



CORNET

ELECTRONIC ACCESS AGREEMENT

Ministry of Justice
Ministry of Children and Family Development

Read-only Electronic Access Agreement

BETWEEN: Her Majesty the Queen in right of the Province of British Columbia, as represented by the British Columbia Ministry of Justice, Corrections Branch, hereafter "CB" and the British Columbia Ministry of Children and Family Development, Youth Justice, hereafter "YJ"

AND: The British Columbia, Ministry of Justice, Security Programs Division, hereafter "SPD".

RE: Electronic access to data in the Corrections Network (hereafter "CORNET") in accordance with Appendix A.

1. Definitions

CB means the Corrections Branch of the Ministry of Justice.

CORNET User means any individual who is authorized to have electronic access to unsealed CORNET data pursuant to this EAA. For the purpose of the Security Programs Division, access to CORNET is granted via FIGARO as defined in section 7.b. of this agreement.

EAA means an electronic access agreement.

FIGARO means the electronic program that is used by SPD employees to retrieve unsealed CORNET data.

FOIPP Act means the Freedom of Information and Protection of Privacy Act, British Columbia.

ITSD means the Information Technology Services Division, Ministry of Justice.

Ministry means the Ministry of Justice.

MCFD means the Ministry of Children and Family Development.

Personal information means unsealed recorded information about an identifiable individual. [FOIPP Act, Schedule 1].

MoJ means the Ministry of Justice of the Province of British Columbia.

Read only access means that the party providing access allows the authorized party to access specific unsealed information in CORNET. The party accessing the information is permitted to read, print or save the information. No authority is provided to create, modify or delete information in CORNET.

SPD means the Security Programs Division of the Ministry of Justice.

SSU means a help desk provided by the Systems Services Unit of CB to assist CORNET users.

TMT means the Corrections Branch Technology Management Team.

Unsealed means recorded data about an identifiable individual that is not sealed according to provisions of the YCJA.

YCJA means Youth Criminal Justice Act (2002 c.1).

YJ means the Youth Justice Division of the Ministry of Children and Families.

2. Background to this Electronic Access Agreement (hereafter “EAA”)

CORNET is an operational integrated offender case management system. It is the provincial repository for all adult and youth Corrections’ offender files.

CORNET is used by CB and YJ for public safety purposes, law enforcement purposes, and the administration of the CB and YJ mandates. Through CORNET, information is shared with other justice agencies.

FIGARO is a licensing and regulatory system supporting several business areas for Security Programs. This program queries and retrieves specific personal information from CORNET. The Security Industry and Licensing Program under the Security Services Act (SSA), the Body Armour Control Act (BACA), the Armoured Vehicle and After-Market Compartment Control Act (AVAMCCA), the Criminal Records Review Program under the Criminal Records Review Act (CRRA), and the Personnel Security Screening Office (PSSO). The PSSO also facilitates criminal record checks for the Ministry of Children and Family Development (MCFD), for initiatives in which individuals are in a position of trust with children.

An electronic access agreement is a written agreement in a format set by the CORNET Electronic Access Policy, which authorizes electronic access to CORNET. Where applicable, it also acts as an Information Sharing Agreement (ISA) pursuant to section 69(5) of the Freedom of Information and Protection of Privacy Act.

This EAA details the authorized access to CORNET data by multiple programs areas within the Security Programs Division. These programs areas access CORNET for the purpose of security screening in accordance with the following mandates:

1. Body Armour Control Act;
2. Armoured Vehicle and After-Market Compartment Control Act;
3. Security Services Act;
4. Criminal Record Review Act (Program);
5. Personnel Security Screening Office;
6. Ministry of Children and Family Development, After-Hours checks

As the purpose for purpose of each of these security screening functions differ, purpose of access and mandate will be detailed for each of these program areas in appendices to this document.

3. Authority for Access

The electronic access described in this EAA is authorized pursuant to:

Authorization for Security Programs Division to Collect Information:

- Section 4(2) of the *Body Armour Control Act*
- Section 3(2) of the *Armoured Vehicle and After-Market Compartment Control Act*
- Section 3(3) of the *Security Services Act*
- Section 4(1) of the *Criminal Record Review Act*
- Section 96 (1) of the *Child Family and Community Services Act*
- Section 26(a) of the *Freedom of Information and Protection of Privacy Act* as per the above
- Section 26(c) *Freedom of Information and Protection of Privacy Act*
- Section 27(1)(a)(i) *Freedom of Information and Protection of Privacy Act*
- Section 27(1)(b) *Freedom of Information and Protection of Privacy Act.*

Authorization for Security Programs Division to Use Information:

- Section 32(a) *Freedom of Information Protection of Privacy Act*
- Section 32(b) *Freedom of Information Protection of Privacy Act*
- Section 32(c) *Freedom of Information Protection of Privacy Act.*

Authorization for CB to Disclose Information:

- Section 33.1(1)(b) *Freedom of Information and Protection of Privacy Act*
- Section 33.1(1)(c) *Freedom of Information and Protection of Privacy Act.*

4. Purpose of the Electronic Access

The purpose of access for each of the SPD program areas are elaborated in the appendices referenced below.

1. Body Armour Control Act - *Appendix B.*
2. Armoured Vehicle and After-Market Compartment Control Act - *Appendix C.*
3. Security Services Act - *Appendix D.*
4. Criminal Record Review Act (Program) - *Appendix E.*
5. Personnel Security Screening Office - *Appendix F.*

6. Ministry of Children and Family Development, After-Hours checks - *Appendix G.*

5. General Provisions

- a) SPD will establish and maintain policies and procedures to ensure that SPD's CORNET users comply with the terms and conditions of this EAA.
- b) SPD's CORNET users will have security screening, including a criminal record check, before accessing CORNET.
- c) CORNET Users' access privileges will be revoked when they no longer require access due to changes in employment duties or employment status.
- d) TMT will not grant access until SPD CORNET Users have completed and submitted an account authorization form and have completed training on CORNET. A copy of the account authorization form is included for reference in Appendix H. This form may be amended from time to time by CB.
- e) SPD CORNET Users will access CORNET only from an access point approved by TMT.
- f) SPD CORNET Users will be provided with read-only access.
- g) CORNET access is only to be used for SPD purposes. Information from CORNET is not to be provided to other provincial, national, or international agencies or persons unless authorized or required by law.
- h) The SPD is responsible for the collection, use, retention, and all subsequent disclosures of information obtained from CORNET in accordance with the Youth Criminal Justice Act and provincial Freedom of Information and Protection of Privacy legislation. If any concern exists with the lawful use or release of CORNET adult data, the SPD will contact the Corrections Branch's Director of Programs and Strategic Services. If any concern exists with the lawful use or release of CORNET youth data, the SPD will contact the Ministry of Children and Family Development, Youth Justice Policy & Program Support's Director.
- i) As per Appendix I, SPD will designate a central contact person who will be responsible for liaising with the CB for CORNET account authorization purposes and to maintain a list of those SPD employees assigned CORNET accounts.
- j) Authority to assign SPD accounts will be delegated to the Executive Director of Security Programs.
- k) The list of SPD employees with CORNET access will be provided to the chair of TMT upon request or at the end of every calendar year.
- l) The central contact person will provide CB with a sample of the authorizing signature that will appear on the Account Application form.

6. Information to be Accessed

TMT will provide access to the information listed in Appendix A as available in CORNET.

7. Method of Providing the Information

- a) Access to information is controlled by account security matrices.
- b) In the FIGARO database, an initial query to CORNET is automatically generated by FIGARO during service creation for a program applicant. Each program has a specific list of offenses which CORNET will reference when returning results. For each potential positive result, CORNET will return the name(s), date of birth, gender and CS number to FIGARO. Authorized CORNET users at SPD will type in the CS number in the CORNET pop up box to retrieve the associated client history report. The client history report for each CS number is compared with the information provided by the applicant via signed consent. Any CS numbers that prove not to be a match to an applicant are disregarded by the user. Once a CS number is provided by CORNET through a FIGARO query, authorized users are granted access to the associated file in CORNET for 30 days.

8. Information Accuracy

CB and YJ do not guarantee the accuracy of the information accessed under this EAA. This information is made available on an "as is" basis. CB and YJ will not be liable for any inaccuracies.

9. Liability

Information contained in CORNET may contain errors and is subject to change or modification, therefore; the Crown in right of the Province of BC or the Ministry, their contractors, or employees is not liable to any person or agency using the specified CORNET modules or information generated there from, for direct, indirect, general, special, or consequential damages including personal injury, lost profits, lost savings, interruption of business, or any other incidental damages arising out of the use of, or inability to use, the specified CORNET modules.

10. Training

- a) The participants agree that SPD will provide users with the necessary instruction and practice in accordance with the EAA before access is granted to CORNET data.
- b) Training will be conducted through the following method:
 - i. The CB and YJ Branch may provide initial train the trainer instruction on the specified CORNET modules to designated SPD trainers. SPD is responsible for subsequent training of SPD CORNET Users.
- c) SPD will maintain records of all users trained, including the dates of training sessions. Only individuals who have signed a user access form, received training on

the use of CORNET, and received a personal user ID account may access information as provided under this agreement.

11. Statement of Services

Technical Support

- a) SPD CORNET Users may request assistance from ITSD for problems relating to hardware, network connectivity and other problems related to hardware infrastructure.

User Support

- a) All inquiries for assistance from SPD employees will be forwarded to SPD's CORNET trainers. If necessary, the CORNET trainers will contact the Corrections Branch System Services unit.

12. Costs

- a) There is no financial cost to SPD for CORNET Data.
- b) SPD is responsible for all costs associated with providing and maintaining the technical infrastructure required to access CORNET Data, training costs, and user and technical support as agreed to between the parties.
- c) If costs arise to both parties as a result of changes to either FIGARO or CORNET, these costs will be discussed in advance and both parties will come to a mutually agreed upon resolution. If a resolution cannot be achieved, the issue will be referred to TMT.

13. Communication and Consultation

The participants agree that when a participant is considering changes to systems, policies or procedures which may affect access to information under this Agreement, the participant will provide reasonable notice to the other participant of any proposed changes and will establish a process for further consultation and communication which takes into account the operational requirements of both participants.

14. Copyright and Licence

SPD will not make copies of any CORNET software that is owned by or licensed to the Ministry, without the written consent of CB. Upon termination of this EAA, SPD will cease using all such software and have it removed from SPD computers.

15. Dispute Resolution

Once this EAA comes into effect, if a policy, legal or technical issue arises that cannot be resolved by the parties, the issue may be brought to TMT for review.

16. Modification

This EAA may be altered by agreement in writing from all parties and may be supplemented with an addendum.

17. Cancellation of this EAA

Either participant may terminate this EAA within 90 days by providing written notice to the other participant.

18. Non-Performance Due to Causes Outside the Control of the Parties

Notwithstanding anything herein to the contrary, none of the parties authorized under section 2 shall be deemed to have breached this EAA with respect to the performance of any of its terms, covenants, or conditions, if same shall be due to any strike, lockout, civil commotion, invasion, rebellion, hostilities, sabotage, governmental regulations or controls, or natural disaster.

19. Unauthorized Collection, Use, Disclosure, Access, Disposal, or Storage of information contained in CORNET (whether suspected or confirmed)

19.1 Response to unauthorized activity

If the Security Programs Division, including any employee, service provider, or other person discovers any of the following activities involving CORNET, whether suspected or confirmed, then this activity shall be reported immediately by the SPD to the Office of the Chief Information Officer (OCIO) in accordance with government policy. The SPD agrees to ensure that all SPD CORNET users are aware of their obligation to report unauthorized activity as prescribed here. The activities that must be reported to the OCIO include:

- Unauthorized access to or modification of the information provided under this Agreement whether it is suspected or confirmed;
- Unauthorized collection, use, disclosure, disposal, or storage of the information provided under this Agreement whether it is suspected or confirmed;
- Breaches or suspected breaches of security of the information provided under this Agreement or the computer system used to access such information.

Once the unauthorized activity has been reported to the OCIO, then SPD will advise the Corrections Branch's Director of Programs and Strategic Services of the unauthorized activity.

Notwithstanding any other provision of this Agreement, Corrections Branch may terminate access to information under this Agreement where information is accessed or used for a purpose not authorized under section 4 of this Agreement. Corrections Branch may terminate an individual user's access or the SPD's access as a whole.

19.2 Complaints about Information Practices

The SPD agrees to respond in a timely manner to complaints about the information practices set out in this agreement. In addition, the SPD will immediately notify the Office of the Chief Information Officer and the Corrections Branch's Director of Programs and Strategic Services of any complaints that relate to the inappropriate collection, use, disclosure, access, disposal, or storage of CORNET information. The Corrections Branch will, in turn, follow provincial government policy for the reporting of information incidents.

19.3 Auditing and Audit Trails

CORNET maintains an audit trail for all direct user access to CORNET, including both access that allows for data modification and read-only access. When FIGARO sends an automatic query to CORNET, no audit trail is maintained. However, whenever CORNET returns such a query, the information returned is maintained in FIGARO with a date stamp. This information can be utilized if necessary for audit purposes. The participants agree that audits of the SPD's access to CORNET may be conducted. Where Corrections Branch has determined that there has been inconsistent use the SPD will assist in resolving any arising concerns.

20. Term

This EAA will remain in effect unless replaced by another agreement or terminated.

21. Transferability

This EAA is neither transferable nor assignable.

22. Legal status of this EAA

Electronic access agreements are intended to facilitate co-operation and communication to the mutual benefit of each party and each party will exercise good faith to comply with the terms of the EAA. No party will commence an action on the basis that this EAA has been breached.

23. Contacts

Corrections Branch:

Bill Young

Director of Strategic Technology and Corporate Projects

(250) 356-7931

Marnie Mayhew

Director of Programs and Strategic Services

(250) 387-1562

Ministry of Children and Family Development:

Nerina Holderness

Youth Justice Project Consultant, Youth Justice

(250) 356-1962

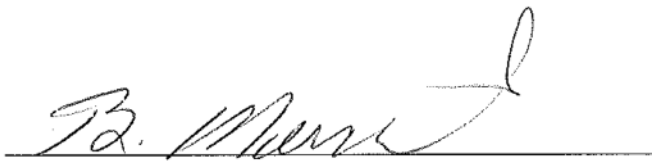
Security Programs Division:

Fraser Marshall

Director

(250) 356-1504

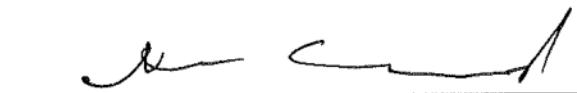
Dated at Victoria, British Columbia, this 18 day of APRIL, 2012.



Brent Merchant

Assistant Deputy Minister
Corrections Branch
Ministry of Justice

Dated at Victoria, British Columbia, this 4 day of May, 2012.



Alan Markwart

Senior Executive Director
Provincial Services
Ministry of Children and Family Development

Dated at Victoria, British Columbia, this 25 day of April, 2012.



Sam MacLeod

Executive Director
Policing, Security & Law Enforcement
Operations
Ministry of Justice

APPENDIX A

PERSONAL INFORMATION TO BE ACCESSED

Programs

SSA = Security Services Act

BACA = Body Armour Control Act

ACAMCCA = Armoured Vehicle and After-Market Compartment Control Act

CRRA = Criminal Records Review Act

PSSO= Personnel Security Screening Office

MCFD= Ministry of Children and Family Development

Program	User Role	Type of Access	Information Returned	# of Users	Name of person authorizing access
SSA	Client Service Clerk	FIGARO Query	List of All Offenses		
SSA - Risk Assessment	Risk Assessment Coordinator	Manual CS# Query	Client History		
BACA	Client Service Clerk	FIGARO Query	List of All Offenses		
BACA - Risk Assessment	Risk Assessment Coordinator	Manual CS# Query	Client History		
ACAMCCA	Client Service Clerk	FIGARO Query	List of All Offenses		
ACAMCCA - Risk Assessment	Risk Assessment Coordinator	Manual CS# Query	Client History		
CRRA	Client Service Clerk	FIGARO Query	Partial List of Offenses If a hit is found on the partial list of offenses, all offenses included in the file are returned.		

CRRRA - Risk Assessment	Risk Assessment Coordinator	Manual CS # Query	Client History		
MCFD	Client Service Clerk	FIGARO Query	List of All Offenses		
MCFD - Adjudication	Client Service Clerk	Manual CS # Query	Client History		
PSSO	Client Service Clerk	FIGARO Query	List of All Offenses		
PSSO - Adjudication	Risk Assessment Coordinator	Manual CS # Query	Client History		

APPENDIX B

Body Armour Control Act

The Body Armour Control Act (BACA) places controls on the possession or selling of body armour. Police have the authority to seize body armour that is illegally sold or possessed without a permit. As well, individuals without permits may face fines and incarceration. Businesses selling body armour without authorization can be heavily fined and their controlling members incarcerated for up to six months. Mandatory criminal record checks are conducted on permit applications. Signed consent to conduct a check is provided to Security Services from each applicant.

APPENDIX C

Armoured Vehicle and After-Market Compartment Control Act

The Armoured Vehicle and After-Market Control Act (AVAMCCA) has two purposes:

1. outlines who may operate an armoured vehicle in British Columbia, the application process to get a permit (if applicable), and the conditions placed on permitted operators.
2. outlines the prohibition of owning, operating or using a vehicle that contains a concealed compartment that was installed after leaving the manufacturer.

Mandatory criminal record checks are required by the AVAMCCA as part of the permit application process. Signed consent to conduct a check is provided to Security Services from each applicant.

APPENDIX D

Security Services Act

The Security Services Act (SSA) enhances public safety by ensuring consistent and appropriate standards across the security industry. Mandatory criminal record checks are conducted on all applicants to the security business as part of the licensing process. Signed consent to conduct a check is provided to Security Services from each applicant.

APPENDIX E

Criminal Records Review Act (Program)

The Purpose of the Criminal Records Review Act (CRRA) is to help protect children from individuals whose criminal records indicate they pose a risk of physical and sexual abuse and to protect vulnerable adults from physical, sexual or financial abuse. Mandatory criminal record checks are required by the legislation and the Criminal Records Review Program makes a determination of risk on each applicant. Consent in writing is received from each applicant to conduct the criminal record checks.

APPENDIX F

Personnel Security Screening Office

The Personnel Security Screening Office (PSSO) checks the history and background of successful applicants and current employees of the BC Public Service. Screening is mandatory for all designated positions in the B.C. Public Service. For most positions, screening consists of a criminal record check – a search for convictions, penalties or outstanding charges.

Under the PSSO, two types of security screening exist:

A) B.C. Public Service Criminal Record Check – required for all designated positions (**note: CORNET is not searched for this category of criminal record checks**)

B) Enhanced Security Screening – may include fingerprinting, professional/educational verification checks, credit/financial checks, and background investigations. (note: CORNET is searched for this category of criminal record check) This category of check requires a business case approved by the Deputy Minister's Committee.

APPENDIX G

Ministry of Children and Family Development, After-Hours

Ministry of Children & Family Development (MCFD) has a signed agreement with SPD to facilitate criminal record checks for the purpose of screening individuals entering into positions of trust with children in settings such as foster homes, adoptive homes, youth justice residences and out-of-care placements. Consent to conduct the criminal record check and review of findings is given by each applicant in writing. MCFD uses the response or summary findings supplied by SPD to assess suitability of an individual or other adult member of a household to be in positions of trust with children in settings described above.

APPENDIX H

Approving Authority Form



CORNET - Approving
Authority Form.pdf

Click on embedded file to access form

APPENDIX I

LIST OF AUTHORIZED USERS

The SPD contact to review and sign all CORNET access applications prior to submission and to maintain a list of all authorized CORNET users is:

s.15; s.17

The list of SPD staff identified at the time of this EAA who will apply for CORNET access will be maintained by the two Business Analysts of the Security Programs Division.



search

British Columbia Guideline for Police Information Checks

POLICE INFORMATION CHECK
POLICE INFORMATION CHECK WITH VULNERABLE SECTOR

Updated November 2016



Ministry of Public
Safety and
Solicitor General

Table of Contents

Introduction	1
1: Overview of Police Information Check Process	3
2: Types of Police Information Checks	5
3: Information Check Release Criteria	8
4: Vulnerable Sector CPIC Query	22
5: Self Declaration	26
6: PIP Police Information Portal	29
7: Refusal to Complete a Police Information Check and Exceptional Disclosure – Assessment and Authority to Disclose	30
8: B.C. Human Rights Considerations	36
9: Privacy Considerations	37
10: Reconsideration Process	39
Glossary	41
Appendix A: Records Check Release Chart	51
Appendix B: PRIME Role Codes	56
Appendix C: Applicant Fact Sheet	57
Appendix D: Organization/Employer Fact Sheet	62
Appendix E: Police Information Check & Police Information Check Vulnerable Sector Application, Waiver, Release and Consents	67

Introduction

The British Columbia Guide for Police Information Checks is intended to assist police agencies to understand and apply relevant legislation, policies, procedures and directives to the processing of Police Information Checks.

In June 2008, the BC Association of Chiefs of Police (BCACP) requested the Ministry of Public Safety and Solicitor General - Police Services convene a working group to review the Criminal/Police Information Check process in British Columbia. The mandate of this working group is to provide a consistent standard of completing Police Information Checks in British Columbia. This guide provides users with a detailed description of the databases that must be queried as well as how that information is disclosed, thus ensuring consistent processing, methodology, terminology and end product.

The working group consists of representatives from municipal police departments, Royal Canadian Mounted Police (RCMP), Ministry of Public Safety and Solicitor General, Police Services and PRIME-BC. In November 2010, the BCACP endorsed the recommendations of this working group and changes to policy and procedure were implemented in the Spring of 2012. In 2014, as a result of recommendations from the Office of the Information and Privacy Commissioner's (OIPC) report on police record checks, the BCACP approved additional policy changes contained in this document.

The working group will continue to conduct quarterly reviews of the Police Information Check processes in an effort to stay abreast of national and provincial policies. These meetings will also be a venue to review and discuss user feedback.

