, date\time and message subject. These logs are archived and retained for 13 months unless there is a litigation hold.

- Exchange also produces various protocol logs for a short time on the server for troubleshooting purposes. The protocol logs age out or are deleted as space requires.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

Applicant will be able to update their personal information through SPS for information until the application is submitted. Note that in a future iteration, the applicants will have the ability to make additions or changes to their personal information (where the information is not provided from the BCSC) once the application has been submitted. The information provided from the BCSC would need to be changed through the normal BCSC processes as opposed to being edited in the portal.

If an applicant identifies that their information needs to be revised or corrected, SPD will make an annotation or correction to the file. If the information has already been shared with CRRU within the last year, SPD will notify the unit.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Once the CRRA check is carried out, SPD will notify the relevant organization of whether:

- the applicant has an outstanding charge or conviction relating to a relevant or specified offence; and whether
- a determination of risk or no risk has been made.

This information will affect the applicant's eligibility to work or volunteer for the organization because as per section 11 of the CRRA, if the deputy registrar (i.e. SPD) identifies a risk in the employee, volunteer, or contractor working in close proximity or with children or vulnerable adults, the organization does not have discretion.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

SPD will verify the identity of the applicant through in-person check or through digital means (i.e. BC Services Card). In certain circumstances, the person may be required to do a fingerprint check with a police agency to confirm their identity. In these cases, SPD will recieve a copy of the fingerprint report from the police agency.

19. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Yes, SPD has an approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Yes, there is systemic information exchange between SPD and CRRU for the purpose of criminal records review.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.	X

Information Sharing Agreement – Required Information	
Description	A regular exchange of personal information between Criminal Records Review Unit (CRRU) and the Ministry of Public Safety and Solicitor General, Security Program Division (SPD) in order to provide CRRA checks and screenings to individuals.
Primary ministry/government agency involved	Ministry of Public Safety and Solicitor General, Policing and Security Branch, SPD

All other ministries/government agencies and public bodies involved	CRRU
Business contact title	Director Business Support and Protective Services
Business contact telephone number	778 974-3574
Indication of whether or not personal information is involved	Yes
Start date	April 2020

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative?

No new PIB will result from this initiative.

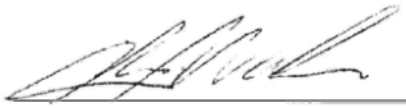
Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Oliver Jones	Oliver Jones	April 15, 2020
Senior Privacy Analyst Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Keleigh Annau	K. Annau	April 15, 2020
Director, Strategic Privacy, Policy and Training Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Karine Bordua		April 15, 2020
Ministry Privacy Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Chris Mah		April 20, 2020
A/Assistant Deputy Minister and Chief Information Officer Information Systems Branch Ministry of Attorney General	Signature	Date
Jess Gunnarson		April 21, 2020
Executive Director Security Programs Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date
Brenda Butterworth-Carr		April 23, 2020
Tr'injà shär njit dintlät Assistant Deputy Minister Policing and Security Branch Ministry of Public Safety and Solicitor General	Signature	Date

Appendix A: Consent Language under FoIPPA

A. Original Online Application

The following language will be included in the terms of use of the SPD portal:

"For the purpose of completing my Criminal Records Review Act (CRRA) check:

- *I hereby consent to the disclosure by the Ministry of Public Safety and Solicitor General to the Deputy Registrar of my names, alias, Correctional Service Number (CS#), history of contact with BC Corrections, and my date of birth found on the BC Corrections' client management software, CORNET.*

- *I hereby consent to the disclosure by the Deputy Registrar to the Criminal Records Review Unit of my names, alias, date of birth, gender, history of contact with BC Corrections CS#.*

- *I consent to the disclosure to the Deputy Registrar by Criminal Records Review Unit of any personal information relating to any outstanding charges or convictions for any relevant or specified offence(s) as defined under the Criminal Records Review Act or any police investigations, charges, or convictions deemed relevant by the Deputy Registrar.*

The disclosures take place within Canada. This consent is valid from the date signed."

B. Manual Application (i.e. paper form)

The following language will also be included in the paper forms:

"*I hereby authorize the indirect collection by the Deputy Registrar of my personal information from my organization for the purpose of completing my CRRA check*."

C. Sharing of a CRRA Check

Following information will be provided to applicant that are looking to share a previous CRRA check with a new agency:

"I understand that to share the result of a criminal record check, I must have completed a criminal record check within the last 5 years through the CRRP and the sharing request must be for the same type of check as previously completed, either for children, vulnerable adults, or both children and vulnerable adults.

I confirm I have completed a criminal record check within the past five years with the CRRP which did not result in a determination of risk to children and/or vulnerable adults as defined in the Criminal Records Review Act.

I understand no details will be disclosed to the organization I am applying to, only the result. I hereby consent to share the result of the completed check with the organization I am applying to.

I understand that if the registrar determines I do not have a criminal record check to share according to the above criteria, I will be promptly notified.

I understand that within 5 years of the date of this sharing form, should the CRRP make a determination that I pose a risk to children and/or vulnerable adults, the Deputy Registrar will promptly provide notification to me and to the persons and entities (organizations) identified on this sharing form.