This Guide does not address the role of third party, for profit and not for profit companies. For further information refer to the RCMP Policy at RCMP.ca.

This guideline incorporates provisions of the:

- ↑ *Criminal Records Act*
- ↑ CPIC Policy and User Manual
- ↑ Freedom of Information and Protection of Privacy Act (FOIPPA)
- ↑ Personal Information Protection Act (PIPA)
- ↑ *Youth Criminal Justice Act*
- ↑ Ministerial Directive on the Release of Criminal Records (2010)
- ↑ PRIME-BC (Police Records Information Management Environment) Policy
- ↑ PIP (Police Information Portal) Policy

In preparing this guideline, the Committee consulted with the following organizations:

- ↑ Canadian Criminal Real Time Identification Services (CCRTIS)
- ↑ BC Office of the Information and Privacy Commissioner
- ↑ BC Police Records Users Group
- ↑ PRIME-BC
- ↑ Law Enforcement & Records Managers Network (LEARN) Committee

Working Group Members

Fraser Marshall (Chairperson)	Director, Security Services, Policing and Security Branch Ministry of Public Safety and Solicitor General
Dennis Verge (Chairperson)	Police Services, Public Safety and Solicitor General (retired)
Cpl. Dean Allchin	RCMP - Operational Policy Unit, E Division Headquarters
Peter Ditchfield	Manager of Police Services, Port Moody PD (retired)
Kyle Friesen	Counsel, Legal Advisory Section (RCMP Pacific Region), Department of Justice Canada
Denise Girvin	Criminal Records Specialist, Victoria PD
Lisa Heron	Civilian Staff Manager, New Westminster PS
Lisa Hoogstins	Manager, Information Management Section, Vancouver PD
S/Sgt. Ab Humayun	Policy and Audit, PRIME-BC
Laura Jacob	Information & Privacy Coordinator, Delta PD
Elaine Klassen	Manager, Records Information, Abbotsford PD
Cpl. Michelle Lakusta	RCMP - CPIC Field Operations BC/YT
Dawna Marshall-Cope	Senior Director, Information Management Section, Vancouver PD
S/Sgt. Mike Nedzelski	Administration Division, Saanich PD (retired)
S/Sgt. Trish Pinkewycz	RCMP - Manager CPIC Field Operations BC/YT
Julia Trasler	Human Resources & Admin Manager, Delta PD
Cpl. Matt Dawson	Supervisor, Information Services Unit, West Vancouver PD
Volker Helmuth	Manager, Information Services Section, Delta PD

1 Overview of Police Information Check Process

- 1) It should be noted that this is not a Criminal Record Check. It is a Police Information Check. It is a comprehensive check by name and date of birth of a local police agency's records management system, queries of the CPIC Identification, Investigative and Intelligence databanks. The query may also include a search of court records and a query of records management systems in other police jurisdictions. To assist applicants and hiring agencies, police agencies should only use the terms: Police Information Check (PIC) and Police Information Check – Vulnerable Sector (PIC-VS) when following the direction of this guideline.
- 2) All applicants are required to present two pieces of valid, government issued identification – one must have a photo.
- 3) In order to ensure consistency and to maintain a required level of due diligence the following systems must be queried, upon completion of a signed consent:
 1. CPIC – Q Pers(ons)
 2. CPIC – CNI (with VS if required and signed consent completed)
 3. CPIC – FIP
 4. PRIME Local indices (see note below)
 5. PIP
 6. PROS (if available)
 7. JUSTIN (consent from court or police agencies not required to release)

It is also required that addresses of residence for the past 5 years be obtained. A CPIC Narrative Message must be sent to each agency of past residence that is outside of BC requesting that a local indices check be completed.

These are minimum standards and the use of any other available systems is at the discretion of the agency conducting the Police Information Check. You must have the authority to use such systems and they must be noted in the signed, informed consent on the Police Information Check document.

NOTE: if a hit is received on PRIME you must follow PRIME BC Policy Chapter 5.2 – Ownership of Records which states "Participating Agencies shall neither confirm the existence of information, nor disclose information created by an Originating Agency to third parties without the written permission of the Originating Agency."

- 4) If the police agency finds any adverse information, complete the appropriate results section of the form. If there is pertinent information it will be attached. Information found on any of the above listed databases may be released subject to the guidelines in this policy, which are summarized in Appendix A. It is only necessary to indicate a particular incident once on the release document, although it is likely that a single incident will be found on more than one data base. For example, a conviction from a CPIC Criminal Record should be released as a conviction only, it is not necessary to repeat information in local information, i.e., a conviction on CPIC CRII should be released as a conviction only, it is not necessary to repeat information in local police information. Otherwise a reader may believe that there may be several instances when in fact there is only one.

- 5) If the applicant has non-pardoned criminal convictions they may complete the "Declaration of a Criminal Record" form and the police agency will verify the accuracy of the declaration and this will become part of the completed record check. This may avoid the fingerprinting requirement.
- 6) A Police Information Check will not contain information related to traffic violations or municipal by-laws. It may contain provincial offences.
- 7) Record suspension (Pardoned) records and certain youth records will not be noted on this record check except for record suspension (Pardoned) sexual offences relating to a vulnerable sector inquiry. (see Vulnerable Sector Searches)
- 8) Absolute and conditional discharges that have not met their non-disclosure date will be noted on this check. The purge criteria for these types of sentences is as follows:

Absolute Discharges – 1 year from the date of discharge
Conditional Discharges – 3 years from date of discharge
- 9) The police agency will **not** give the result of a Police Information Check to anyone but the applicant, even with consent, with the exception of disclosed VS hits released by the Minister of Public Safety.
- 10) Local police files are subject to PRIME retention schedules regardless of whether these files are visible on PRIME past their retention.
- 11) Youth records will only be disclosed according to the *Youth Criminal Justice Act* (YCJA). Non-disclosure dates set out in the YCJA must be used.
- 12) If the applicant will be working in a position responsible for "vulnerable persons" (children, disabled, senior citizens, etc.) a Form I consent must be completed. This gives permission to the police agency to check for any sexual offences for which a record suspension was received. The applicant may be required to submit fingerprints to the RCMP Ottawa prior to the police department completing the Police Information Check. If police receive information that a record suspension for a sexual offence has been received, the applicant will be required to sign Form 2 consent to allow the information to be released to the employer/agency.
- 13) The police agency will provide the results of the search and will not be responsible for determining relevance to any proposed employment or volunteer position. This determination must be made by the employer or volunteer organization through its own background investigation and in accordance with human rights legislation and employment law.
- 14) The Police Agency will emboss, with a seal, each page of the completed Police Information Check.
- 15) The police agency has the right to discontinue or deny a request for a Police Information Check.

****Fact Sheets for Applicants and Employers is
located in the appendices to this guide****

2 Types of Police Information Checks

British Columbia police agencies offer two types of Police Information Checks: Police Information Check (PIC), and Police Information Check with Vulnerable Sector Screening (PIC-VS). If an organization determines that a check for convictions only is required, this information can be obtained by submitting fingerprints to CCRTIS, either through the RCMP or an accredited private company.

A search of only convictions is not offered by BC police agencies because of the significant delay of charge and conviction information being entered into the National Repository for Criminal Records and CPIC.

For more information please see www.rcmp.ca

1. Police Information Check (PIC)

It is a collection of offence information, including convictions, outstanding warrants, charges and judicial orders available from a local police agency's records management system and other systems/records where authorized.

This check is intended for applicants who are seeking volunteer and/or employment with agencies who require a criminal record check. The agency has determined that a search of sex offenders with a record suspension is NOT required (e.g., border crossing or visa) therefore this check is NOT intended for applicants who are seeking volunteer and/or employment with vulnerable persons.

The Police Information Check will include the following information (refer to Self Declaration requirements and Record Check Release Chart):

NOTE: See section on Verification of a Criminal Record

- a) Criminal convictions from CPIC, local police databases or JUSTIN.
- b) Summary convictions.
- c) Findings of Guilt under the Youth Criminal Justice Act within the applicable disclosure period.
- d) Outstanding entries, such as charges and warrants, judicial orders, Peace Bonds, Probation and Prohibition Orders. As per CPIC policy, information obtained from the Investigative Databank must be confirmed and authorized for release by the contributing agency.
- e) Absolute and conditional discharges for 1 or 3 years respectively.

The Police Information Check WILL NOT include:

- a) Convictions where a record suspension has been granted.
- b) Convictions under provincial statutes.
- c) Local, adverse police contact.
- d) Traffic violations, including roadside suspensions.
- e) Special Interest Police (SIP) category of CPIC.

- f) Family Court restraining orders.
- g) Foreign information.
- h) A Vulnerable Sector (VS) Query to ascertain if the applicant has been convicted of and granted a record suspension for any of the sexual offences that are listed in the schedule to the Criminal Records Act (CRA).
- i) Any reference to incidents involving mental health contact.
- j) Diversions will not be released as police contact and no reference to the occurrence is permitted (CCS.717.4).
- k) *Youth Criminal Justice Act* (YCJA) information beyond applicable disclosure period.
- l) Any reference to contagious diseases.
- m) Dispositions including, but not limited to, Stay of Proceedings, Withdrawn, Dismissed, Not Criminally Responsible by Reason of Mental Disorder, Acquittals and Not Guilty findings.

2. **Police Information Check with Vulnerable Sector Screening (PIC-VS)**

This check is restricted to applicants seeking employment and/or volunteering in positions responsible for vulnerable individuals. This product is a collection of offence information, including convictions, outstanding warrants, charges, judicial orders, non-convictions and adverse police contact information available from a local police agency's records management system and other systems/records where authorized. This check will include sexual offence convictions for which the individual has received a record suspension, subject to authorization by the Minister of Public Safety and Emergency Preparedness.

The Police Information Check with Vulnerable Sector Screening (PIC-VS) will include the following information (refer to Self-Declaration requirements and Record Check Release Chart):

- a) Criminal convictions (summary and indictable) from CPIC, local databases or JUSTIN, and findings of guilt within the YCJA non-disclosure schedule.
- b) Outstanding judicial orders, such as charges and warrants, judicial orders, Peace Bonds, Probation and Prohibition Orders. As per CPIC policy, information obtained from the Investigative Databank must be confirmed and authorized for release by the contributing agency.
- c) Absolute and conditional discharges for 1 or 3 years respectively.
- d) Charges recommended and/or processed by other means such as Diversion or Alternative Measures.
- e) Dispositions listed in the CPIC Identification Databank or CRII under non-convictions including, but not limited to, withdrawn, dismissed, and cases of not criminally responsible by reason of mental disorder.

- f) Any additional information recorded in police databases documenting the applicant to have been a suspect in an offence (whether or not charged), subject to provincial retention periods specific to the offence type.
- g) Adverse contact involving the threat or actual use of violence directed at other individuals and oneself that places others at risk regardless of, but without disclosing, mental health status (e.g., uttering threats, assault, etc.).
- h) As authorized for release by the Minister of Public Safety all record suspension (pardoned) criminal convictions, including non sex offences, identified as a result of a VSquery.

The Police Information Check with Vulnerable Sector Screening (PIC-VS) WILL NOT include:

- a) Convictions where a record suspension has been granted (except for sexual offences).
- b) Apprehensions under s. 28 of the *Mental Health Act*, or suicide threats or attempts where there was no harm or threat to others (e.g., no 'subject of threat or harm to others').
- c) Convictions under federal and provincial statutes unless under exceptional circumstances.
- d) Traffic violations, including roadside suspensions.
- e) Suspect information that would hinder an ongoing investigation or where the suspect has not been spoken to may result in the record check being delayed or terminated.
- f) *Youth Criminal Justice Act* (YCJA) information beyond applicable disclosure period.
- g) Special Interest Police (SIP) category of CPIC.
- h) Information gathered outside formal occurrence reports (i.e. street checks, CAD) except under exceptional circumstances.
- i) Any reference to contagious diseases.
- j) Victim/Complainant information unless under exceptional circumstances.
- k) Information from foreign law enforcement systems.

3 Information Check Release Criteria

1. Outstanding Criminal Charges & Warrants (CPIC, PRIME, JUSTIN)

A query of the Investigative Databank of the Canadian Police Information Centre (CPIC) must be conducted for PIC and PIC-VS to identify outstanding criminal charges and warrants held by any Canadian police agency.

As per CPIC Policy (Sec 8.3) and PRIME Policy (5.2), hit confirmation **MUST** be conducted on all hits and permission to include the information on a PIC or PIC-VS must be obtained from the originator.

In Section 8.3, Release of Investigative and Ancillary Databank Information, the CPIC Reference Manual states:

CPIC Information from the Investigative Data Bank may be released for security and reliability clearances or for private employment purposes; however, no CPIC information should be released for this purpose unless:

1. confirmation and verification with the record owner (originating agency) has been carried out; and,
2. the originating agency has been notified of the reason for the check and has consented to the release; and,
3. personal visual identification by the law enforcement agency of the subject of the check has taken place; and,
4. the results of the checks are communicated directly to the subject of the check. The applicable information may be released verbally or in writing; however, printouts should not be released.

A query of JUSTIN will also be conducted and may identify outstanding criminal charges and/or warrants held by any BC police agency. The information located in JUSTIN is available to the public. Police agencies are not required to have consent to release this information on a PIC or PIC-VS unless JUSTIN indicates there is a publication ban in place.

2. Current Judicial Orders (CPIC, PRIME, JUSTIN)

A query of the Investigative Databank of CPIC (QPERS) should be conducted, for a PIC or PIC-VS to identify any current Judicial Orders (e.g., Firearm Prohibition Orders, Probation Orders, Prohibition Orders, Peace Bonds, etc.) held by any Canadian police agency.

As per the CPIC Policy (Sec 8.3) and PRIME Policy (5.2), hit confirmation **MUST** be conducted on all hits and permission to include the information on a PIC or PIC-VS must be obtained from the originator.

Queries of PRIME and JUSTIN must also be conducted and may reflect current judicial orders not presently on CPIC. Permission to include this information must adhere to PRIME Policy 5.2 – Ownership of Records.

If the information is confirmed in the court system (JUSTIN), you do not require permission from the police agency.

3. Local Police Involvement (PRIME, PIP, PROS)

When processing a PIC or PIC-VS, records management system (RMS) databases should be reviewed to identify if the applicant has had any adverse contact with police. Contact may include events relating to, but not limited to, theft, weapons, sex offences, violent, harmful or threatening behavior which may or may not have involved a mental health incident. Involvement roles to review may include: Arrested, Accused, Charged, Wanted, Suspect/Chargeable, Charges Recommended and Suspect. (See Appendix B – PRIME Role Codes)

The applicant must be in an adverse role of a *bona-fide substantiated* investigation. Allegations where the applicant has no knowledge of the file will not be released/disclosed.

Information may be released on a PIC-VS until it has met its retention date. Retention periods commence on the clearance date of the file, i.e., not date of the offence. Consideration of significant events for applicants requesting a PIC only should follow your police agency guidelines. As a tool, your police agency may want to review Section 7 - Exceptional Disclosure Assessment for assistance.

Traffic violations, municipal bylaw offences and incidents that are unsubstantiated or incidents where the applicant is unaware of the allegations/occurrence may not be released.

Adverse police contact may include summary conviction offences. These are criminal offences where there is no requirement under the Criminal Code for fingerprints to be taken and as such, neither the offence nor the disposition will appear in the Identification Databank of CPIC.

The role codes Subject of Complaint (SOC) and Other (OTH) are non-accusatory and should NOT be released unless there are exceptional circumstances, e.g., where there is a demonstrated risk to the vulnerable sector. It is recommended that files with this role code, especially for serious offences, be reviewed to insure proper use of role codes.

Victim and complainant information should NOT be released unless there are exceptional circumstances where there is a demonstrated risk to the vulnerable sector, e.g., a pattern of domestic violence in a home daycare situation.

Role Codes of Witness should NOT be released.

Generally speaking, street checks and computer aided dispatch (CAD) incidents where there is no formal report generated should NOT be included, unless there are exceptional circumstances e.g., where there is a demonstrated risk to the vulnerable sector.

If the police agency intends to release information under exceptional circumstances, it is recommended that the file be approved by a person in authority (e.g. Inspector, Manager) who is not conducting the initial PIC or PIC-VS.

Intelligence file may only be released with the consent of the investigating officer. If the information is not to be released, consideration should be given to possibly discontinuing the record check. (See "Refusal to Complete a PIC".)

Youth:

Where a criminal occurrence has been cleared by way of an Extrajudicial Measure, i.e. by warning, caution, referral or no further action, the information may not be released.

*Note: Extrajudicial Sanctions are a unique form of Extrajudicial Measures and may be disclosed in a VS PIC until their non-disclosure diary date has been met per section 119(2)(a) YCJA.

Requesting the release of information from other agencies

When you have received a hit on local police information regarding the applicant and the information was contributed by another agency, you may not release it to anyone without the written consent of that agency. (PRIME Policy 5.2 – Ownership of Records)

Forward an email, v-mail, fax or CPIC message request to the contributing agency advising that your check of police record systems led you to a positive hit on your applicant pertaining to their file number. Before releasing the information to the applicant, permission to do so must be granted.

If permission is received, keep a copy of the reply on the file and continue with the Police Information Check by completing the appropriate section and disclosing the nature of the event.

If permission is denied and a valid reason under the guidelines (e.g., retention date or role code) has been given, do not note the file but keep a copy of the reply on file to indicate the request was made. If you have read the file and believe it should have been noted on the completed check you may wish to follow up with agency for clarification. However if you feel this should have been noted and permission is denied, you may discontinue the Police Information Check. (See Refusal to Complete PIC section below)

****When requesting permission to disclose keep in mind that if it was your agency's file and you would not disclose it as per the Provincial guideline – there is no requirement to request permission****

Receiving a request to release information from your agency's files

When you have received a written request from another Police Agency asking permission to release information regarding an applicant it is important to review each file.

Ensure that releasing the information will not jeopardize an ongoing investigation, fits the requirements for such a release, and the file reflects the proper scoring.

If the file meets the requirements for release, respond to the agency granting permission. Note on your file that this was released and keep copies of all communications.

If the file does not meet the requirements, respond to the requesting agency advising them not to release and the reason for this. Keep copies of this communication.

Refusal to Complete a PIC

In some instances PIC service must be denied or refused; however, *caution* should be used in making the decision to refuse service. Please review the Refusal to complete a Police Information Check and Exceptional Disclosure Assessment and Authority to Disclose section of this guide.

In the event of an *ongoing investigation* suspect information should NOT be released when it may hinder the investigation and/or the suspect has not yet been spoken to by police. The investigator(s) should be contacted to confirm whether to disclose or to suspend/terminate the Police Information Check process. Police agencies retain the right to terminate the Police Information Check process, without explanation if information of concern exists within PRIME, PIP or other records management systems that cannot be disclosed. Issuing a refund in such instances is left to the discretion of each police agency.

The following statement will be given when refusing to complete a check:

“Our agency has adopted the provincial Police Information Check standards. We are not obliged to provide this service. In this instance we decline to provide you with a Police Information Check.”

Do not reveal the reason why nor direct them to any other agency for information or explanation.

4. Mental Health Occurrences

A query of local records should be conducted for PIC-VS applicants but will only include information involving the threat or actual use of violence directed at other individuals, regardless of, but without disclosing, mental health status.

If a determination is made to release the information, only the substantive incident type should be released. (e.g., Suspect, Possession of a Dangerous Weapon, assault, uttering threats, etc.)

5. Information from other Police Agencies (PIP query, FIP Query, CPIC narrative message)

The applicant must provide a five-year address history. Contact must be made with each police agency having jurisdiction over previous addresses to request a search for any adverse police contacts as well as permission to release any information provided. This information should be released on a PIC-VS.

NOTE: Canadian Police Agencies do not have authority to conduct checks with law enforcement agencies outside of Canada.

A query of the Police Information Portal (PIP) database must be conducted as a National Query through PRIME. A PIP query is a tool to identify local police files held by other police agencies. Hit confirmation **MUST** be conducted on all hits and permission to include the information on a PIC or PIC-VS must be obtained from the originator. (See PIP section)

If you are unable to conduct checks with police agencies outside of BC, a notation must be made on the completed PIC that indicates which checks were not completed.

A query of the Firearms Interest Police (FIP) databank may be done through a Canadian Police Information Centre (CPIC) query. A FIP query is used only as a tool to identify reports held by other police agencies. The FIP entry itself must never be disclosed on a completed PIC or PIC-VS. Hit confirmation MUST be conducted on all hits and permission to include the agencies file information (not the FIP entry) on a PIC or PIC-VS must be obtained from the originator.

6. Special Interest Police (SIP) (CPIC)

A query of the Canadian Police Information Centre (CPIC) Investigative Databank may reveal a Special Interest Police (SIP) hit. This information may be used only as a tool to identify reports held by a police agency. Hit confirmation MUST be conducted on all hits and permission to include the relating information (not the SIP entry) on a PIC or PIC-VS must be obtained from the originator.

NOTE: When foreign information is entered in the SIP category (e.g., foreign warrants) the information must not be included on any level of Police Information Checks, as per Section 3.1 of the Interpol Charter.

7. BC Motor Vehicle Branch, Police Automated Registration Information System (PARIS)

PARIS information must not be disclosed for any level of Police Information Checks. Driver's abstract information is available through the BC Motor Vehicle Branch.

8. Interpol/NCIC

A police agency is not permitted to access the data bank of the National Crime Information Centre (NCIC) or the Interpol I-24/7 system when conducting a PIC or PIC-VS. (S.12.5 CCRTIS Dissemination of Criminal Record Information)

9. Dispositions (CPIC CNI/CR, PRIME, JUSTIN)

A query of the Identification Databank of CPIC must be conducted to identify court dispositions (e.g., convictions, suspended sentence, and conditional discharge). These queries are generally referred to as a CNI and a CRII. Dispositions may also be found within local police databases.

NOTE: When foreign dispositions are included on a CRII they must not be included on any level of Police Information Checks as per Section 3.1 of the INTERPOL Charter. The exception is entries on the conviction part of the CRII identified as international transfer of offenders may be disclosed.

Information may only be released from the Identification (CR/CNI) Databank through fingerprint confirmation or if the police agency is satisfied the applicant's self-declaration matches the information from the CRII (see Self-Declaration section).

Information relating to summary conviction offences for which fingerprints were not taken will only be available through local police databases and court systems (JUSTIN). Where available, this information should be included on a PIC or PIC-VS. If this information originates with another police agency, confirmation and permission to release must be obtained. If the information is confirmed in the court system (JUSTIN), you do not require permission from the police agency.

Querying the Firearms Interest Police (FIP) database, the Police Information Portal (PIP), JUSTIN and your local police databases may also reveal criminal dispositions.

When information obtained from the Identification Databank is being released on any level of Police Information Checks, without having the applicant submit fingerprints, the following caution must be included:

CAUTION: Based solely on the name(s) and date of birth provided and the criminal record information declared by the applicant, a search of the RCMP National Repository of Criminal Records has resulted in a POSSIBLE match to a registered a criminal record. Positive identification that a criminal record does or does not exist at the RCMP National Repository of Criminal Records can only be confirmed by FINGERPRINT comparison. As such, the criminal record information declared by the applicant does NOT constitute a Certified Criminal Record by the RCMP. Delays exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records.

10. Convictions, Suspended Sentence or Finding of Guilt (CPIC CNI/CRII, JUSTIN, PRIME)

Criminal convictions, Suspended Sentence or findings of guilt that are included on the CPIC CRII, PRIME or JUSTIN should be released on the PIC or PIC-VS.

Information may only be released from the Identification Databank through the submission of fingerprints or if the police agency is satisfied the applicant's self-declaration matches the information from the CRII (see Self-Declaration section) or confirmation can be made through your local police databases.

If the applicant's self-declaration does not match the information found on the CRII the applicant must submit fingerprints. Dispositions may be released from your local police databases, if you are satisfied with the identity of the applicant.

When information relating to these dispositions does not appear on the CRII, the relating information should be released from your local police database or JUSTIN as additional court information. If the information is confirmed in the court system (JUSTIN), you do not require permission from the police agency.

Youth:

Criminal dispositions may not be self-declared by a young person and therefore any information identified by way of a CRII query may not be included on a PIC or PIC-VS; however, if the information is confirmed through your own local database, the information may be released on a PIC or PIC-VS as follows:

If a young person has been found guilty of a summary offence, the information should be released from your own local database on a PIC or PIC-VS for a period of three years after the youth sentence has been completed.

See Section 119 (2) (g) of the YCJA.

If a young person has been found guilty of an indictable offence, the information should be released from your own local database on a PIC or PIC-VS for a period of five years after the youth sentence has been completed.

See Section 119(2) (h) of the YCJA.

NOTE: If the young person is subsequently charged with committing another criminal offence, during the disclosure period of a preceding offence, the disclosure period automatically becomes whichever retention period is the lengthier (S.119(2)(i) YCJA). Additionally, if the subject is convicted of a criminal offence as an adult during the disclosure period of any previous charges under the YCJA, the youth record becomes a part of a permanent adult record. (S. 115 YCJA.)

11. Acquittal / Not Guilty

An Acquittal or finding of Not Guilty is a non-conviction disposition rendered by a judge. Non-convictions do not meet the self-declaration qualifications for CRII, however information can be released from local police database until retention date is met for applicants who require a PIC-VS.

Adult:

Information relating to these court dispositions should be released on a PIC-VS. If an appeal has been launched, the relating CPIC entry reverts back to an Accused entry within the Investigative Databank and may be released on a PIC or PIC-VS with the confirmation and permission of the originating agency (the onus is on the releasing agency to confirm if an appeal has been launched).

Youth:

If a young person is Acquitted of an offence other than by reason of Not Criminally Responsible, the information should be released on a PIC or PIC-VS for a period of two months following the 30 day appeal period or, if an appeal is taken, the period ending three months after all proceedings of the appeal have been completed. The information should not be included on a PCRC.

See Section 119 (2) (b) of the YCJA.

12. Not Criminally Responsible (NCR)

Adult:

CPIC entries relating to an applicant who has been found Not Guilty by Reason of Insanity (prior to February 1992) or Not Criminally Responsible on Account of a Mental Disorder (after February 1992), and is awaiting disposition from a Review Board, will be found in the CPIC Investigative Databank under the Accused category. Once confirmed by the originating agency and permission to release is granted, this information should be released on a PIC- VS; as a non-conviction or adverse local police contact.

Youth:

The only reference to disposition of Not Criminally Responsible within the YCJA can be found in Section 119(2) (b) which states:

“The period of access referred to in subsection (1) is: if the young person is acquitted of the offence otherwise than by reason of a verdict of not criminally responsible on account of mental disorder, the period ending two months after the expiry of the time allowed for the taking of an appeal or, if an appeal is taken, the period ending three months after all proceedings in respect of the appeal have been completed”.

The YCJA is silent on a period of access for dispositions of NCR. Without a specified period of access restriction, the information could be accessed at any time by the youth/counsel. As a result, and as the information would only be provided to the applicant (youth), the NCR disposition should be released on a PIC or PIC-VS.

13. Absolute or Conditional Discharges (except by BC Review Board relating to Not Criminally Responsible)

In accordance with Prime-BC policy, Section 8.4:

The *Criminal Records Act* (s. 6.1(1)) prohibits the disclosure, to any person, of a record of a discharge under section 730 of the Criminal Code of Canada, the existence of the record, and the fact of the discharge:

- a) in the case of an absolute discharge, after one year from the granting of the discharge;
- b) in the case of a conditional discharge, after three years from finding of guilt; and
- c) in any other case, only upon approval of the Solicitor General of Canada.

ABSOLUTE OR CONDITIONAL DISCHARGES PRIOR TO JULY 24, 1992 MAY NOT BE PURGED FROM CPIC BUT SHOULD NOT BE RELEASED AS CRII OR LOCAL POLICE FILE INFORMATION

Absolute or Conditional Discharges after July 24, 1992

Adult:

Dispositions of Absolute or Conditional Discharge issued after July 24, 1992 should NOT be released on a PIC or PIC-VS as CRII information. These dispositions do not meet the self-declaration qualifications and therefore should not be released from the CRII, however, the relating information may be released from your own local files up to the end of the disclosure period.

Youth:

Dispositions of Absolute or Conditional Discharge do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the information may be released from local files on a PIC or PIC-VS as follows: Absolute Discharge for one year after finding of guilt, Conditional Discharge for 3 years after finding of guilt. See Section 119 (2) (c) of the YCJA.

14. Dismissed

Adult:

Dispositions of Dismissed do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the relating information may be released on a PIC-VS from local police files until the retention date is met.

Youth:

Dispositions of Dismissed do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the information may be released for two months after the disposition date from your own local files on a PIC or PIC-VS. After two months, no information should be released. See Section 119 (2) (c) of the YCJA.

15. Finding of Guilt with Reprimand (Youth only)

Youth:

A Finding of Guilt with a Reprimand does not meet the self-declaration qualification and therefore should not be released from the CRII; however, the information may be released for 2 months after the disposition date from your own local files on a PIC- VS.

See Section 119 (2) (c) of the YCJA.

16. Stays of Proceedings

Adult:

Stays of Proceedings do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the relating information may be released on a PIC-VS, from local police files until the retention period is met.

Youth:

Stays of Proceedings do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the information may be released for one year after the disposition date from your own local files on a PIC-VS. After one year, no information should be released. See Section 119 (2) (d) of the YCJA.

17. Withdrawn

Adult:

Dispositions of Withdrawn do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the relating information may be released on a PIC-VS from local police files until retention date is met.

Youth:

Dispositions of Withdrawn do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the information may be released for two months after the disposition date from your own local files on a PIC-VS. After two months, no information should be released. See Section 119 (2) (c) of the YCJA.

18. Peace Bond

Adult:

A Peace Bond does not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the information may be released on a PIC- VS from local police files until retention has been met.

While the Peace Bond is in effect, that information should be released on a PIC and a PIC-VS as a current judicial/disposition order. Thereafter, the relating information may be released on a PIC-VS, from local police files until the retention period is met.

Youth:

The Peace Bond is not protected by the YCJA and may be released from local police files until the retention period is met. While the Peace Bond is in effect, the information should be released on a PIC or a PIC-VS as a current judicial order.

19. Diversion (Alternative Measures) (Adult)

Adult:

Information relating to charges dealt with by way of Diversion or Alternative Measures should only be released on a PIC- VS as police contact information from local police files until retention has been met, with no reference to the court disposition. See Section 717.4 of the CCC.

20. Diversion (Youth only)

Youth:

Dispositions of Withdrawn – Diversion should NOT be released on a PIC or PIC-VS.

21. Extrajudicial Sanction (Youth only)

Youth:

Extrajudicial Sanctions do not meet the self-declaration qualifications and therefore should not be released from the CRII; however, the information may be released from your own local files on a PIC-VS for two years after the youth consents to the sanction. See Section 119 (2) (a) of the YCJA.

22. Extrajudicial Measures (Youth only)

Youth:

Extrajudicial Measures refers to actions other than judicial proceedings under the Youth Criminal Justice Act. See Section 2(1) of the YCJA.

Extrajudicial Measures include:

- no further action
- warning
- police caution
- Crown caution (post-charge the Crown may establish caution program)
- referral to community program or agency with consent of young person.

Where an occurrence was dealt with by way of an Extrajudicial Measure, including “no further action”, the information must not be included on a PIC or PIC-VS. See Section 9 of the YCJA.

NOTE: *Extrajudicial Measures can ONLY be used by police for NON-VIOLENT OFFENCES. Any incident related police contact information for violent offences (e.g., sexual assault) should be considered for release on a PIC- VS.*

23. Record Suspensions (formerly known as Pardons)

Unless written permission has been granted by the Minister of Public Safety, information relating to an offence and its disposition, for which a Pardon has been granted, should not be released on a PIC or PIC-VS. (See Pardons – Sexual Offences.)

24. Record Suspensions (formerly known as Pardons) – Sexual Offences (Bill C7, Criminal Records Act 2000)

As a result of Bill C7, passed on August 1, 2000, the CRA was amended to permit the flagging of record suspensions (pardoned) sex offenders. CPIC system changes were made to permit CPIC

agencies with law enforcement authority (Category I Agencies) to conduct queries using the CNI format screen and the "VS" keyword (Vulnerable Sector). This query searches the CPIC system for any flagged pardoned sex offenders for the purpose of conducting any level of Police Information Checks for persons wanting to work or volunteer in a position of authority or trust with the vulnerable sector.

Employers and/or volunteer organizations are responsible for advising the police agency when a "VS" query is required. Police should not make this determination; however, they must satisfy themselves in some manner that the position being applied for is one that will be dealing with the vulnerable sector as defined in the CRA.

See Section 4 - Vulnerable Sector CPIC Query.

25. Prohibition Orders (Criminal Code)

Prohibition orders will be identified through a query of the CPIC Investigative Databank, and include Criminal Code Prohibition Orders specific to liquor, firearms, vehicle/driving (and boat operation) or hunting, and any other court or statute-imposed prohibition such as, for example, under the *Aeronautics Act*.

While the Prohibition Order is in effect, that information should be released on a PIC and a PIC-VS as a current Prohibition Order.

Once confirmed and permission from the originator is obtained, all Criminal Code Prohibition Orders should be released on PIC-VS as court disposition. Non-criminal driving suspensions are not to be included on a PIC or PIC-VS.

IMPORTANT NOTES (Prohibitions after Record Suspension)

- ↑ If the subject of a firearm prohibition order has been granted a Record Suspension (pardon), the offence recorded in the REMNO field as well as the FPS number must be removed from the PROHIB entry.
- ↑ If the subject of a firearm prohibition order has been granted a discharge pursuant to s730CC, the agency may elect not to enter the offence and FPS number into the REMNO field. Should an agency elect to enter this information it must be removed from the entry by the end of the disclosure date.
- ↑ These measures apply equally to adults and young persons.

26. Provincial Offences

Provincial offences, where a person was charged by way of an RCC, may be released from local police files until the retention period has been met on a PIC-VS. Consideration should be given to provincial offences of a more serious nature (e.g., trafficking in animal parts, on-going supplying of liquor to minors, large bootleg operations).

27. Appeals

When a charge results in a conviction that has then been appealed, police services should release the details under the heading of Convictions for all levels of checks with the current disposition and a notation that it is under appeal.

4 Vulnerable Sector CPIC Query

As part of the Police Information Check with Vulnerable Sector Check (PIC-VS), a vulnerable sector (VS) CPIC query must be conducted. This query is used to determine if an individual seeking employment and/or volunteering in a position of authority or trust relative to vulnerable persons has any convictions for a sexual offence listed in the *Criminal Records Act* (CRA) for which a record suspension was granted.

Section 6.3(3) of the CRA places the responsibility on the employer (whether that be an individual or an organization) or volunteer agency to determine whether or not vulnerable sector screening is required. However, police services are prohibited from conducting VS checks if they do not feel the position meets the requirements for a VS check [CRA 6.3(4)]. In compliance with the CRA, the applicant or agency must be responsible for the well-being of vulnerable persons.

6.3 (3) At the request of any person or organization responsible for the well-being of a child or vulnerable person and to whom or to which an application is made for a paid or volunteer position, a member of a police force or other authorized body shall verify whether the applicant is the subject of a notation made in accordance with subsection (2) if:

- (a) the position is one of trust or authority towards that child or vulnerable person; and
- (b) the applicant has consented in writing to the verification.

Child means: a person who is less than 18 years of age.

Vulnerable Persons are described in the CRA as:

"Persons who, because of their age, a disability or other circumstances, whether temporary or permanent,

- a) are in a position of dependence on others; OR,
- b) are otherwise at a greater risk than the general population of being harmed by persons in a position of authority or trust relative to them.

Therefore, a query of Sex Offenders with a record suspension will be conducted through CPIC if:

1. The person or organization has determined that the applicant will be responsible for the well-being of one or more children or vulnerable persons; and
2. The applicant is a resident of the local police service's jurisdiction (as per the RCMP Dissemination of Criminal Record Information Policy); and
3. The applicant proves identification; and
4. The applicant completes the RCMP Vulnerable Sector Consent FORM 1 or the police agency's application with equivalent wording incorporated into the form.

IMPORTANT NOTE: Possible matches are based on name, gender and date of birth. When the VS flag is set on a CNI query, the computer does an initial or standard CNI surname query. The computer uses a find code for the surname in the search so that similar surnames as well as exact matches will be a hit. It also includes a search of a date of birth range of 10 years before and 10 years after the date of birth specified on the query. If the vulnerable sector flag was set and one or more records were returned, and the score was zero or more the VS message will appear and the process ends. If no possible hits were returned from the initial surname query, a subsequent query is automatically conducted, searching for an exact match on sex (male, female or unknown) and date of birth only. This CPIC enhancement was implemented in July 2010. If the VS flag was set and one or more records were returned, the VS message will appear.

A possible match on a query will respond with the following pre-formatted message:

“For screening of applicants applying for positions working with vulnerable persons, submit fingerprints on Form C216-C and consent forms to the RCMP Identification Services in Ottawa. Any records returned may or may not pertain to the subject of your enquiry. Positive identification can only be confirmed through the submission of fingerprints. No information relating to this message may be disclosed.”

If the above message is received, fingerprints are mandatory to complete a PIC-VS.

NOTE: There will be no name associated to this pre-formatted message. The hits returned from this CNI VS query may also include CNI information on other possible hits which may or may not pertain to the applicant.

Refusal to submit fingerprints

If the applicant refuses to submit fingerprints, the PIC-VS application process must be discontinued.

Fingerprinting for a possible VS match

If the applicant elects to continue the process, the police agency must submit the following package to Canadian Criminal Real time Identification Service (CCRTIS):

- a) Digital fingerprints. Identify that the fingerprints are being submitted for the purpose of a VS check, the position applied for, the types of vulnerable individuals and the name of the organization the applicant will be employed/volunteering with.
- b) The mandatory signed RCMP Vulnerable Sector Consent FORM 1 - Consent for Check for a Sexual Offence for Which a Record Suspension has Been Granted or Issued. This will be done biometrically through the digital fingerprint system. This consent must indicate if the VS check is required for employment or volunteer purposes (not both), the position applied for, a description of the vulnerable persons, and the name of the organization that determined the requirement for a VS check. (this information will auto-load from the system)
- c) For volunteers, a letter on letterhead from the volunteer organization confirming that a VS check is a requirement. This does not need to be submitted however must

be retained for a 2 year period for auditing purposes. A letter is required only for the submission of volunteer VS fingerprints.

- d) For paid VS checks (e.g., employment, school or homestay) the RCMP charges a fee. For applicable fees and mailing address see the RCMP website at <http://www.rcmp-grc.gc.ca/cr-cj/vulner/index-eng.htm> (at present this fee is \$25.00)

If the RCMP returns the fingerprints with no disclosed sexual offence convictions for which a record suspension was granted, the police agency will complete the search using the PIC-VS guidelines.

If the RCMP confirms that the applicant has a sex offence with a record suspension, the information will be forwarded to the Minister of Public Safety to authorize disclosure of the information contained in the file. If a suspended sexual offence is disclosed to police, see "Disclosure of Information" below.

NOTE: If the applicant chooses not to disclose the information, the police agency must contact the requesting person (employer) or volunteer organization in writing indicating that the police agency was unable to complete the PIC-VS.

Disclosure of Information

When the information is authorized for disclosure by the Minister of Public Safety and Emergency Preparedness, any sex offence with a record suspension and criminal records associated with the fingerprints will be returned to the submitting police service. If CCRTIS returns the criminal record and a record suspension for a sex offence do not transcribe the record, release the RCMP product as authorized by the Minister.

If CCRTIS returns the criminal record and sexual offence with a record suspension the police service will then obtain the applicants consent in writing for disclosure on RCMP Form 2 – Consent for Disclosure of Record. If the applicant refuses, the entire PIC-VS process is considered abandoned and all documentation must be destroyed.

Once the applicant has signed FORM 2 giving consent for the release of the record(s) the police service must forward the result to the person (employer) or volunteer agency. Under Section 6.3(7) of the CRA, "a police force or other authorized body shall disclose the information referred to in subsection (6) to the person or organization that requested verification, if the applicant for a position has consented in writing to the disclosure".

The RCMP does not retain any fingerprints submitted for a VS query. Therefore, if the employer or volunteer organization requires future VS checks, the applicant must submit fingerprints.

If the information is not authorized for disclosure, no reference is to be made to the information.

NOTE: Any hard copy fingerprint results returned from CCRIS should be returned to the applicant. In the case of digital responses the required approved document will be provided to the applicant.

Fingerprinting for an Adoption Application

CCRTIS encourages police agencies to conduct fingerprint based criminal record checks for all adoption applications and applicants may request a Police Information Check for a security clearance in the Adoption Process.

The PIC-VS procedure is to be followed; however, given that "Vulnerable Sector" is defined in the *Criminal Records Act* as only applying to "paid or volunteer" positions, by definition, when verifying a criminal record for adoption purposes, a "Vulnerable Sector" check is not completed. Nonetheless, the same search as a "Vulnerable Sector" search is completed by Ottawa, including a fingerprint search, which will verify if the person has a record suspension for sex offences, along with seeking approval from the Minister for disclosure.

The police agency's response, issued on a cleared check, will indicate that the "Vulnerable Sector" check was not completed (though, in fact, a VS search has been conducted).

5 Self Declaration

There are two methods for verification of a Criminal Record; either through the submission of fingerprints or by (self) declaration.

(Self) Declaration of a Criminal Record is a process whereby the Applicant declares their adult criminal convictions to the Police Service in accordance with the CCRTIS Dissemination of Criminal Record Information policy.

Declaration MUST include:

- a) All convictions for offences under Federal Law.

Declaration must NOT include:

- a) A conviction for which the applicant has received a Record Suspension in accordance with the Criminal Records Act.
- b) A Finding of Guilt where the applicant was a "young person" under the Youth Criminal Justice Act, however, the RCMP will provide a response if fingerprints are submitted.
- c) An Absolute or Conditional Discharge, pursuant to section 730 of the Criminal Code.
- d) An offence for which the applicant was not convicted.
- e) Any Provincial or Municipal offences.
- f) Any charges dealt with outside of Canada.

In order to release criminal convictions identified through a name based query, the Police Service must be satisfied that the applicant's declared criminal record information is a match to their registered criminal record held at the RCMP National Repository of Criminal Records.

Name-Based Criminal Record Check Responses

NEGATIVE – Standard Response

When the CNI/CRS query does not identify any possible criminal record associated to the applicant the following standard response is to be used:

Based solely on the name(s) and date of birth provided, a search of the RCMP National Repository of Criminal Records did NOT identify any records with the name(s) and date of birth of the applicant. Positive identification that a criminal record does or does not exist at the RCMP National Repository of Criminal Records can only be confirmed by FINGERPRINT comparison. Delays do exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records.

CONFIRMATION OF A CRIMINAL RECORD – Standard Response

When the CNI/CRS query identifies a criminal record that matches to the criminal record information declared by the applicant, the results of a name based query may be released using the following standard response:

Based solely on the name(s) and date of birth provided and the criminal record information declared by the applicant, a search of the RCMP National Repository of Criminal Records has resulted in a POSSIBLE match to a registered criminal record. Positive identification that a criminal record does or does not exist at the RCMP National Repository of Criminal Records can only be confirmed by FINGERPRINT comparison. As such, the criminal record information declared by the applicant does NOT constitute a Certified Criminal Record by the RCMP. Delays do exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records.

INCOMPLETE – Standard Response

If a police service is not satisfied the applicant's declared criminal record information is a match to their registered criminal record held at the RCMP National Repository of Criminal Records, the following response must be used, advising fingerprints are required:

Based solely on the name(s) and date of birth provided and any criminal record information declared by the applicant, a search of the RCMP National Repository of Criminal Records could NOT be completed. Positive identification that a criminal record does or does not exist requires the applicant to SUBMIT FINGERPRINTS to the RCMP National Repository of Criminal Records by an authorized police service or accredited private fingerprinting company. Delays do exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records.

Name-Based Vulnerable Sector Check Responses

NEGATIVE – Standard Response

When the CNI/CRS query does not identify any possible criminal record associated to the applicant AND the scoring criteria have not been met for Flagged Suspended Sex Offender Records (VS:Y), the following standard response is to be used:

Based solely on the name(s) and date of birth provided, a search of the RCMP National Repository of Criminal Records, including suspended sex offender records, did NOT identify any records with the name(s) and date of birth of the applicant. Positive identification that a criminal record does or does not exist at the RCMP National Repository of Criminal Records can only be confirmed by FINGERPRINT comparison. Delays do exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records.

CONFIRMATION OF A CRIMINAL RECORD (Active criminal record only) – Standard Response

When the CNI/CRS query identifies a criminal record that matches to the criminal record information declared by the applicant AND the filtering criteria have not been met for Flagged Suspended Sex Offender Records (VS:Y), the results of a name based query may be released using the following standard response:

Based solely on the name(s) and date of birth provided and the criminal record information declared by the applicant, a search of the RCMP National Repository of Criminal Records, including suspended sex offender records, has resulted in a POSSIBLE match to a registered criminal record, but not to a suspended sex offender record. Positive identification that a criminal record does or does not exist at the RCMP National Repository of Criminal Records can only be confirmed by FINGERPRINT comparison. As such, the criminal record information declared by the applicant does NOT constitute a Certified Criminal Record by the RCMP. Delays do exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records.

INCOMPLETE – Standard Response

When the CNI/CRS query identifies any criminal record of possible association to the applicant that does not match to the criminal record information declared by the applicant AND/OR the filtering criteria have been met for Flagged Suspended Sex Offender Records (VS:Y), the following response must be used, advising fingerprints are required:

Based solely on the name(s) and date of birth provided and any criminal record information declared by the applicant, a search of the RCMP National Repository of Criminal Records, including suspended sex offender records, could NOT be completed. Positive identification that a criminal record does or does not exist requires the applicant to SUBMIT FINGERPRINTS to the RCMP National Repository of Criminal Records by an authorized police service or accredited private fingerprinting company. Delays do exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records.

PIP

6 Police Information Portal

The Police Information Portal (PIP) will be used to process a Police Information Check or Police Information Check with Vulnerable Sector Screening. The PIP Policy and Procedure Manual was designed to include this function. Section 7.42 of the PIP manual states:

Queries for Non-Criminal Purposes

- 7.42 If the request for release of any PIP information is for security and reliability clearances, the requester must have documented written consent of the subject of the query. The subject must agree to the release of information identifiable to that person that may be on the PIP System.

Proper use of information must be observed. For example, Extrajudicial Measures under the YCJA may be used for police investigative purposes but shall not be used for non-investigative purposes such as background checks. All information must be confirmed and authorized for release by the contributing agency.

List of Police Agencies Currently Publishing to PIP

Only Category 1, Law Enforcement agencies can obtain a copy of the police services currently publishing to PIP by sending an email to CPIG-CENTRE-PIP@rcmp-grc.gc.ca and requesting a copy. This email address can also be used for any other PIP inquiries.

When conducting a check for an applicant who has previously resided outside of B.C., a written request (CPIC narrative message, v-mail or fax) must be sent to the police agency in the jurisdictions of previous residence. The written request is to ask that a local indices check be performed. This is necessary because certain files, in particular private/invisible files, do not appear in PIP query results. Should a PIP contributing agency outside of B.C. fail to acknowledge or deny a request, this should be noted on the response portion of the form as: "local indices from agency X, not available".

Within B.C., it is not necessary to send a written request to another police agency in a jurisdiction of previous residence, as B.C. agencies' files are all visible through a query of the jurisdiction specific PRIME server.

7

Refusal to Complete a Police Information Check and Exceptional Disclosure – Assessment and Authority to Disclose

As detailed in this Guideline, findings released in response to a PIC request do not routinely include the following information, as located in police databases, which documents that:

- ↑ the applicant was a suspect in an offence, but was not charged;
- ↑ the applicant is suspected of having committed an offence, the investigation is on-going, and a decision whether charges will be recommended has not yet been made;
- ↑ police recommended the applicant be charged with an offence, but Crown counsel has not yet decided whether to approve the charge(s);
- ↑ police recommended the applicant be charged with an offence, but Crown counsel decided not to approve the charge(s); and
- ↑ police have had adverse contact with the applicant specific to an incident involving the threat or actual use of violence directed at other individuals, regardless of the applicant's mental health status.

If information, as above, is located, a police agency retains the right to refuse to complete the PIC. If refusing to complete the PIC is determined not to be sufficient, because a risk to the public or organization exists, then alternatively, in exceptional cases the information may be disclosed, or may be required to be disclosed.

Right to refuse to complete a PIC:

As an alternative to disclosing additional information on the results form, or notifying the listed employer or volunteer agency, a police agency processing a submitted PIC request also retains the discretion to refuse completion of the PIC. A police agency may decide to refuse to complete a PIC, if it determines that it would be counter to the interests of the employer or volunteer agency listed on the submitted form, to receive PIC results that do not include additional information located by the police agency in databases.

Statutory Authority to release additional information:

Police agencies' authority to disclose additional information, about the applicant, is contained in the provincial or federal legislation detailed below, or derived from a common law duty to warn, rather than the applicant's consent. *Due to the need to interpret legislation and give consideration to legal precedent, in the course of determining whether disclosure is legally authorized and/or required, the decision maker may determine that it is necessary to obtain legal advice.*

How to Disclose:

An exceptional disclosure of information that is not otherwise routinely released would be effected by either including it as part of the PIC results that are reported on the form returned to the applicant, or by way of separate communication, from the police agency, to the employer or volunteer agency listed by the applicant on the form (or potentially by both methods).

Municipal police discretion to release additional information:

In accordance with the provincial Freedom of Information & Protection of Privacy Act, R.S.B.C., c. 165, (FIPPA), a municipal police agency may (discretionary) disclose additional information about an applicant, if it is determined that compelling circumstances exist that affect anyone's safety or health. The applicant is required to be provided with notice of such disclosure, unless doing so could harm someone's health or safety. The FIPPA states:

Disclosure inside or outside of Canada

33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

(m) if

(i) the head of the public body determines that compelling circumstances exist that affect anyone's health or safety, and

(ii) notice of disclosure is mailed to the last known address of the individual the information is about, unless the head of the public body considers that giving this notice could harm someone's health or safety;

Municipal police requirement to release additional information:

Further in accordance with the FIPPA, a municipal police agency is required (mandatory) to disclose additional information about an applicant, if it determines that the information is about a risk of significant harm to the safety or health of others posed by the applicant. Again, the applicant is normally required to be provided with notice of such disclosure, and here the provincial Information and Privacy Commissioner must be notified as well. The FIPPA states:

Information must be disclosed if in the public interest

25 (1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information

(a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or

(b) the disclosure of which is, for any other reason, clearly in the public interest.

(2) Subsection (1) applies despite any other provision of this Act.

(3) Before disclosing information under subsection (1), the head of a public body must, if practicable, notify

(a) any third party to whom the information relates, and

(b) the commissioner.

(4) If it is not practicable to comply with subsection (3), the head of the public body must mail a notice of disclosure in the prescribed form

(a) to the last known address of the third party, and

(b) to the commissioner.

RCMP discretion to release additional information:

The disclosure of additional information by the RCMP is authorized under the federal Privacy Act, R.S.C., 1985, c. P-21, and the RCMP may disclose additional information about an applicant where the public interest in disclosure clearly outweighs any invasion of privacy that could result. The federal Privacy Commissioner must normally be notified in advance of the disclosure and the Privacy Commissioner may notify the applicant. The Privacy Act states:

Disclosure of personal information

- 8 (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where personal information may be disclosed

- (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(m) for any purpose where, in the opinion of the head of the institution,

- (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or
- (ii) disclosure would clearly benefit the individual to whom the information relates.

Common law duty to warn:

Litigation in a small number of civil cases has established that, in certain circumstances police have a duty to warn those at risk, of the dangers presented by a particular situation or by a particular individual. The duty to warn has been found to manifest when the police have information establishing a foreseeable risk, and there exists a special relationship of proximity between the danger and those at risk.

While every situation will always be decided by a court on its own facts, it is reasonable to expect that police could be considered subject to a duty to warn when:

- ↑ information in police reviewed records establishes that an applicant poses a foreseeable risk;
- ↑ the risk is specifically to persons who would be exposed to the applicant, if he or she were to be employed or volunteering as indicated in the completed PIC form; and

- ↑ the basic premise of the PIC application is to allow for a determination of the applicant's suitability by the listed employer or volunteer agency.

No threshold of the degree of danger that the applicant would have to pose to engage the duty to warn, has been conclusively established at law; however, the greater the risk of harm to the physical or mental wellbeing of others, posed by an applicant, the greater the likelihood that a duty to warn could be considered to exist.

Relatively few cases have been litigated, so as to provide more definitive decision making guidance in relation to the duty to warn. Decision making about exceptional releases is further complicated by consideration of the following competing pressures:

- ↑ the potential of an allegation of misconduct for failure to discharge the duty to warn by making a proper notification;
- ↑ the potential of an allegation of misconduct based on a claim that a notification was improperly motivated;
- ↑ municipal employees being subject to the risk of committing a statutory offence, under the FIPPA, of "unauthorized disclosure";
- ↑ the risk of complaints to the provincial Information & Privacy Commissioner or federal Privacy Commissioner alleging improper release of information; and
- ↑ the potential for applications for judicial reviews of decisions to release information, constitutional challenges of decisions made, applications for injunctions, or civil claims, including allegations of misfeasance in public office.

Category examples of exceptional cases:

The information in each record concerning an applicant must be assessed on its own merit; however, an attempt to define categories of information, that would likely be released, yields the following:

- a. information establishing a foreseeable future risk of harm, to the physical or mental health or safety of others, posed by the applicant being in the environment of the listed employer or volunteer agency; and
- b. information about an applicant specific to criminal activity, where that activity tends towards destabilizing individuals' economic security, or the greater social or economic fabric and order, which could include, but is not limited to, single incidents or patterns of incidents of: fraud; criminal activity targeted at the same employment or volunteer sector; or affiliation with organized crime groups.

A police agency must assess the information, on a case by cases basis, and assess application of the FIPPA and the Privacy Act disclosure authorities and mandatory disclosure requirements, detailed above.

Exceptional release decision making:

The decision to release additional information in response to a PIC request is not to be made by the employee processing the record check. Instead, the employee must forward the information to a decision maker in a supervisory or managerial position, in order to determine if an exceptional disclosure is warranted. Agencies engaging in a disclosure subject to the FIPPA require approval by a delegate of the designated head of the agency.

Exceptional Disclosure Assessment

When applying the following assessment, care should be taken to not determine risk based on an attempted prediction of future behavior, but rather to identify whether an applicant demonstrates documented patterns of behavior that have put the safety, wellbeing or health of others at risk, or been aimed at destabilizing individuals' economic security, or destabilizing the social or economic fabric or order.

Step 1: Identify and Collect Records

- ↑ A search of national and local database reveals information that would be releasable pursuant to PIC-VS request or information that gives rise to a concern that the applicant, if s/he were to be engaged by the listed employer or volunteer agency, potentially presents a risk: to the safety, wellbeing or health of others; to individuals' economic security; or to the social or economic fabric or order.
- ↑ Prepare a list of the files containing the information and present for supervisory review.

Step 2: Review Records

The following are factors for the decision maker to consider in the review:

- ↑ whether the behavior was specific to a targeted individual or individuals in the same or a similar employment or volunteer sector as listed in the PIC application;
- ↑ whether the listed employer or volunteer agency, and persons associated thereto, bear similar vulnerabilities as exploited by previous behavior;
- ↑ whether there is a pattern of repeated behavior;
- ↑ whether the behavior was towards more than a single person;
- ↑ when the incident(s) took place;
- ↑ the number of incidents; and/or
- ↑ the reason the incident(s) did not result in charges or a conviction.

Step 3: Disclosure Assessment

Decision making by the supervisor / manager, with recommendation to the head as applicable, as to whether:

- ↑ circumstances exist that affect anyone's safety or health (municipal agency);
- ↑ the applicant poses a risk of significant harm to the safety or health of others (municipal agency);
- ↑ the disclosure is, for any other reason, clearly in the public interest (municipal agency);
- ↑ the public interest in disclosure clearly outweighs any invasion of privacy that could result (RCMP); or
- ↑ the circumstances engage the common law duty to warn.

In the course of completing this step, the decision maker may determine that legal advice is necessary, in order to assist with the determination of whether disclosure is legally authorized and/or required.

The decision maker must also comply with the statutory requirements specific to notifying the applicant of the decision, i.e., the pending release of the additional information, and must determine whether the applicant is to be given an opportunity to respond, and if so, the timeframe for the same.

Step 4: Release Record(s)

Once the decision maker has determined that the additional records are to be released, then the additional non-conviction information can be released on the PIC results pages (for example, with a heading such as Non-Conviction Records Concerning Public Safety) or disclosed by standalone written notice to those at risk. Alternatively, the completion of the PIC can be refused.

As per PRIME policy, if the non-conviction records are from another police agency, release permission must be obtained from the agency.

Step 5: Reconsideration Process

Applicants may apply for reconsideration of this decision (see Reconsideration Process specific section of the Guideline).

8 B.C. Human Rights Considerations

In determining what information should be included on a Police Information Check, this guideline strives to balance the privacy and human rights of the applicant against the safety of the public and, in particular, vulnerable individuals with whom the applicant would be interacting.

It is the responsibility of the organization/employer, not the police agency, to determine whether an applicant requires a Police Information Check (PIC) or a Police Information Check with Vulnerable Sector Screening (PIC-VS). To avoid potential discrimination under British Columbia's Human Rights Code, the organization/employer should have the applicant obtain any police check as one of the last steps involved in the hiring process, only after a conditional offer has been made.

Prior to having an applicant apply for a police check, an organization/employer should determine if it is a bona fide requirement for the job in question. The Supreme Court of Canada has set out a three step test, referred to as the Meiorin* test, which states such a requirement must be:

1. For a purpose or goal that is rationally connected to the function being performed.
2. Made in good faith, in the belief that it is necessary for the fulfillment of the purpose or goal.
3. Reasonably necessary to accomplish its purpose or goal, in the sense that there is no other alternative to accomplish the goal and it is impossible to accommodate the claimant without undue hardship (i.e., the health and safety of others is put at risk, or cost).

* *British Columbia (Public Service Employee Relations Commission) v. BCGSEU*, [1999] 3 S.C.R. 3.

If criminal charges have been laid and are still before the courts, the charges are to be listed on a PIC. If a criminal charge was laid, but did not result in a conviction, the charge(s) and status/disposition of each charge is to be listed on a PIC-VS.

If an investigation resulted in a criminal charge not being laid, the applicant is listed by role code, along with the incident type on a PIC-VS. The following factors should be considered by the police agency in deciding whether to release this information:

1. The report indicates the applicant's involvement as, but not limited to, suspect, accused, warned, cautioned.
2. Whether any actions by the applicant placed themselves or a member of the public at risk or harm.
3. Whether any weapon or force was used by the applicant.
4. How long ago the incident occurred.

9 Privacy Considerations

In order to engage in suitability assessments and conduct risk management, employers and volunteer organizations may determine that they require certain kinds of background information about prospective employees and volunteers. British Columbia police agencies offer two types of Police Information Checks: Police Information Check (PIC), and Police Information Check with Vulnerable Sector Screening (PIC-VS). If an organization determines that a check just for convictions is required, such a check can be obtained by submitting fingerprints to CCRTIS, either through the RCMP or an accredited private company. Police agencies play a neutral role in relation to such decisions regarding employment risk assessment. The PIC process formalizes and standardizes the information that organizations and public bodies obtain from a police agency, should a prospective employee or volunteer be required to provide the results of a PIC or PIC-VS. The PIC also acts to limit the amount of detail in the information released.

Businesses and non-profit organizations must comply with the Personal Information Protection Act ("PIPA"), and every public body must comply with the Freedom of Information & Protection of Privacy Act ("FIPPA"). These provincial Acts, and similar federal laws, contain rules governing how a business, non-profit or public body is allowed to collect, use or disclose information about a candidate for employment or a volunteer position.

Before requiring a potential volunteer or employee to attend a police agency for a police information check, every organization or public body is expected to be familiar, and ensure compliance, with the legal requirements concerning the collection, use and disclosure of the information obtained through such a check.

A police agency's disclosure of releasable information, concerning an applicant, is permitted, as the disclosure is at the request, and with the consent, of the applicant. Once released, the subsequent use or further disclosure of the information is beyond the police agency's control. Recognizing the potentially highly sensitive and personal nature of the police information, the PIC processes set out in this guideline include the following:

1. PIC or PIC-VS result are only disclosed to the applicant, and require confirmation of identity through the presentation of photo identification.
2. Due to the seriousness of the offence, and in accordance with the requirements of the federal Criminal Records Act, where an applicant consents to the release of a record concerning a sexual offence conviction for which a record suspension was granted, that record must be released directly to the potential employer or volunteer agency (as per the process in Form 2 - RCMP GRC 3924e).
3. Incident information contained in local police indexes will routinely only be disclosed on a PIC-VS if it has not yet reached the retention date set out in provincial PRIME-BC retention schedules.
4. In order to ensure the utmost accuracy of any information that is to be disclosed, if an applicant challenges the accuracy of the information provided to them, a formal reconsideration process is available, providing an internal supervisory level review of the information.

Without the PIC process, employers and volunteer organizations seeking information from police, about an applicant's background, may consider it necessary to have applicants make requests for their personal information pursuant to the FIPPA or the federal Privacy Act, and then provide the records received, in some manner, to the employer or volunteer agency. Such a practice is undesirable as it could potentially result in the routine disclosure, to employers and other organizations, of records containing extremely detailed personal information.

It remains open to an applicant to make a FIPPA or Privacy Act request for records relating to any incident disclosed through the PIC process. An applicant may wish to make such a request in order to confirm the PIC results, or possibly to provide a potential employer or volunteer agency more detailed information about an event documented in the PIC results. Again, Police agencies play a neutral role in relation to employment practices, unless a situation exists in which a police agency has a duty to disclose information, due to circumstances that affect the health or safety of others.

10 Reconsideration Process

1. An applicant who had a Police Information Check with Vulnerable Sector Screening (PIC-VS) may wish to have information excluded from the results. This process is not suitable for the Police Information Check (PIC) because the process is for the purposes of non-convictions only. Individuals wishing to have information removed from their PIC can utilize the Record Suspension process through the Parole Board of Canada. Information that is listed incorrectly because of a mistake or lack of information should be handled outside of this process.
2. A reconsideration request **MUST** be made by the applicant in writing and submitted to:

The Authority Identified Within Your Agency

Unit Identified

Name of Police Agency

Street Address

City, Province

Postal Code

3. Requests for reconsideration should be made within 30 days of the completion of the applicant's Police Information Check with Vulnerable Screening (PIC-VS). Reconsideration requests will be processed as quickly as possible.
4. The reconsideration process will take into account the request of the applicant, and will include the following stages:
 - ↑ Check that all procedures in accordance with these guidelines have been followed;
 - ↑ Check that all disclosed offences or contacts are confirmed and releasable;
 - ↑ Consideration of the applicant's request for information to be excluded;
 - ↑ A written explanation of the final decision of the police agency.
5. The reconsideration request will be considered by an individual not involved in the original application, and senior to original processor. All decisions regarding the reconsideration application will be made in accordance with these guidelines.

Below are some further considerations when developing a reconsideration procedure.

To qualify for the reconsideration process:

- ↑ Process is only available for PIC-VS.
- ↑ Appeal should be made within 30 days upon receipt.
- ↑ Can only appeal entries that appear on the record check.
- ↑ Convictions will not be eligible for reconsideration.
- ↑ Outstanding judicial orders or cases that are before the courts are not eligible for reconsideration
- ↑ Youth Criminal Justice Act entries are not eligible for reconsideration.

Note: If any of the above qualifications are not met, the application will be rejected upon receipt and the applicant will be notified in writing.

To apply for reconsideration:

- ↑ Applicant submits letter or form designed by police service for reconsideration.
- ↑ Applicant should include a copy of their current record check.
- ↑ Applicant may include any documents they feel may support their request.
- ↑ Police services may wish to limit the length of written representation to one or two pages.

The reconsideration person in authority:

- ↑ Reviews submissions and responds in writing to the applicant.

Considerations during the review:

- ↑ Whether the incidents target a vulnerable person.
- ↑ Whether there is repeated behaviour towards more than one person.
- ↑ When the incidents took place.
- ↑ The number of incidents.
- ↑ Whether there is a pattern of incidents.
- ↑ The reason the incident did not result in a conviction.

Glossary

Absolute Discharge Adult	A court disposition where the accused is not convicted, but is found guilty of an offence and is discharged with no conditions. [CCC 730]
Absolute Discharge Youth	A court disposition where the accused youth is not convicted, but is found guilty of an offence and is discharged with no conditions. [YCJA 42(2)(b)]
Accused	A person against whom legal proceedings have commenced.
Acquittal	A court disposition where the accused has been found not guilty of the charges presented before the court.
Agency	An organization, company, bureau or in some cases an individual that would require an applicant to obtain a Police Information Check.
Alternative Measures	A community supervision program that allows charges to be stayed after an adult accused of a criminal charge who would be prepared to plead guilty or at minimum, acknowledge guilt. The result is a mild penalty such as community service, an apology to the victim or counseling. May also be referred to as Diversion or a Pre-Trial Diversion.
Ancillary Data Bank	The Ancillary Data Bank is one of four data banks of operational information within the CPIC system. It contains diverse files of information on subjects such as vehicle registered owners, driver's licenses, wandering persons and penitentiary inmates. The information in the files is contributed and maintained by either non-police agencies (i.e., Correctional Agencies of Canada for inmate data) or police agencies (i.e., the RCMP for Restricted Weapon Registration System (RWRS) data). Only the owner of the information may grant access to the data.
Applicant	An individual undergoing a Police Information Check.
Bill C7 (1999)	Proclaimed August 1, 2000 to amend the <i>Criminal Records Act</i> to permit the flagging of sex offenders with a record suspension.
British Columbia Association of Chiefs of Police BCACP	The objective of the BCACP is encouraging and developing co-operation among all its members in the pursuit of and attainment of their goals, Promoting a high standard of ethics, integrity, honour and conduct. Fostering uniformity of police practices. Encouraging the development and implementation of efficient and effective practices in the prevention and detection of crime and effectively communicating problems and concerns to appropriate levels of authority.

<i>Canadian Charter of Rights and Freedoms</i>	Enacted in 1982, the Charter contains provisions protecting the rights of an individual.
Canadian Criminal Real Time Identification Service CCRTIS	Canadian Criminal Real Time Identification Service (CCRTIS) maintains the national repository of fingerprint and criminal record information and is mandated to provide direct operational support to the Canadian law enforcement, criminal justice and public security communities, as well as international partners such as the Federal Bureau of Investigation (FBI) and Interpol for criminal, civil and immigration purposes. CCRTIS is the national provider of biometric-based criminal record verifications for civil and criminal court purposes as well as the security screening environment for all levels of government and the general public.
CCRTIS Dissemination of Criminal Record Information Policy	CCRTIS policy that outlines the requirements for name based criminal record and VS checks of the Identification Databank on CPIC.
Canadian Police Information Centre CPIC	The Canadian Police Information Centre (CPIC) is a computerized national repository of information that facilitates the sharing of information among authorized agencies. The CPI Centre manages the CPIC system as well as PIP and PSP.
Certified Criminal Record Product	A collection of an individual's offence convictions and non-convictions (where authorized) that are releasable in accordance with federal laws. Based on the results of a Fingerprint-based Criminal Record Verification.
Conditional Discharge Adult	A court disposition where the accused is not convicted but found guilty of an offence and is discharged with conditions. [CCC 730]
Conditional Discharge Youth	A court disposition where the accused youth is not convicted but found guilty of an offence and is discharged with conditions. [YCJA 42(2)]
Consent Form 1	A form to be signed by the applicant that allows police agencies to conduct a query for sex offences with a record suspension for the purpose of vulnerable sector screening. [CRA 6.3(3) & Reg. Part 2 CRA]
Criminal Name Index CNI	CPIC query function based on name, gender, and date of birth. This query is used to match names against possible criminal records on the Identification Databank or to identify potential hits to a sex offence with a record suspension.

CRII	Full criminal record, containing conviction history, a summary of police-related information and a list of agencies who have contributed information to the record.
Declaration of Criminal Record	A process whereby the Applicant declares all offence convictions to the CPIC Agency in accordance with CPIC policy requirements and federal laws. Based on the declared criminal record information, the CPIC Agency may confirm that the Applicant's declared criminal record information possibly matches to a registered criminal record held at the RCMP National Repository of Criminal Records, pursuant to CCRTIS Dissemination of Criminal Records Information Policy.
Dismissed	A court disposition where the court stops or interrupts criminal proceedings against the accused.
Diversion	A community supervision program that allows charges to be stayed after an adult accused who would be prepared to plead guilty or at minimum, acknowledge guilt. The result is a mild penalty such as community service, an apology to the victim or counseling. May also be referred to as Alternative Measures. [CC 717]
Dual-Procedure Offence	An offence that can be prosecuted either as a summary conviction offence or an indictable offence. The Crown Attorney chooses the mode of prosecution. Examples include but are not limited to: Impaired Driving, Assault, and Theft Under. Also referred to as Hybrid Offences.
Extra-Judicial Measures EJM	Extrajudicial Measures are actions other than judicial proceedings under the <i>Youth Criminal Justice Act</i> (YCJA) used to deal with a young person alleged to have committed an offence. Extrajudicial Measures include: Warning, Caution, Referral, and No Further Action. [YCJA 2(1)]
Extra-Judicial Sanctions	Extrajudicial Sanctions may be used to deal with a young person alleged to have committed an offence only if the young person cannot be adequately dealt with by a warning, caution or referral because of the seriousness of the offence, the nature and number of previous offences committed by the young person or any other aggravating circumstances. Extrajudicial Sanctions are dealt with and managed by the Ministry of the Attorney General thereby being outside of police control. [YCJA 10]

Finding of Guilt	A court disposition where a young person is found guilty (the term convicted does not apply to youth). Or an adult is discharged of an offence pursuant to CC730.
Firearms Interest Police FIP	Firearms Interest Police (FIP) is a category within the Investigative Databank of the CPIC system. This category is used to record data on persons who, in the last five years, have been involved in incidents such as, but not limited to: violence, harassment and drug related events. See CPIC User Manual for further details.
Foreign Information	Information obtained via CPIC contributed by foreign countries.
Forensic Science and Identification Services	Forensic Science and Identification Service (FS&IS), is an integral part of NPS with a mandate to provide quality investigative support services for front line policing.. FS&IS provides a wide range of forensic programs and services to clients in Canada and internationally through forensic science services.
Hit	A response to a CPIC or police database query.
Hybrid Offences	An offence that can be prosecuted either as a summary conviction offence or an indictable offence. The Crown Attorney chooses the mode of prosecution. Examples include but are not limited to: Impaired Driving, Assault, and Theft Under. Also referred to as Dual Procedure Offences.
Identification Data Bank	The Identification Data Bank within the CPIC system contains criminal record information. The RCMP Information and Identification Services maintain the information on behalf of police agencies who contribute the records. See RCMP National Repository of Criminal Records.
Identity Documents	A document, in accordance with CCRTIS Dissemination Policy requirements and applicable privacy laws that may be used to authenticate an Applicant's identity in support of a Police Information Check.
Indictable Offence	An indictable offence is a serious crime that has sufficient evidence where the judge/jury can formally charge a person with committing the crime. Such crime can range from rape, kidnapping, murder, robbery etc.

Informed Consent	<p>Informed consent is generally an agreement to do something or to allow something to happen only after all the relevant facts are disclosed.</p> <p>An informed consent can be said to have been given based upon a clear appreciation and understanding of the facts, implications, and future consequences of an action.</p> <p>In order for informed consent to be considered valid, the subject must be competent and the consent must be given voluntarily.</p>
Intelligence Data Bank	<p>The Intelligence Data Bank within the CPIC system contains criminal intelligence information. The information is contributed and maintained by members of the police community responsible for gathering and analyzing criminal intelligence. Access to this data bank is restricted.</p>
Interpol	<p>INTERPOL is an international police organization, with 187 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.</p>
Investigative Databank	<p>The Investigative Data Bank within the CPIC system contains information, grouped into Persons, Vehicles, Marine and Property files, on cases under investigation and includes details on wanted and missing persons, stolen vehicles, stolen boats and other items of stolen or lost property. The information in this data bank is contributed and maintained by police agencies.</p>
JUSTIN	<p>British Columbia's province wide justice information system; a single integrated database comprising almost every aspect of a criminal case.</p>
<i>Juvenile Delinquents Act</i> JDA	<p>Introduced in 1908 as Canada's first legislation to govern young persons in conflict with the law. In 1984, Canada replaced the JDA with the <i>Young Offenders Act</i>.</p>
Local Criminal Record	<p>Criminal dispositions held by individual police agencies, including those not supported by fingerprints.</p>
<i>Mental Health Act</i> MHA	<p>The <i>Mental Health Act</i> in British Columbia is a law that governs how people are admitted to psychiatric facilities, how their mental health records are kept and accessed, their financial affairs are handled, and their release into the community.</p>

National Police Service	National Police Service (NPS) supports Canada's law enforcement community through service lines that provide: forensic analyses of criminal evidence; criminal records information; identification services; technological support; and enhanced learning opportunities and coordination of criminal information and intelligence.
Not Criminally Responsible NCR	No person is criminally responsible for an act committed or an omission made while suffering from a mental disorder that rendered the person incapable of appreciating the nature and quality of the act or omission or of knowing that it was wrong. [CCC 16 and 672.34]
Not Guilty	This court disposition simply means the accused has not been found guilty; however, it does not necessarily equate to innocence. It is a determination by the court that the evidence is insufficient to convict the accused.
Notice and Acknowledgement Forms	Provide individuals with notice of the scope of police records check practices and serve to limit necessary and authorized disclosures to those circumstances where an individual acknowledges his or her intention to pursue an application or accept a conditional offer for a particular position with a service provider.
Occurrence	A report generated as a result of an incident or event investigated by police.
Offender	A person who had been determined by a court to be guilty of an offence, whether on acceptance of a plea of guilty or a finding of guilt.
British Columbia Human Rights Code BCHR	British Columbia's Human Rights Code was enacted in 1973. The Code protects people in British Columbia against discrimination in employment, accommodation, goods, services and facilities, and membership in vocational associations and trade unions.
Organization	An agency, company or bureau that would require the individual to obtain a Police Information Check.
Pardon	See Record Suspension.

Police Automated Registration Information System PARIS	The Police Automated Registration Information System (PARIS) is an Ancillary Data Bank within the CPIC system. It contains information regarding vehicle registration and driver information through the Ministry of Transportation.
Peace Bond	A Court Order that requires a person to keep the peace and be of good behavior especially toward another person. It may also include a no contact condition. [CCC810]
Physical Verification	A process whereby the identity of an applicant is physically authenticated in support of a Police Information Check.
Police Information Check PIC	This level of screening is intended for applicants who are involved as a volunteer, employee or in any situation where a basic PIC is requested (i.e., retail or immigration). This check is NOT intended for applicants who are seeking volunteer and/or employment with vulnerable persons.
Police Information Portal PIP	A nationally integrated master name indexing and records management gateway, allowing participant agencies to access certain information contained in each other's law enforcement databases.
Policing Support Services	Policing Support Services (PSS) is responsible for providing support services to front line police officers, including: service lines that interact with units internal to the RCMP; and service lines that provide services to external RCMP partners.
Police Information Check with Vulnerable Sector PIC-VS	This level of screening is restricted to applicants seeking employment and/or volunteering with vulnerable individuals. It is a collection of offence information, including convictions, non-convictions and other relevant police contact information available from a local police agency's records management system and other systems/records where authorized. This check will include sexual offence convictions for which the individual has received a record suspension where authorized by the Minister of Public Safety and Emergency Preparedness.

Private Information	<p>Anyone who has reasonable grounds to believe that a person has committed an offence may lay information in writing and under oath before a Justice of the Peace.</p> <p>When a private citizen presents the information to the court, it is then referred to either a provincial court judge or a designated justice of the peace, who holds a special hearing. The purpose of the hearing is to determine whether a summons or warrant should be issued to compel the person to attend court and answer to the charge.</p>
Pre-Trial Diversion	<p>Police may refer a person accused of committing a minor offence to a pre-charge diversion program. The accused must attend an interview where they agree to complete a program such as community service, restitution, donation, letter of apology, etc. in order to avoid a court proceeding. May also be referred to as Diversion or Alternative Measures.</p>
PRIME	<p>Police Records Information Management Environment. In February 2003 the BC government committed to connecting every law enforcement agency with one provincial records management system. Today, PRIME is shared by 14 municipal police agencies and 135 RCMP detachments across BC.</p>
Prohibition Orders	<p>A Court Order that prohibits the subject from certain rights or behavior. (Examples: driving, hunting, firearms, parks, etc.)</p>
Real Time Identification System RTID	<p>The RTID system is part of a major Crown project designed to improve the efficiency of Canada's national fingerprint and criminal record repository. It will replace outdated paper processes and legacy systems with re-engineered workflows and automation. Electronically accessed by authorized agencies based on fingerprint submissions.</p>
Record Suspension (formerly called Pardon)	<p>A record suspension allows people who were convicted of a criminal offence to have their criminal record kept separate and apart from other criminal records. Under the <i>Criminal Records Act</i>, the National Parole Board may issue, grant, deny or revoke record suspensions for convictions under federal acts or regulations of Canada. [CRA 4.1]</p>
Reprimand	<p>A youth found guilty receives a lecture or warning from the judge. Section 42.2(a) YCJA</p>
Restraining Order	<p>A Court Order that prohibits the subject from having direct or indirect contact with identified person(s).</p>

RCMP National Repository of Criminal Records	Canada's repository of criminal records relating to individuals that have been charged with indictable and/or hybrid offences. Since the <i>Identification of Criminals Act</i> only allows the taking of fingerprints in relation to indictable or hybrid offences and the RCMP National Repository of Criminal Records is fingerprint-based, the National Repository only contains information relating to these two categories of offences. Summary conviction offences are only included in the National Repository if submitted to the RCMP as part of an occurrence involving an indictable or hybrid offence. With the exception of "young person" indictable or hybrid offence convictions, police agencies are not required by law to report offences to the RCMP. A search of local police records may reveal criminal record information that has not been reported to the RCMP
Special Interest Police SIP	Special Interest Police (SIP) is a category within the Investigative Databank on CPIC.. This category is used to record data on persons who are KNOWN to be dangerous to self or others, a record suspension applicant, overdue on a pass from a federal institution, etc. See CPIC User Manual for further details.
Stayed	The court disposition of Stayed is a halting of proceedings. The charge(s) is suspended and the Crown Attorney has the authority to recommence court proceedings at a later date, within one year. [CC 579]
Summary Conviction Offence	Summary Conviction Offences encompass minor offences in the Criminal Code (i.e., Cause Disturbance, Harassing Telephone Calls). Charges are proceeded with summarily or without an indictment or full trial. The court is generally comprised of a Provincial Court Judge or a Justice of the Peace.
Suspect	A person believed to have committed a crime or offence.
Suspended Sentence	Unless law prescribes a minimum punishment, the court has the power to suspend the passing of sentence (generally for a period of three years) and place the offender on probation. It is the passing of the sentence, not the sentence itself that is being suspended. This means that if the defendant is convicted of another offence during the period when the passing of sentence had been suspended, then the offender may be sentenced for the original offence. [CCC731]

Unfit To Stand Trial	Unable on account of mental disorder to conduct a defense at any stage of the proceedings before a verdict is rendered or to instruct counsel to do so. [CC 673.31]
Vulnerable Person	A person who, because of their age, a disability or other circumstances, whether temporary or permanent are (a) in a position of dependence on others or (b) are otherwise at a greater risk than the general population of being harmed by a person in a position of authority or trust relative to them. [CRA 6.3(1)]
Withdrawn	Withdrawn refers to the Crown stopping or interrupting criminal proceedings against the accused.
<i>Young Offenders Act</i> YOA	The <i>Young Offenders Act</i> (YOA) replaced the <i>Juvenile Delinquents Act</i> in 1984. The <i>Youth Criminal Justice Act</i> replaced the YOA on April 1, 2003.
<i>Youth Criminal Justice Act</i> YCJA	An Act in respect of criminal justice for young persons and to amend and repeal other Acts. The <i>Youth Criminal Justice Act</i> (YCJA) replaced the <i>Young Offenders Act</i> on April 1, 2003.
Young Person	The <i>Youth Criminal Justice Act</i> defines a young person as someone twelve years of age or older, but less than eighteen years of age at the time of committing an offence or alleged to have committed an offence. [YCJA 2(1)]

Appendix A: Records Check Release Chart

Refer to Records Check Release Criteria for further details

Please note that the Records Release Chart is intended to ensure that policies and practices align among police agencies in British Columbia so that citizens, employers and volunteer organizations receive consistent information on Police Information Checks. This chart balances public safety interests with the privacy and human rights of citizens.

OTHER LEGAL POWERS NOT AFFECTED

Nothing in this chart prevents a police agency from disclosing information under either a statutory or common law duty to provide warnings where the health, safety or well-being of an individual or individual is at risk of significant harm.

At times, the Police Information Check service must be denied or refused; however, caution should be used in making the decision to refuse service and it is recommended that a person in a higher authority manage the decision making process.

Record Type	Police Information Check ADULT	Police Information Check YOUTH	Police Vulnerable Sector Check ADULT	Police Vulnerable Sector Check YOUTH
Current Judicial Orders (Peace Bonds, Restraining Orders, Criminal Code Prohibition Orders & Probation Orders)	✓	✓	✓	✓
FIP Firearms Interest Police	⚡ FIP information is not released but can be used as a tool to identify reports or incidents held by other police agencies	⚡ FIP information is not released but can be used as a tool to identify reports or incidents held by other police agencies	⚡ FIP information is not released but can be used as a tool to identify reports or incidents held by other police agencies	⚡ FIP information is not released but can be used as a tool to identify reports or incidents held by other police agencies
INTERPOL	Do Not Query	Do Not Query	Do Not Query	Do Not Query
NCIC	Do Not Query	Do Not Query	Do Not Query	Do Not Query
Outstanding Criminal Charges & Warrants	✓	✓	✓	✓
Motor Vehicle Branch	Do Not Query	Do Not Query	Do Not Query	Do Not Query

Record Type	Police Information Check ADULT	Police Information Check YOUTH	Police Vulnerable Sector Check ADULT	Police Vulnerable Sector Check YOUTH
PIP	✓ All information must be confirmed and authorized for release by the contributing agency (for convictions, outstanding charges, and warrants only – does not include local police information)	✓ All information must be confirmed and authorized (for release by the contributing agency (for convictions, outstanding charges, and warrants only – does not include local police information)	✓ All information must be confirmed and authorized for release by the contributing agency	✓ All information must be confirmed and authorized for release by the contributing agency
Mental Health Information	û	û	Do not disclose apprehensions under the Mental Health Act or Suicide attempts. If applicant had police contact involving the threat or actual use of violence directed at <i>other individuals</i> , release the information without disclosing mental health status.	Do not disclose apprehensions under the Mental Health Act or Suicide attempts. If applicant had police contact involving the threat or actual use of violence directed at <i>other individuals</i> , release the information without disclosing mental health status.
Police Information from Indices Query	û	û	Any adverse contact with police may be released until the retention period has been met. For example - roles of Suspect, Suspect Chargeable, Accused, and Recommended Charges. Non-accusatory roles are not released except under exceptional circumstances. For example – roles of Victim, Witness or Subject of Complaint. Intelligence files are only released if approval is received from the investigating officer. Retention periods commence on the clearance date of the file (not the date of the offence).	Any adverse contact with police may be released until the retention period has been met, except if extrajudicial <i>measures</i> were taken (including no action, warning or police caution, referral to a community program. Incidents that resulted in extrajudicial <i>sanctions</i> (following Crown assessment that charges could have been laid) may be released for 2 years from the date the sanction was agreed to. Non-accusatory roles are not released except under exceptional circumstances. Intelligence files are only released if approval is received from the investigating officer. Retention periods commence on the clearance date of the file (not the date of the offence).

British Columbia Guideline For Police Information Checks

Record Type	Police Information Check ADULT	Police Information Check YOUTH	Police Vulnerable Sector Check ADULT	Police Vulnerable Sector Check YOUTH
Police Information from Other Police Agencies	Query PIP and FIP on all applicants. NOTE: If applicant has resided in another jurisdiction in the past 5 years, contact police agency directly via CPIC. Non-responding agencies must be noted.	Query PIP and FIP on all applicants. NOTE: If applicant has resided in another jurisdiction in the past 5 years, contact police agency directly via CPIC. Non-responding agencies must be noted.	Query PIP and FIP on all applicants. NOTE: If applicant has resided in another jurisdiction in the past 5 years, contact police agency directly via CPIC. Non-responding agencies must be noted.	Query PIP and FIP on all applicants. NOTE: If applicant has resided in another jurisdiction in the past 5 years, contact police agency directly via CPIC. Non-responding agencies must be noted.
SIP Special Interest Police	û	û	SIP Information is not released, but can be used as a tool to identify reports/incidents held by other police agencies.	SIP Information is not released, but can be used as a tool to identify reports/incidents held by other police agencies.

Dispositions	Police Information Check ADULT	Police Information Check YOUTH	Police Vulnerable Sector Check ADULT	Police Vulnerable Sector Check YOUTH
Absolute Discharge (Prior to July 1992, this information was not automatically purged from the CRII. Therefore, it may be visible, but should not be released)	Shall not be self-declared and therefore not released from CRII. May be released from own local files without (self) declaration for 1 year. The information may be released from another police service's local file, for 1 year, with permission.	Shall not be self-declared and therefore not released from CRII. May be released from own local files for 1 year after disposition is rendered.	Shall not be self-declared and therefore not released from CRII. May be released from own local files without (self) declaration for 1 year. The information may be released from another police service's local file, for 1 year, with permission.	Shall not be self-declared and therefore not released from CRII. May be released from own local files for 1 year after disposition is rendered.
Acquittal / Not Guilty	û	û	Release from local files until retention period is met.	Release from local files until retention period is met.
Conditional Discharge (Prior to July 1992, this information was not automatically purged from the CRII. Therefore, it may be visible but should not be released)	Shall not be self-declared and therefore not released from CRII. May be released from own local files without (self) declaration for 3 years. The information may be released from another police service's local file, for 3 years, with permission.	Shall not be self-declared and therefore not released from CRII. May be released from own local files for 3 years after disposition is rendered.	Shall not be self-declared and therefore not released from CRII. May be released from own local files without (self) declaration for 3 years. The information may be released from another police service's local file, for 3 years, with permission.	Shall not be self-declared and therefore not released from CRII. May be released from own local files for 3 years after disposition is rendered.

Dispositions	Police Information Check ADULT	Police Information Check YOUTH	Police Vulnerable Sector Check ADULT	Police Vulnerable Sector Check YOUTH
Convictions (Indictable/Dual), Suspended Sentence OR Findings of Guilt Not Including Discharges	All released from CRII if self-declared or confirmed by fingerprints. All may be released from own local files without (self) declaration.	Shall not be self-declared and therefore not released from CRII. From local database – 5 years for indictable offences after completion of most recent sentence.	All released from CRII if self-declared or confirmed by fingerprints. All may be released from own local files without (self) declaration.	Shall not be self-declared and therefore not released from CRII. From local database – 5 years for indictable offences after completion of most recent sentence.
Convictions (Summary), Suspended Sentence OR Findings of Guilt Not Including Discharges	Not available on the CR therefore (self) declaration is not required. All Released for the retention period of the file.	Shall not be self-declared and therefore not released from CRII. Released for 3 years after the sentence has been completed.	Not available on the CR therefore (self) declaration is not required. All may be released from own local files without (self) declaration.	Shall not be self-declared and therefore not released from CRII. If a young person has been found guilty of a summary offence, the information should be released from your own local database on a PIC or PIC-VS for a period of three years after the youth sentence has been completed. See Section 119(2) (g) of the YCJA
Dismissed	û	û	Release from local files until retention period is met.	Release from local files for a period of 2 months.
Extrajudicial Measures (Before or after court) YOUTH Only	Not Applicable	û	Not Applicable	û
Finding of Guilt with Reprimand YOUTH Only	Not Applicable	û	Not Applicable	May be released from local files for a period of 2 months.
Not Criminally Responsible (NCR)	û	û	Release from local files until retention period is met.	Release from local files until retention period is met.
Prohibition Orders – Criminal Code	✓	✓	✓	✓
Prohibition Orders – Non-Criminal (Driving)	û	û	û	û
Provincial Offences	û	û	May be released if a person was charged by way of an RCC, until the retention period has been met.	May be released if a person was charged by way of an RCC, until the retention period has been met.
Record Suspensions (Pardons)	û	Not Applicable	Released If Approved By Minister of Public Safety	Not Applicable

British Columbia Guideline For Police Information Checks

Dispositions	Police Information Check ADULT	Police Information Check YOUTH	Police Vulnerable Sector Check ADULT	Police Vulnerable Sector Check YOUTH
Stay of Proceedings	û	û	Release from local files until retention period is met.	Release from local files for a period of 1 year.
Withdrawn	û	û	Release from local files until retention period is met.	Release from local files for a period of 2 months.
Diversion Alternative Measures	û	û	Release from local files until retention period is met with no reference to the court.	û
Withdrawn – Extrajudicial Sanctions YOUTH Only	Not Applicable	û	Not Applicable	May be released from local files for two years after the youth consented to the sanction.
Expired Peace Bonds (Also See Current Judicial Orders)	û	û	Release from local files until retention period is met.	Release from local files until retention period is met.

Appendix B: PRIME Role Codes

Code #	Translation	Definition (greyed role codes are not subject to release in a Police Information Check)
1	Other	Non Accusatory
2	Charged	Charges have been approved by Crown Counsel
3	Complainant	A subject requesting the Services of a law enforcement body
4	EDP	Emotional disturbed person - a person who appears to be mentally unstable and who might use a threat to an investigator/himself or others **MAY OR MAY NOT BE DISCLOSE ABLE - Requires follow-up**
11	Suspect	A subject that is believed to be involved in a commission of a crime or statute breach but charges have not been laid
10	Street Check	A mandatory code for street check subjects, indicates that the subject came to the attention of a law enforcement agency as a result of a self-generated check. Not due to an investigation or occurrence.
12	Victim	A subject that has suffered as a result of the commission of an offence or the breach of a statute (all 1000 UCR series)
14	Witness	A subject who is observed or has some knowledge relating to a crime or statute breach, or incident
34	Suspect Chargeable	A subject for whom grounds exist to support the recommendation of a charge but police choose against this course of action.
39	Recommend Charges	use of this code is mandatory when a police agency has submitted a report to Crown Counsel who has either not yet approved or not approved charges. Once charges are approved this role code is changed to "charged" .
92	Subject of Complaint	Non Accusatory, subject that is being complained about or a subject in relation to whom a call for service was received.
102	Youth Charged	An Information or Summary offence Ticket has been laid or issued against the subject by the unit or agency with jurisdiction
139	Youth Recommended Charges	Mandatory when the agency has submitted a RCC against a juvenile subject, but Crown has either not yet laid charges or has not approved charges. (Some agencies elect to use "charged" in the first instance, and then change to "charges recommended" if Crown Counsel does not approve charges)
134	Youth Suspect Chargeable	A subject for which grounds exist to support the recommendation of a charge but police choose against this course of action
111	Youth Suspect	A subject that is believed to be involved in the commission of a crime or statute breach but charges have not been laid.
112	Youth Victim	A subject that has suffered as a result of the commission of an offence or the breach of a statute (all 1000 UCR series)
202	Youth Non-Disclosure	System generated, not to be disclosed
239	Youth Non-Disclosure	System generated, not to be disclosed

Appendix C: Applicant Fact Sheet

An employer or a volunteer organization has requested that you obtain a Police Information Check, as part of determining your suitability for employment or volunteer duties, as well as, possibly, because the position is responsible for children or vulnerable persons. At your request and with your permission, the “insert name” Police Agency (the Agency) will complete a Police Information Check about you for employment or volunteer duties.

The organization/employer you are applying to is expected to:

- ↑ have completed an initial review of your suitability and to be considering you for employment or a volunteer opportunity; and
- ↑ understands its obligation under the Human Rights Code with respect to evaluation, hiring and training volunteers or employees and what constitutes a bona fide reason for refusing to hire any individual or volunteer.

In order for us to complete the Police Information Check, you must reside within the jurisdiction of this police agency, and have signed the required consent form.

The “insert name” Police Agency offers two types of record checks:

1. Police Information Check (PIC)
2. Police Information Check with Vulnerable Sector Screening (PIC-VS)

Police Information Check (PIC)

This check is intended for applicants who are seeking volunteer and/or employment with agencies requiring a review of warrants, outstanding charges and convictions about an applicant. The organization/employer has determined that a search of record suspensions (formally known as Pardons) is not required; therefore, this information check is NOT intended for applicants who are seeking volunteer and/or employment with vulnerable persons.

A Police Information Check will include:

- a) Criminal convictions from CPIC and/or local databases.
- b) Summary convictions, when identified.
- c) Findings of Guilt under the Youth Criminal Justice Act within the applicable disclosure period.
- d) Outstanding entries, such as charges and warrants, judicial orders, Peace Bonds, Probation and Prohibition Orders. As per CPIC policy, information obtained from the Investigative Databank must be confirmed and authorized for release by the contributing agency.
- e) Absolute and conditional discharges for 1 or 3 years respectively.

A Police Information Check will NOT include:

- a) Convictions where a record suspension has been granted.
- b) Convictions under provincial statutes.
- c) Local police contact.
- d) Traffic violations, including roadside suspensions.
- e) Special Interest Police (SIP) category of CPIC.
- f) Family Court restraining orders.
- g) Foreign information.
- h) A Vulnerable Sector (VS) Query to ascertain if the applicant has been convicted of and granted a record suspension for any of the sexual offences that are listed in the schedule to the Criminal Records Act (CRA).
- i) Any reference to incidents involving mental health contact.
- j) Diversions will not be released as police contact and no reference to the occurrence is permitted (CCS.717.4).
- k) Youth Criminal Justice Act (YCJA) information beyond applicable disclosure period.
- l) Any reference to contagious diseases.
- m) Dispositions including, but not limited to, Stay of Proceedings, Withdrawn, Dismissed, Not Criminally Responsible by Reason of Mental Disorder, Acquittals and Not Guilty findings.

Police Information Check with Vulnerable Sector Screening (PIC-VS)

This check is restricted to applicants seeking employment and/or volunteering in a position of authority or trust relative to vulnerable persons in Canada only. With your consent, a query of sex offences for which a record suspension (formerly known as a Pardon) has been granted will be conducted in compliance with the *Criminal Records Act (CRA)*.

Police Information Check with Vulnerable Sector Screening will include:

- a) Criminal convictions (summary and indictable) from CPIC and/or local databases.
- b) Outstanding judicial orders, such as charges and warrants, judicial orders, Peace Bonds, Probation and Prohibition Orders. As per CPIC policy, information obtained from the Investigative Databank must be confirmed and authorized for release by the contributing agency.
- c) Absolute and conditional discharges for 1 or 3 years respectively.
- d) Charges recommended and/or processed by other means.

- e) Dispositions listed in the CPIC Identification Databank or CRII under non-convictions including, but not limited to, withdrawn, dismissed, and cases of not criminally responsible by reason of mental disorder.
- f) Any additional information recorded in police databases documenting the applicant to have been a suspect in an offence (whether or not charged), subject to provincial retention periods specific to the offence type.
- g) Adverse contact involving the threat or actual use of violence directed at other individuals, regardless of, but without disclosing, mental health status.
- h) As authorized for release by the Minister of Public Safety all record suspension criminal convictions, including non sex offences, identified as a result of a VS query.

PIC with Vulnerable Sector Screening will NOT include:

- a) Convictions where a record suspension has been granted (except for sexual offences)
- b) Convictions under provincial statutes unless under exceptional circumstances.
- c) Traffic violations, including roadside suspensions.
- d) Suspect information that would hinder an ongoing investigation or where the suspect has not been spoken to may result in the record check being delayed or terminated.
- e) Youth Criminal Justice Act (YCJA) information beyond applicable disclosure period.
- f) Special Interest Police (SIP) category of CPIC.
- g) Information gathered outside formal occurrence reports, e.g., street checks or CAD, except under exceptional circumstances.
- h) Any reference to contagious diseases.
- i) Victim/Complainant information unless under exceptional circumstances.
- j) Foreign information for applicants who have resided outside of Canada.
- k) Mental Health Act information.

Self-Declaration

Self-declaration of a criminal record is a process where you may declare your adult criminal record convictions to the police agency. This may allow the police agency to assess the accuracy of your criminal record information without taking your fingerprints and without the delay formal fingerprinting would cause.

Do NOT declare:

- ↑ A conviction for which you have received a record suspension (formerly known as a pardon).
- ↑ A finding of guilt when you were a “young person”.
- ↑ Absolute or Conditional Discharges.

↑ Any offences where you were not convicted (i.e. stays of proceedings, dismissed charges)

↑ Provincial or municipal offences.

↑ Any charges dealt with outside of Canada.

The police agency will verify if the information matches a criminal record contained within the RCMP National Repository of Criminal Records. If the police agency is not satisfied that your declared criminal record information is a match to a criminal record held at the repository, fingerprints are required.

Requirement for Fingerprints

Criminal Record: If the police agency is not satisfied that your self-declaration is a match to a criminal record held at the RCMP National Repository of Criminal Records, your fingerprints must be submitted to the RCMP.

Vulnerable Sector: If you are applying to work in a paid or volunteer position where you will be responsible for children or vulnerable persons you may be required to submit fingerprints to verify whether you have received a record suspension for a sexual offence contained within the RCMP National Repository of Criminal Records.

Release of Completed Police Information Check

Police Information Check

The police agency will provide the results of a completed Police Information Check *only to you, the applicant*.

It is your decision to discuss the results of a Police Information Check with the organization/employer where you want to work or volunteer. The role of the police agency is to provide you with the results of the Police Information Check. The hiring organization is responsible to determine your suitability for the position.

If you have questions regarding the results of your PIC or PIC-VS you should contact the police agency that conducted the check for further information and directions.

Police Information Check with Vulnerable Sector Screening

The police agency will complete a Vulnerable Sector Check based on your name and date of birth. If no record is found a completed Police Information Check with Vulnerable Sector Screening will be provided *only to you, the applicant*.

If the Vulnerable Sector Search is inconclusive a fingerprint based search will be required. If the RCMP confirms that you have a record suspension for a sex offence, the information will be forwarded to the Minister of Public Safety to authorize disclosure of all or part of the information contained in your file. When the information is authorized for disclosure by the Minister, the criminal record associated with your fingerprints will be returned to the police agency and will include the sexual offence information for which you received a record suspension. At this point the police agency will be required to obtain

your consent in writing for disclosure of the record(s). When you have signed the form giving consent to release the record(s) the police agency must forward the information to the requesting agency (employer or volunteer agency).

If you choose not to disclose your record(s), the police agency must contact the requesting agency in writing and advise that they are unable to complete the Police Vulnerable Sector Check.

Reconsideration Request Process

If you wish to request reconsideration of any information disclosed on the Police Information Check you may apply in writing to (Name & address of Agency).

You may also refer to the (name of Police Agency) website at (website address) for further information regarding the Police Information Check process.

Appendix D:

Organization/Employer Fact Sheet

Police Information Checks for Employment or Volunteer Opportunities

Police Record Checks are performed only with the written consent of the applicant for employment or a volunteer position, and only by the police agency for the area where the applicant lives. The applicant must attend in person at the police agency to request the police information check.

The organization/employer plays an integral role in the initial stages of the hiring process. Before an individual applies for a Police Record Check the organization/employers should:

- a) Complete an initial review for suitability and be considering the individual for an employment or volunteer opportunity.
- b) Understand its obligation under the Human Rights Code with respect to evaluation, hiring and training volunteers or employees and what constitutes a bona fide reason for refusing to hire any individual or volunteer.
- c) Understand the legal rules concerning the collection, use, security and any further disclosure of the information obtained through a police information check, as contained in the Personal Information Protection Act (for businesses and non-profit organizations) and in the Freedom of Information & Protection of Privacy Act (for public bodies).
- d) Determine whether a Police Vulnerable Sector Check is required, as this type of information check is designed to assist the organization/employer in determining the suitability of potential employment/volunteer candidates whose duties will include responsibility for the well-being of persons who, because of their age, disability or other circumstances are at a greater risk than the general population.

For further information on selecting employees or volunteers refer to Volunteer Canada 10 step guideline at <http://volunteer.ca/content/screening-10-steps>

By performing a Police Record Check, “insert name” Police Agency (the Agency) is in no way making a recommendation as to the suitability of the applicant for the position, nor should the agency consider the existence of police information to mean a compulsory disqualification of the individual. It is important to note that information contained within a Police Information Check is based upon information provided by the applicant and a police agency cannot guarantee it will identify all information pertaining to the individual.

The “insert name” Police Agency provides two types of Police Information Checks:

1. Police Information Check (PIC)
2. Police Information Check with Vulnerable Sector Screening (PIC-VS)

Police Information Check (PIC)

This check is intended for applicants who are seeking volunteer and/or employment with agencies requiring a review of warrants, outstanding charges and convictions about an applicant. The organization/employer has determined that a search of record suspensions (formally known as Pardons) is not required; therefore, this information check is NOT intended for applicants who are seeking volunteer and/or employment with vulnerable persons.

A Police Information Check will include:

- a) Criminal convictions from CPIC and/or local databases.
- b) Summary convictions when identified.
- c) Findings of Guilt under the Youth Criminal Justice Act within the applicable disclosure period.
- d) Outstanding entries, such as charges and warrants, judicial orders, Peace Bonds, Probation and Prohibition Orders. As per CPIC policy, information obtained from the Investigative Databank must be confirmed and authorized for release by the contributing agency.
- e) Absolute and conditional discharges for 1 or 3 years respectively.

A Police Information Check will NOT include:

- a) Convictions where a record suspension has been granted.
- b) Convictions under provincial statutes.
- c) Local police contact.
- d) Traffic violations, including roadside suspensions.
- e) Special Interest Police (SIP) category of CPIC.
- f) Family Court restraining orders.
- g) Foreign information.
- h) A Vulnerable Sector (VS) Query to ascertain if the applicant has been convicted of and granted a record suspension for any of the sexual offences that are listed in the schedule to the Criminal Records Act (CRA).
- i) Any reference to incidents involving mental health contact.
- j) Diversions will not be released as police contact and no reference to the occurrence is permitted (CCS. 717.4).
- k) Youth Criminal Justice Act (YCJA) information beyond applicable disclosure period.
- l) Any reference to contagious diseases.
- m) Dispositions including, but not limited to, Stay of Proceedings, Withdrawn, Dismissed, Not Criminally Responsible by Reason of Mental Disorder, Acquittals and Not Guilty findings.

Police Information Check with Vulnerable Sector Screening (PIC-VS)

This check is restricted to applicants seeking employment and/or volunteering in a position of authority or trust relative to vulnerable persons *in Canada only*. With your consent, a query of sex offences for which a record suspension (formerly known as a Pardon) has been granted will be conducted in compliance with the *Criminal Records Act (CRA)*.

Police Information Check with Vulnerable Sector Screening will include:

- a) Criminal convictions (summary and indictable) from CPIC and/or local databases.
- b) Outstanding judicial orders, such as charges and warrants, judicial orders, Peace Bonds, Probation and Prohibition Orders. As per CPIC policy, information obtained from the Investigative Databank must be confirmed and authorized for release by the contributing agency.
- c) Absolute and conditional discharges for 1 or 3 years respectively.
- d) Charges recommended and/or processed by other means
- e) Dispositions listed in the CPIC Identification Databank or CRII under non-convictions including, but not limited to, withdrawn, dismissed, and cases of not criminally responsible by reason of mental disorder.
- f) Any additional information recorded in police databases documenting the applicant to have been a suspect in an offence (whether or not charged), subject to provincial retention periods specific to the offence type.
- g) Adverse contact involving the threat or actual use of violence directed at other individuals, regardless of, but without disclosing, mental health status.
- h) As authorized for release by the Minister of Public Safety all record suspension criminal convictions, including non sex offences, identified as a result of a VS query.

PIC with Vulnerable Sector Screening will NOT include:

- a) Convictions where a record suspension has been granted (except for sexual offences)
- b) Convictions under provincial statutes unless under exceptional circumstances.
- c) Traffic violations, including roadside suspensions.
- d) Suspect information that would hinder an ongoing investigation or where the suspect has not been spoken to may result in the record check being delayed or terminated.
- e) Youth Criminal Justice Act (YCJA) information beyond applicable disclosure period.
- f) Special Interest Police (SIP) category of CPIC.
- g) Information gathered outside formal occurrence reports, e.g., street checks or CAD, except under exceptional circumstances.
- h) Any reference to contagious diseases.

- i) Victim/Complainant information unless under exceptional circumstances.
- j) Foreign information for applicants who have resided outside of Canada.
- k) Mental Health Act information.

Self-Declaration

Self-declaration of a criminal record is a process where the applicant may declare his/her adult criminal record convictions to the police agency. This may allow the police agency to assess the accuracy of the applicant's criminal record information without taking fingerprints and without the delay that a fingerprint comparison would cause.

Applicants are NOT required to declare:

- ↑ A conviction for which the applicant has received a record suspension.
- ↑ A finding of guilt when the applicant was a "young person" under the YCJA.
- ↑ Absolute or Conditional Discharges.
- ↑ Any offences for which the applicant was not convicted, e.g., stay of proceedings or dismissed charges.
- ↑ Provincial or municipal offences.
- ↑ Any charges dealt with outside of Canada.

The police agency will confirm if the information matches a criminal record contained within the RCMP National Repository of Criminal Records. If the police agency is not satisfied that the applicants declared criminal record information is a match to a Criminal Record held at the repository, fingerprints are required.

Requirement for Fingerprints

Criminal Record:

If the police agency is not satisfied that the applicants self declaration is a match to a criminal record held at the Criminal Record Repository, fingerprints must be submitted to the RCMP.

Vulnerable Sector:

If the applicant is being considered to work in a paid or volunteer position where they will be in a position responsible for children or vulnerable individuals they may be required to submit fingerprints to verify whether there is a criminal record including the existence of any sex offences for which they received a record suspension contained within the RCMP National Criminal Records Repository.

Release of Completed Police Information Check

Police Information Check

The police agency will provide the results of a completed Police Information Check to the applicant only.

It is the choice of the applicant to decide whether he/she wants to discuss the results of the Police Information Check with the requesting organization/employer. The role of the police agency is to provide the applicant with the results of the Police Information Check. The hiring organization/employer is responsible for determining the suitability of the applicant for the position. The result of any Police Information Check is just one component of the information available to and evaluated by the organization/employer.

Police Information Check with Vulnerable Sector

The police agency will complete a Vulnerable Sector Check based on the applicant's name and date of birth. If no record is found, a completed Police Information Check with Vulnerable Sector will be provided to the applicant.

If the Vulnerable Sector Search is inconclusive a fingerprint based search will be required. If the RCMP confirms that the applicant has a record suspension for a sex offence, the information will be forwarded to the Minister of Public Safety to authorize disclosure of all or part of the information contained in the file. When the information is authorized for disclosure by the Minister, the criminal record associated with the applicant's fingerprints will be returned to the police agency and will include the record suspension sexual offence information. At this point the police agency will be required to obtain the applicant's consent in writing for disclosure of the record(s). When the applicant has signed the form giving consent to release the record(s) the police agency must forward the information to the requesting organization/employer.

If the applicant chooses not to disclose their record(s) the police agency must contact the requesting organization/employer in writing indicating that they were unable to complete the Police Vulnerable Sector Check.

You may also refer to the (name of Police Agency) website at (website address) for further information regarding the Police Check process.

Appendix E: Police Information Check & Police Information Check Vulnerable Sector Application, Waiver, Release and Consents

XXXXX Police Department

Police Information Check

XXXX Police Use Only

Log:

Receipt:

Received at:

IDENTIFICATION – one form must be photo ID (office use only).

Type of ID Produced:	Number:
Type of ID Produced:	Number:

INSTRUCTIONS FOR COMPLETION

(PERSONAL INFORMATION ON THIS FORM IS COLLECTED UNDER THE AUTHORITY OF THE BC FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT & FEDERAL PRIVACY ACT)

Please complete clearly in ink

You must apply in person at the Police Agency in the jurisdiction you reside. At the time of application you must present:
 Any applicable fee (see website for costs and payment options).
 One piece of current, government-issued photo identification and one piece of identification verifying name and date of birth.
 If you are unable to provide proper identification the police agency cannot complete your check.

Your Police Information Check will review all available law enforcement systems, including any local police records. This check will NOT include: overseas or US records, traffic tickets, or municipal bylaw offences.

The results of this check will not be forwarded to a third party
 (with the exception of confirmed positive Vulnerable Sector responses, or if a "Duty to Warn" arises).

PART I – PERSONAL INFORMATION (COMPLETED BY APPLICANT)				
LAST NAME	FIRST NAME	MIDDLE NAME(S)		
PREVIOUS NAMES (including name changes and birth/maiden name)			SEX (circle one) M F	
DATE OF BIRTH (YYYY/MM/DD)	PLACE OF BIRTH:			
ADDRESS (Apartment, street # and name)	CITY	PROV	POSTAL CODE	
PHONE NUMBER (residence)	PHONE NUMBER (cell)			
PREVIOUS ADDRESS (LIST ALL ADDRESSES WITHIN THE LAST FIVE YEARS)			*Check Completed (office use only)	
STREET NAME: _____	CITY: _____	PROVINCE: _____	<input type="checkbox"/> yes	<input type="checkbox"/> no
STREET NAME: _____	CITY: _____	PROVINCE: _____	<input type="checkbox"/> yes	<input type="checkbox"/> no
STREET NAME: _____	CITY: _____	PROVINCE: _____	<input type="checkbox"/> yes	<input type="checkbox"/> no
STREET NAME: _____	CITY: _____	PROVINCE: _____	<input type="checkbox"/> yes	<input type="checkbox"/> no
STREET NAME: _____	CITY: _____	PROVINCE: _____	<input type="checkbox"/> yes	<input type="checkbox"/> no

REASON FOR APPLICATION (check appropriate): ☐ Volunteer (attach letter) ☐ -Employment ☐ Other (specify below)

Key Contact Name: _____

Volunteer Agency/ Employer Name: _____

Volunteer Agency/ Employer Address and Phone Number: _____

IS YOUR REQUEST RELATED TO WORK/VOLUNTEERING WITH VULNERABLE PERSONS: ☐ YES ☐ NO

(if yes – please complete Vulnerable Sector Search Consent FORM 1 on page 2)

Applicant Name	Applicant DOB
<u>VULNERABLE SECTOR APPLICANTS:</u>	
FORM 1 – CONSENT FOR A CRIMINAL RECORD CHECK FOR A SEXUAL OFFENCE FOR WHICH A PARDON HAS BEEN GRANTED OR ISSUED	
<p>This form is to be used by a person applying for a position with a person or organization responsible for the well-being of one or more children or vulnerable persons, if the position is a position of authority or trust relative to those children or vulnerable persons and the applicant wishes to consent to a search being made in criminal conviction records to determine if the applicant has been convicted of a sexual offence listed in the schedule to the Criminal Records Act and has been pardoned.</p>	
Reason for Consent:	
<p>I am an applicant for a paid or volunteer position with a person or organization responsible for the well-being of one or more children or vulnerable person(s).</p>	
<p>Description of the paid or volunteer position (<i>what you will be doing</i>): _____</p>	
<p>Provide details regarding the children or vulnerable person(s) (<i>what ages, type of client(s) you will be in authority over</i>): _____</p>	
<p>Consent: I consent to a search being made in the automated criminal records retrieval system maintained by the Royal Canadian Mounted Police to determine if I have been convicted of, and been granted a pardon for, any of the sexual offences that are listed in the schedule to the Criminal Records Act. I understand that as a result of giving this consent, if I am suspected of being the person named in a criminal record for one of the sexual offences listed in the schedule to the Criminal Records Act in respect of which a pardon was granted or issued, that record may be provided by the Commissioner of the Royal Canadian Mounted Police to the Minister of Public Safety of Canada, who may then disclose all or part of the information contained in that record to a police force or other authorized body. That police force or authorized body will then disclose the information to me. If I further consent in writing to disclosure of that information to the person or organization referred to above that requested the verification, that information will be disclosed to that person or organization.</p>	
_____ Signature of Applicant	_____ Date Signed
DECLARATION OF A CRIMINAL RECORD (if applicable) – Completed by Applicant	
<p>By declaring any offences of which you have been convicted, your criminal convictions record can be confirmed without needing to submit your fingerprints for verification of your identity and the processing delay that this causes.</p> <ul style="list-style-type: none"> Please list below all offences of which a judge has convicted you (whether indictable or summary) and specifically identify the offence, date you were convicted, and place where the offence was committed. Do Not disclose convictions for which you have received a pardon pursuant to the <i>Criminal Records Act</i>, or charges that were dismissed, stayed, or resulted in absolute or conditional discharges. Do Not disclose offence convictions where you were found guilty of an offence committed while you were a “young person” (younger than eighteen years), pursuant to the <i>Youth Criminal Justice Act</i>. 	
Date of Conviction	Nature of Offence
Location/Jurisdiction	

Signature of Applicant

Date signed

Applicant Name	Applicant DOB
----------------	---------------

SEARCH AND DISCLOSURE CONSENT, AND LIABILITY RELEASE

I request and consent to the _____ POLICE DEPARTMENT and its employees searching any policing agency or court databases, based on the information I have provided, in order to locate any records and information in which I am referred to, and to report, by way of this form, any formal criminal records or pending charges that I am the subject of. If I have indicated that I will be working with the vulnerable sector, I also request and consent to the reporting of any documented adverse contact with police, any incident in which no charges were laid, or any matter regulated by provincial statutes, that I am the subject of. I understand that records may continue to exist even if they are no longer listed in particular records database indices.

I understand that information collected as a result of this Police Information Check will only be released **directly to me and not to any third party**; however, I specifically intend to provide the reported information to the employer or volunteer agency that I have listed. I understand that they alone, and not the police, will determine the impact of any reported search results, on whether I obtain the position for which I am being considered. I understand that the accuracy of the reported information, to be disclosed to me, is not and cannot be guaranteed, and may include errors or omissions.

By my signature below, and for and in consideration of this Police Information Check being completed for me, the receipt and sufficiency of which I hereby acknowledged, I agree not to bring any legal actions, claims or demands, for losses or damages, including indirect or consequential, that I might sustain by reason of the Police Information Check being performed for me, against the Municipality / Corporation of _____, its associated Police Board and any employees thereof, and to release them each from any and all liability and any actions, claims or demands, even if arising from their negligence or even gross negligence.

I have read and understood this form, and in particular this section, and by signing below I am consenting to the above terms. By signing, I also certify that the information that I have provided is true and correct to the best of my knowledge and belief.

Signature of Applicant

Date Signed

*******FOR OFFICE USE ONLY*******

<u>QUERY TYPE</u>	<u>Queried by:</u>	<u>Negative</u>	<u>Attached</u>	<u>Date</u>
<u>CPIC</u>				
<u>PRIME</u>				
<u>PIP/LEIP</u>				
<u>JUSTIN</u>				
<u>VS – FP REQ.</u>				

NOTES (office use only):

XXXXX Police Department Police Information Check

(The completed application pages to this form have been retained by the issuing agency.)

This is page 1 of 3 pages making up the complete results form; an embossed XXXXX Police Department seal is required on all pages.

Applicant Name	Applicant DOB
----------------	---------------

Position and Volunteer Agency, Group or Employer:

RESULTS OF CRIMINAL CONVICTION CHECK

Records of criminal conviction for which a record suspension (formally pardon) has not been granted, obtainable through the Canadian Police Information Centre (CPIC) National Repository for Criminal Records Identification Data Bank.

RESULTS: CRIMINAL RECORD CHECK INFORMATION IS BASED ON NAME AND DATE OF BIRTH ONLY

■ NEGATIVE

Based solely on the name(s) and date of birth provided and the criminal record information declared by the applicant a search of the RCMP National Repository of Criminal Records **did not identify any records** for a person with the name(s) and date of birth of the applicant. **Positive identification that a criminal record may or may not exist at the RCMP National Repository for Criminal Records can only be confirmed by fingerprint comparison.** Not all offences are reported to the RCMP National Repository of Criminal Records. A local police indices check may or may not reveal criminal record convictions that have not been reported.

■ INCOMPLETE

Based solely on the name(s) and date of birth provided and the criminal record information declared by the applicant a search of the RCMP National Repository of Criminal Records **could not be completed.** In order to complete the request, the applicant is required to have fingerprints submitted to the RCMP National Repository of Criminal Records by an authorized police service or accredited private fingerprint company. **Positive identification that a criminal record may or may not exist at the RCMP National Repository for Criminal Records can only be confirmed by fingerprint comparison.** Not all offences are reported to the RCMP National Repository of Criminal Records. A local police indices check may or may not reveal criminal record convictions that have not been reported.

■ POSSIBLE MATCH - *SEE LIST BELOW OF SELF DECLARED CONVICTIONS*

Based solely on the name(s) and date of birth provided and the criminal record information declared by the applicant a search of the RCMP National Repository of Criminal Records **has resulted in a possible match to a registered criminal record.** **Positive identification that a criminal record may or may not exist at the RCMP National Repository for Criminal Records can only be confirmed by fingerprint comparison.** **The declared criminal record does not constitute a *certified* criminal record by the RCMP and may not contain all criminal record convictions.** Not all offences are reported to the RCMP National Repository of Criminal Records. A local police indices check may or may not reveal criminal record convictions that have not been reported.

BASED ON COMPARISON SEARCH WITH THE NATIONAL REPOSITORY OF CRIMINAL RECORDS:

■ NOT APPLICABLE – NO FINGERPRINT SEARCH CONDUCTED

■ NEGATIVE – CERTIFIES THAT OUR SEARCH DID NOT IDENTIFY ANY RECORDS ASSOCIATED WITH THE APPLICANT THAT MAY BE DISCLOSED IN ACCORDANCE WITH FEDERAL LAW.

■ MATCH – A SEARCH IDENTIFIED THAT THE FINGERPRINTS SUBMITTED BY THE APPLICANT WERE CERTIFIED AS IDENTICAL TO THE FINGERPRINTS REGISTERED IN THE REPOSITORY – SEE ATTACHED RECORD OF CONVICTIONS FROM RCMP OTTAWA.

DISCLOSURE OF CRIMINAL CONVICTIONS

DATE	OFFENCE	LOCATION

DELAYS MAY EXIST BETWEEN A CONVICTION BEING RENDERED IN COURT AND THE DETAILS BEING ACCESSIBLE ON THE RCMP NATIONAL REPOSITORY OF CRIMINAL RECORDS

Applicant Name		Applicant DOB	
RESULTS OF VULNERABLE SECTOR CHECK FOR SEXUAL OFFENCES WHERE A RECORD SUSPENSION WAS GRANTED			
<p><input type="checkbox"/> A vulnerable sector check was not requested.</p> <p><input type="checkbox"/> A vulnerable sector check for record suspensions (formerly pardons) for sexual offences has been conducted based on a name, gender and date of birth and was met with negative results.</p> <p><input type="checkbox"/> A vulnerable sector check was verified by fingerprints and name could not be associated to any records that may be disclosed in accordance with Federal Laws.</p> <p><input type="checkbox"/> A vulnerable sector check was verified by fingerprints and a record suspension (formerly pardon) for a sexual offence was disclosed to the requesting employer/agency as per Form 2 Consent.</p> <p><input type="checkbox"/> A vulnerable sector check was requested but can't be processed as the hiring agency is outside Canada.</p> <p><input type="checkbox"/> A vulnerable sector check was requested but is not applicable as the applicant is too young to have been granted a record suspension (formerly pardon)</p>			
RESULTS OF INVESTIGATIVE DATA BANK, COURT & LOCAL POLICE INDICES CHECK			
Outstanding Charges: Records of outstanding criminal charges and warrants which the police agency is aware of or are indicated within the Investigative Data Bank of CPIC or any other available police computer systems (e.g. BC PRIME, CPIC, JUSTIN and PIP)	<input type="checkbox"/> negative – no information that can be disclosed according to federal laws and policies	<input type="checkbox"/> see below disclosure	
Other Court Findings: Records of court findings that resulted in conditional or absolute discharges, stays of proceedings, Peace Bonds, or other dispositions or criminal information, as located on police computer systems (e.g. BC PRIME, CPIC, JUSTIN, PIP or other systems).	<input type="checkbox"/> negative – no information that can be disclosed according to federal laws and policies	<input type="checkbox"/> see page 3 disclosure	
Adverse Contact: Information located on police computer systems (e.g. BC PRIME, CPIC, JUSTIN and PIP) and through local indices checks, <u>including incidents where no charges were laid, adverse contact with police, or breaches of provincial statutes.</u>	<input type="checkbox"/> negative – no information that can be disclosed according to federal laws and policies <input type="checkbox"/> Search not permitted – applicant does not work with vulnerable sector	<input type="checkbox"/> see page 3 disclosure	
<p>****If the position involves operation of a motor vehicle, obtain a BC Driver's Abstract from the Superintendent of Motor Vehicles. This Police Information Check does <u>not</u> indicate traffic violation tickets, Motor Vehicle Act or Municipal Bylaw offences****</p>			
DISCLOSURE OF OUTSTANDING CHARGES/WARRANTS INFORMATION (if applicable)			
DATE	CHARGE & COURT FILE #	POLICE AGENCY	STATUS

Applicant Name				Applicant DOB	
DISCLOSURE OF CONVICTIONS NOT ON LISTED ON CPIC/CONDITIONAL/ABSOLUTE DISCHARGES/STAY OF PROCEEDINGS /PEACE BOND INFORMATION (if applicable)					
DATE	CHARGE & COURT FILE #	POLICE AGENCY	DISPOSITION/RESULT		
DISCLOSURE OF LOCAL POLICE INDICES (ONLY FOR VULNERABLE SECTOR APPLICANTS)					
POLICE AGENCY / FILE NUMBER	APPLICANT'S ROLE	OFFENCE	STATUS		

The XXXXXX Police Department will not be responsible for determining whether the results are relevant to any proposed employment or volunteer position. This determination must be made by the employer or volunteer organization in accordance with human rights legislation and employment law.

NOTE: These results do NOT include checks of U.S.A or other foreign jurisdiction records, traffic violations or municipal bylaw offences.

☐

This applicant has indicated addresses outside of Canada in the previous 5 years – the results of this check are for Canada only.

 XXXXXX Police Department
 Authorized Signature

 PIN Number

 Date



XXXXX Police Department seal

**Local Letter of Agreement between the Royal Canadian
Mounted Police "E" Division Informatics and the British
Columbia Ministry of Public Safety and Solicitor
General, Policing and Community Safety Security
Programs and Police Technology, Criminal Records
Review Program**

July 2009

**Local Letter of Agreement between the Royal Canadian Mounted Police
"E" Division Informatics and the British Columbia Ministry of Public Safety
and Solicitor General, Policing and Community Safety Security Programs
and Police Technology, Criminal Records Review Program**

Purpose:

Disclosure of Information to the British Columbia Ministry of Public Safety and Solicitor General, Policy and Community Safety Security Programs and Police Technology, Criminal Records Review Program by the RCMP Criminal Record Review Unit for the purpose of screening applicants pursuant to the Criminal Record Review Act and for the purpose of screening British Columbia Public Service applicants/employees where required pursuant to their employment.

References:


1. Criminal Record Review Act (Appendix "A").
2. Memorandum of Understanding between the Canadian Police Information Centre a National Police Service of the Royal Canadian Mounted Police and the British Columbia Ministry of Public Safety and Solicitor General, Policing and Community Safety Security Programs and Police Technology Division (Appendix "B").
3. Privacy Act, Paragraph 7 (Appendix "C").
4. Privacy Act, Paragraph 8(1)(Appendix "D").
5. Agreement Between the Minister of Justice and Attorney General and the Government of the Province of British Columbia. Dated, July 27, 1983 (Appendix "E").
6. Provincial Freedom of Information and Protection of Privacy Act (RSBC 1996), Chapter 165, Part 3, Division 6, 26 (Appendix "F").
7. Provincial Freedom of Information and Protection of Privacy Act (RSBC 1996), Chapter 165, Part 3, Division 6, 27(a) (Appendix "F").
8. Provincial Freedom of Information and Protection of Privacy Act (RSBC 1996), Chapter 165, Part 3, Division 6, 27(b) (Appendix "F").
9. British Columbia Criminal Records Review Program Form PSSG 06-005 (11/2006), "Consent to a Criminal Record Check" (Appendix "G").

10. RCMP Form 3584 (Appendix "H").
11. British Columbia Public Service Form, "Consent for Disclosure of Criminal Record Information" (Appendix "I").


Pursuant to the noted references, the Royal Canadian Mounted Police (RCMP) Criminal Record Review Unit will provide information to the British Columbia Ministry of Public Safety and Solicitor General, Policing and Community Safety Security Programs and Police Technology, Criminal Records Review Program. This information is being disclosed pursuant to Form PSSG 06-005 (11/2006) (Appendix "G"), RCMP Form 3584 (Appendix "H") or British Columbia Public Service Form, "Consent for Disclosure of Criminal Record Information" (Appendix "I") in which the applicant is providing informed written consent.

The RCMP shall have access to the processed PSSG 06-005 (11/2006), RCMP Form 3584 and British Columbia Public Service Form, "Consent for Disclosure of Criminal Record Information" for the purpose of verifying applicant consent and for audit purposes (IE: CPIC audits).

This agreement between the Royal Canadian Mounted Police and the Ministry of Public Safety and Solicitor General can be terminated at any time with ninety (90) days written notice by either party.


for Supt. M. Dunbar (AOL)
Royal Canadian Mounted Police
Pacific Region Informatics Officer

Date: 2009-07-16


Sam McLeod, Executive Director
Ministry of Public Safety and Solicitor General
Province of British Columbia

Date: 09-07-16



from one post to a substantially similar post provided the employee has been screened within the last 5 years.

- 1.6 Promotions: If a current BCCS employee that has never been screened is promoted within the organization, then that employee will be subject to the same security screening checks as a new employee. If a BCCS employee that has been screened is promoted within the organization, then that employee will be subject to the same security screening checks as per the 5 year re-check noted above.

2.0 PURPOSE AND SCOPE:

- 2.1 The purpose of this Letter of Agreement (LOA) is to set out the roles and responsibilities of the parties in relation to the type of enhanced security screening performed, disclosure of information, timelines and fees.

3.0 THE PARTIES AGREE AS FOLLOWS:

- 3.1 BCCS will request enhanced security screening services by emailing PSSO@gov.bc.ca. When requesting an initial check, BCCS agrees to provide PSSO with proof that there has been a conditional offer of employment. BCCS also agrees to provide PSSO with the job title and category for which the applicant will be employed. When requesting a re-check or a check upon promotion, BCCS will provide all relevant details regarding the employee.
- 3.2 PSSO agrees to obtain the signed consent form from the applicant.
- 3.3 PSSO agrees to conduct the enhanced security screening on an applicant as outlined in Part 4 below and provide a report, including reasons and recommendation on security screening clearance based strictly on the information PSSO collected. This information is provided for the review of BCCS which is responsible for making the final decision on whether or not to grant a security clearance to any individual undergoing enhanced security screening.
- 3.4 PSSO will provide the report to the Deputy Chief Coroner.
- 3.5 BCCS and PSSO acknowledge the necessity to respect the privacy of individuals and to protect the data available through CPIC. BCCS and PSSO shall comply with applicable provincial privacy laws.
- 3.6 The information released to BCCS shall be used only for the purpose of security screening an individual entering into a position of trust. The final hiring decision is made by BCCS, not PSSO. BCCS will destroy all copies of the PSSO's report once the hiring decision has been made.

4.0 FINANCIAL ARRANGEMENTS

- 4.1 BCCS shall be responsible for compensating PSSO at a cost per service as follows:

For new screening and re-checks for the following positions:

Chief Coroner, Deputy Chief Coroner, Coroners and Community Coroners:

- ✓ Level 4 police record check
- ✓ JUSTIN/CORNET check

Approved Fees by Level of Adjudication			
No Adjudication	Simple	Intermediate	Difficult
\$115	\$150	\$200	\$400

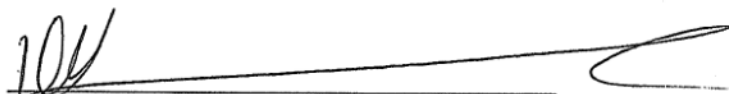
Report including recommendation to be returned to the Deputy Chief Coroner within approximately one week.

- 4.2 BCCS shall reimburse PSSO by a Journal Voucher, completed on a monthly basis in accordance with the fiscal year defined as April 1st to March 31st.

5.0 EFFECTIVE DATE OF AGREEMENT, AMENDMENTS, AND TERMINATION

- 5.1 This LOA was effective on April 8, 2015.
- 5.2 This newly amended LOA is effective January 1, 2019.
- 5.3 This LOA may be amended at any time by the written consent of the parties and any such amendments will be dated and signed by both parties and attached to this LOA as a schedule.

Signed on behalf of the Personnel Security Screening Office, the Ministry of Public Safety and Solicitor General



Dianne Small

A/Director, Security Screening

Security Programs Division, Ministry of Public Safety and Solicitor General

Date:

Sept 28/18

Signed on behalf of the Ministry of Public Safety and Solicitor General, BC Coroners Service



Vincent Stancato

Deputy Chief Coroner Investigations, the Ministry of Public Safety and Solicitor General

Date:

Oct 26/2018

**MINISTRY OF PUBLIC SAFETY AND SOLICITOR GENERAL
POLICING AND SECURITY BRANCH**

Proposed Business Model for the Criminal Record Review Unit (CRRU)

1.0 PURPOSE

The Criminal Records Review Unit requires a new service delivery model to provide long-term sustainable screening practices to eliminate operational risks and inefficiencies for the Province and the RCMP.

April 1, 2019 is identified as a hard deadline for the new model to be operationally ready.

PROPOSAL – A new provincial policing unit model within E-Division RCMP, comprised of Organized Crime Agency BC (OCABC) oversight positions as well as Provincial civilian support staff positions is to be operational effective April 1, 2019. The new model will continue to provide centralized service delivery of criminal records checks on behalf of the Security Programs Division (SPD), which includes BC public service checks, as well as checks done under the *Criminal Records Review Act*, *Security Services Act*, and the *Cannabis Control and Licensing Act*. Funding for the new model will be provided from the existing CRRU budget and examining the need for additional funds.

2.0 BACKGROUND

The *Criminal Records Review Act (CRRRA)*, implemented in 1995/96, requires all individuals working with children or vulnerable adults to obtain a criminal record check. Under the *CRRRA*, the Registrar (Executive Director, Security Programs Division) has statutory authority to carry out these checks. In addition to legislating criminal record checks, the *CRRRA* also provided an operational requirement for the centralization of criminal record checks to prevent downloading required checks to police departments.

The provincial government created and funded the Criminal Records Review Unit (CRRU) under the RCMP² to conduct criminal record checks for the purposes of the *CRRRA* and to support the authority of the Registrar.

To perform criminal record checks, access to information on police databases (CPIC and PRIME) is required, and this access is highly regulated. Canadian Police Information Centre (CPIC) policy states that, for the purpose of Vulnerable Sector checks, access to the CPIC database is restricted to Category I agencies (police only). SPD enters into contracts with retired RCMP members to make up the CRRU due to their legacy security clearance and experience with CPIC and PRIME databases.

² As identified in a 2009 Letter of Agreement between RCMP E Division Informatics and the Ministry of Public Safety and Solicitor General for the purpose of information sharing between the RCMP CRRU and the Community Safety Security Programs and Police Technology, CRRU Program (Appendix A).

In addition to checks performed under the *CRRRA*, the scope of CRRU work has expanded to include criminal record checks under the *Security Services Act (SSA)*, the *Body Armour Control Act*, and the *Armoured Vehicle and After-market Compartment Control Act, Cannabis Control and Licensing Act (CCLA)*, as well as checks for the Personnel Security Screening Office, pursuant to legislation, regulation, policy and/or agreement. The CRRU completes approximately 320,600 CPIC, PRIME, and PIRS/PROS checks per year for SPD programs. Depending on the program area and the applicable statutory authority, the type and depth of information reported back to SPD can vary considerably.

2.1 Current Model

The CRRU consists of seven retired RCMP members and one clerical staff member who are Direct Awarded contracts which are administered and funded by SPD. The contracts are renewed annually through a General Service Agreement (GSA) with the current GSA expiring on March 31, 2019. Despite being contracted by the Province, the CRRU is identified as an RCMP unit in the 2009 Letter of Agreement (LOA) between the RCMP and PSSG. The CRRU is based in Victoria, BC at RCMP E-Division Island District headquarters and is funded through the base delegation, subject to the 70/30 (provincial/federal) Provincial Policing Service Agreement cost share ratio.

In addition to accommodation, RCMP E-Division also provides network access and technical support at the provincial cost share ratio. Funding for supplies and equipment (computers, monitors, furniture, scanner, fridge, etc.) for the Unit is provided by SPD through reimbursement of expenses.

The CRRU formally reports to an RCMP Staff Sergeant Advisory NCO i/c, Information Management and Technology Operations, who is responsible for overseeing CRRU operations, however there is no on-site supervision. Functionally, the Unit reports to the Executive Director, Security Programs Division. SPD also provides the contractors with program specific training to ensure all CRRU activities fulfill SPD program requirements.

2.2 Risks and Limitations

Investigation and discussion around the current CRRU model identified several potential operational risks, as well as some inconsistencies with government procurement best practices, including:

- a) *Lack of supervision* – The unit lacks appropriate supervision required to ensure quality control and efficiency. Further, lack of supervision and standard procedures performing checks has led to inconsistent vetting practices between contractors and places the Province and RCMP at risk.
- b) *Authorization to access police data* – CPIC policy states that only Category I agencies may access CPIC data for the purposes of Civil Screening³. The current CRRU use the legacy security clearance of the retired RCMP members to access CPIC and PRIME data under RCMP E-Division; however no formal authorization has been provided.

³ CPIC Policy Manual, May 2015, Civil Screening refers to a Criminal Record Check and/or a Police Information Check for non-criminal justice purposes such as employment, reliability, security or accreditation purposes, and may also be required for volunteer activities such as vulnerable sector checks.

- c) *Sustainability* – There has been no documentation surrounding ownership of the assets purchased by the contractors and reimbursed by the Province. Further, the annual procurement process for the contractors is not sustainable.

The above concerns pose considerable risk to both the Province and RCMP, motivating the requirement for a new service delivery model. The option to maintain the status quo is not recommended as doing so would place unnecessary risk to the province.

3.0 PROPOSED SOLUTION

3.1 Proposed Model Overview

The new model will see the restructuring of a current provincial Unit within RCMP E-Division, which will maintain responsibility for the CRRU.

Re-establishment of the RCMP CRRU within a Category I police agency (the RCMP) will ensure alignment of police function and oversight within the policing environment as well as ongoing appropriate access to police databases to conduct the checks. To support these requirements, the CRRU will be established as a stand-alone RCMP Provincial Police Unit under the Combined Forces Special Enforcement Unit (CFSEU-BC) umbrella.

The proposed revision of the CRRU ensures that the unit continues to operate as a centralized service delivery model to support the obligations and requirements of the Registrar under the *CRRRA*, *SSA*, *CCLA*, and other criminal record checks as deemed appropriate through a service level agreement between the Ministry and the RCMP (see section 3.3.ii). The Ministry will fund the CRRU by providing a fenced delegation to the RCMP's Provincial Business Line to cover incremental costs above what is currently being provided to support the unit.

3.2 Staff and Resources

i. Organizational Structure

The proposed CRRU will consist of a 0.5 police position (Sgt level, to be shared with Cannabis Organized Crime Counter Proliferation Unit) and one FTE Team Coordinator, as well as eight SPD investigative positions. The Sergeant and the Team Coordinator will be staffed by OCABC, and will provide direction and oversight of unit activities, while the eight investigative positions will conduct the criminal record and associated background checks.

Proposed Model			FY 18/19	FY 19/20	FY 20/21	FY 21/22+
Role	Classification	Agency	# FTEs			
Unit Lead	Sgt	OCABC	0.125	0.5	0.5	0.5
CRRU Team Coordinator		OCABC	0.17	1	1	1
Investigator	AO 21	SPD	0.83	6.5	8	8
Investigator	Contract	OCABC	0	2.25	0	0
Total Unit FTEs			1.125	10.25	9.5	9.5

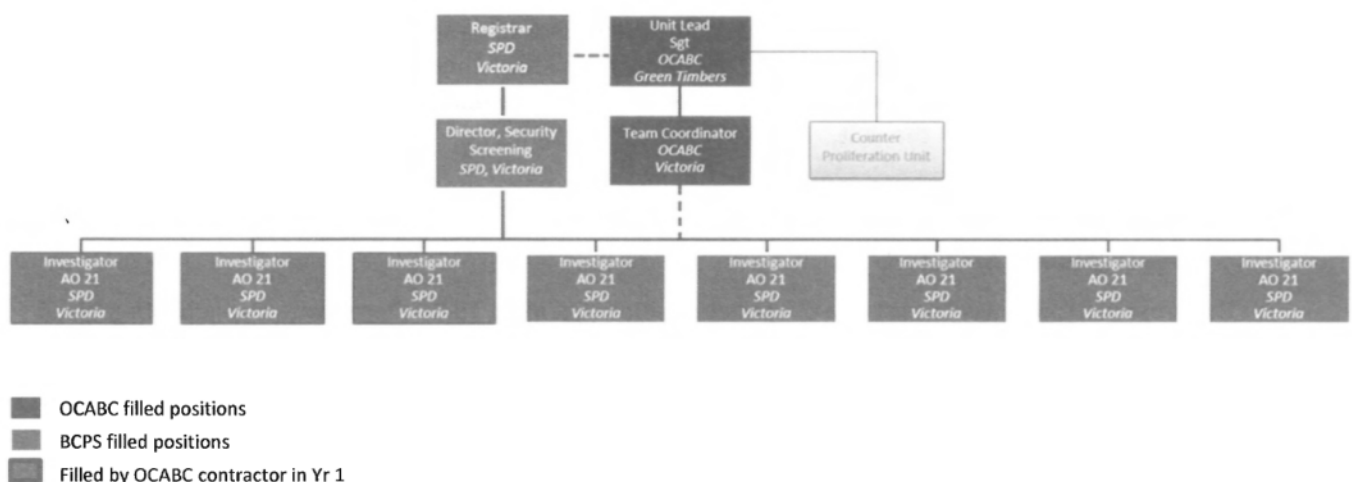
Note: 10.25 FTE's in Yr 1 include a period of overlap between the contractors and SPD staff to allow for training of the SPD staff. Total OCA contract investigators 3 x 9 months = 2.25 FTE's.

As the CRRU falls under the responsibility of the RCMP; the oversight positions will monitor and control unit policies and procedures to ensure consistent quality and efficiency.

During early discussion with the RCMP, it was identified that OCABC would not be able to classify and staff the eight staff investigator positions for an April 1, 2019 deadline. As a result, RCMP and PSB executive determined that three of the current SPD contractors would be offered nine month contracts through OCABC, April 1, 2019 to December 31, 2019, to ensure the continuity and consistency of the unit. Additionally, SPD employees would be the best option to fill the remaining five investigator positions in order to be operationally ready for April 1, 2019.

The integration of SPD and OCABC staff will ensure timely Unit establishment and mitigate the administrative weight for the RCMP, while also ensuring the necessary expertise and oversight required.

A preliminary organizational chart is shown below which outlines the proposed structure for the first year of service⁴. An option to review this structure will be built into the service agreement to ensure work demands are continually met.



ii. Location & Resources

The updated CRRU will continue to be located in Victoria at RCMP E-Division Island District headquarters, with the Unit Lead (Sgt) located primarily out of Green Timbers. To work in the building and access the required databases, all CRRU support staff will be required to pass RCMP security screening.

⁴ In year one (FY19/20), it is expected that three of the eight investigator positions will be contracted by OCABC to three of the current CRRU contractors to ensure continuity and opportunities to cross train new PSB staff.

The current location can accommodate up to ten FTEs without any additional renovation costs, however, ten smaller 2.0 size desks may be required to accommodate all ten FTEs (three more than are currently located there). Any start-up costs associated with the updated CRRU must be pre-approved and will be provided through additional fenced funding by PSB, at the Provincial cost share (see 3.4, Unit Costs) model.

3.3 Governance and Reporting

The updated CRRU will remain a Provincial RCMP Unit; however it will be re-established under the CFSEU-BC umbrella in order to provide increased oversight of the unit. Reinforcing RCMP supervision of the CRRU will ensure better quality control and efficiency, as well as provide an opportunity to develop standardized procedures for informed decision making.

The oversight and responsibility for the CRRU and its output will fall under the RCMP. The provincial employees will be members of BCGEU and will formally report to the Director, Security Screening at SPD, with a dotted line reporting relationship to the CRRU Team Coordinator.

Further details on unit governance and reporting requirements will be built into a Service Level Agreement.

i. Liability

As per the *CRRA*, *SSA*, and the *CCLA*, the Registrar/Security Manager (Executive Director, Security Programs Division) is ultimately responsible to interpret the criminal record checks and act as the final decision maker. This includes completing follow up with the originating police agency where the record is held to confirm details as required.

The responsibility of the Unit under the RCMP will be the collection and communication of accurate and complete police information to support reliable decision making. The updated model ensures the RCMP have greater oversight and control over the Unit and the checks themselves, including the ability to instil consistent policies and processes for performing checks. This structure may improve the efficiency and effectiveness of the Unit as well as provide a standard to defend decisions.

ii. Service Level Agreement

It is recommended that a Service Level Agreement for the RCMP CRRU be prepared to address the parameters of each reporting relationship, as well as outline responsibilities and expectations of all parties involved. This should include but is not limited to: supervisory considerations, capacity issues, service level expectations, training, reporting requirements, issues management, liability, and asset management. A formalized reporting and review structure will be established to ensure Unit resources, funding, and parameters remain appropriate for the effectively delivery of identified responsibilities for all parties.

3.4 Unit Costs

To support the formalization of the provincial RCMP CRRU within CFSEU-BC, and ensure the continued safety of specialized programs in B.C., the Province will provide fenced funding towards the implementation, maintenance and approved additional costs incurred by RCMP E-Division. This will include contributions to workstation accommodations, operations and maintenance, as well as staff salary and benefits above what is currently being provided under the current CRRU arrangement (see Table 2 below).

As previously mentioned, a review period will also be established to ensure that resources are adequate to effectively deliver Unit responsibilities.

Table 2: Total estimated costs of updated CRRU

	FY 18/19*	FY 19/20	FY 20/21	FY 21/22
RCMP Positions				
1.5 OCABC staff	26,866	131,133	131,133	131,133
Allowances & Benefits	7,017	33,986	33,986	33,986
3 x 1-Yr OCABC Contract		191,250	0	0
OT and O&M Costs**		39,623	34,239	34,239
Training (CPIC, PRIME, etc.)		11,250	4,500	4,500
Travel	7,000	15,000	15,000	15,000
Accommodations		no additional funding		
RCMP Subtotal (100%)	\$ 40,883	\$ 422,242	\$ 218,858	\$ 218,858
Provincial SPD Positions				
8 x AO21 (5 in 18/19 & 19/20)	56,651	426,735	525,212	525,212
Allowances & Benefits	14,049	105,830	130,253	130,253
OT		5,000	5,000	5,000
O&M Costs		15,555	19,144	19,144
Training (CPIC, PRIME, etc.)	15,000	24,000	24,000	24,000
Accommodations		no additional funding		
SPD Staff (100%)	\$ 85,700	\$ 577,120	\$ 703,609	\$ 703,609
Start-up costs				
(renos & fit up) OCABC	57,300			
(renos & fit up) Prov	58,000			
Start-up Subtotal(100%)	\$ 115,300	\$ -	\$ -	\$ -
Total Cost for Unit (100%)	\$ 241,883	\$ 999,362	\$ 922,467	\$ 922,467
Total Cost to Province (70%)	\$ 169,318	\$ 699,553	\$ 645,727	\$ 645,727

* FY18/19 cost is in addition to current CRRU contracts, payable to a maximum of approximately \$710K

** includes 0.5 GT accommodations charge for shared Sgt position

Note: Additional staffing costs are built into FY 18/19 to support start-up activities, as well as anticipate any added requirement to train investigative staff in preparation for April 1, 2019 start date.

i. Policing Cost Share

Throughout Canada, the processing of criminal record checks, especially for the purpose of working within the vulnerable sector, is a police agency responsibility. While a centralized CRRU was established as a provincial priority in response to the *CRRA*, the dismantling of this Unit would see all required checks become the responsibility of local police detachments due to the public safety requirement, necessary access to confidential police databases, and the effective interpretation of police records.

The proposed restructured model presents an improved provincial RCMP CRRU in support of Provincial and policing responsibilities which not only increases public safety, but also promotes improved information exchange, centralizes administrative services and establishes mutual benefit for all parties.

Formalization of the proposed Unit provides clear delineation of provincial and RCMP roles and responsibilities to support provincial policing requirements. The CRRU currently falls within the parameters of the Provincial Police Service Agreement. As per article 2.6 of the 2012 Municipal Police Service Agreement, in circumstances where support staff are provided to Canada by the Province in support of provincial policing, Canada will pay the Province a proportional share of the salaries; therefore, total costs for the Unit will be at the applicable 70/30 cost-share.

4.0 Risks and Considerations

The following risks have been identified for this project:

Risk	Probability	Impact	Proposed Risk Response
Current CRRU contractors' willingness to stay/extend their contract.	Medium	High	Premature loss of the contractors would shut down security branch processes. Must ensure that every effort is given to maintain sensitivity of the project and consideration for current contractors.
New model may not be ready for April 1, 2019 start	High	High	Initiate discussion early with RCMP to ensure ability to implement proposed model as early as possible. Expedite the staffing process by hiring provincial SPD employees to fill the intake and investigator positions.
RCMP enhanced Security Screening not completed before April 1, 2019	Medium	High	Possibility of SPD paying overtime costs for the RCMP to complete the security screenings quicker.
Service interruption or delays to service delivery during transition to new model	Medium	Medium	Work with current contractors to overlap service delivery, if possible. Possible option to obtain federal resource at the Security Intelligence Background Section to provide training and set up guidance.

Risk	Probability	Impact	Proposed Risk Response
CPIC and/or other legislative or legal restrictions could complicate or delay development of new Unit.	Low	High	Continue communication with CPIC agency to ensure service delivery is in line with regulatory requirements. Ensure legal advice is attained on proposed model.

4.1 Stakeholder Impacts

The service delivery system for the updated model is not expected to change; the CRRU will continue to function as a centralized unit to perform the criminal record checks required under the *CRRRA* and other mandated programs. SPD will retain the client-facing role, collecting requests for checks, fielding service questions, and reporting on results back to clients.

5.0 Implementation

The updated CRRU must be established and operational by April 1, 2019. To support this transition, all staff must be hired, trained, and have obtained security clearance prior to March 31, 2019. Further, all information access agreements (ex. CPIC, Information Sharing) will need to be updated and approved.

In addition to hiring the five Investigator positions for, the SPD will work with the RCMP to establish the necessary approvals, as well as support any required role specific training. Following the close of the cross-over OCABC contractor positions in December 2019, SPD will work to fill the remaining three investigator positions with full time SPD staff.

As the Unit and the unit output is the responsibility of the RCMP, it is expected that policies and procedures to support decision making and ensure the accurate and effective interpretation of the information, will be established.

Pending the approval of this business case, it is recommended that a formal transition and communication plan be established collaboratively with SPD and the RCMP. This plan will ensure the timely establishment of the updated unit, as well as address communication and close of the current CRRU contracts.

6.0 Approvals

This business case has been reviewed and is recommended by:



Shera Skinner, ED Security Programs Division



Date

Policing and Security Branch
Ministry of Public Safety and Solicitor General

A/Commissioner Eric Stubbs
E-Division, Royal Canadian Mounted Police

Date

D/Commissioner Brenda Butterworth-Carr
Commanding Officer of E-Division
Royal Canadian Mounted Police

Date



Clayton Pecknold, Director of Policing Services
and ADM, Policing and Security Branch
Ministry of Public Safety and Solicitor General



Date

MODIFICATION AGREEMENT

To the JUSTIN Electronic Access Agreement dated August 10, 2016

BETWEEN: Ministry of Attorney General
Court Services Branch
6th Floor, 850 Burdett Avenue
Victoria, BC
V8W 9J2

AND: Ministry of Attorney General
BC Prosecution Service
9th Floor, 1001 Douglas Street
Victoria, BC
V8W 2C5

AND: Ministry of Public Safety and Solicitor General
Personnel Security Screening Office
Security Programs Division
Policing and Security Branch
914 Yates Street
Victoria BC
V8V 3M2

('PSSO')

1. Background to this Modification Agreement

This is a Modification Agreement to the Electronic Access Agreement (EAA) dated August 10, 2016 regarding electronic access to the Court Inquiry Module and the Report to Crown Counsel Module of the Justice Information System ('JUSTIN') between CSB, BC Prosecution Service, and the Office of the Chief Judge, and Policing and Security Branch, Ministry of Public Safety and Solicitor General.

2. Continuation of terms and conditions of the EAA

The parties agree to the continuation of all the terms and conditions of the EAA except for the amendments described in this Modification Agreement.

3. Amendment to 'Requirement of Security Screening Pursuant to the BC Public Service Security Screening Policy'

Paragraph 15(a) is added as follows:

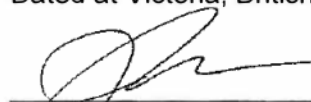
15(a). PSSO further agrees that if, after carrying out a standard security screening, a security clearance has not been granted and the applicant requests reasons, or a reconsideration, of a decision by the Deputy Minister pursuant to the BC Public Service Human Resources Policy #14 (Security Screening), the data extract from the RCC Module will not be sent to the Deputy Minister. Rather, the summarized information in the Investigative Report to the Director will be sent. The Investigative Report will be emailed to the Deputy Minister with the subject line: Confidential: Deputy Minister review only – security screening review.

4. Authority to sign:

The Judiciary has control of all court record information. CSB is responsible for collecting, maintaining, and security all court record information under the direction of the Chief Justices and Chief Judge. In this capacity and under the direction of the Judiciary, CSB is entering into this agreement.

This Modification Agreement is effective upon signing by all parties.

Dated at Victoria, British Columbia, this 24 day of December, 2018



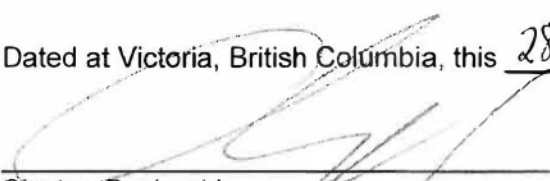
Lynda Cavanaugh
Assistant Deputy Minister
Court Services Branch
Ministry of Attorney General

Dated at Victoria, British Columbia, this 17th day of December, 2018



Peter Juk, QC
~~Assistant Deputy Attorney General~~
BC Prosecution Service
Ministry of Attorney General

Dated at Victoria, British Columbia, this 28 day of November, 2018



Clayton Pecknold
Assistant Deputy Minister
Security Programs Division
Policing and Security Branch
Ministry of Public Safety and Solicitor General



LETTER OF AGREEMENT

SUPERIOR COURTS JUDICIARY AND PROVINCIAL COURT OF B.C.

Between: The Ministry of Public Safety and Solicitor General, Personnel Security Screening Office
(hereinafter known as PSSO)

And: SUPERIOR COURTS JUDICIARY AND PROVINCIAL COURT OF B.C.
(hereinafter known as "the Judiciary")

1.0 BACKGROUND:

- 1.1 The BC Public Service Security Screening Policy covers the requirement for criminal record checks and enhanced security screening for designated positions within the BC Public Service, facilitated by the PSSO. An enhanced security screening business case was approved for the Superior Courts Judiciary and Provincial Court of B.C. on December 4, 2018.
- 1.2 The enhanced screening is completed by the PSSO and includes all Judiciary positions covered under the Public Service Act. This excludes any judges or masters positions.
- 1.3 The enhanced screening approved in the business case is for the following enhanced security screening services:
 - ✓ Level 4 police record check
 - ✓ JUSTIN/CORNET check
 - ✓ Education check
 - ✓ Five year employment history check
 - ✓ Credentials check
- 1.4 The Public Service Agency's Security Screening Policy mandates that employees subject to enhanced security screening are required to undergo a re-check every five years. The business case stipulates that the enhanced screening services required upon re-checks are:
 - ✓ Level 4 police record check
 - ✓ JUSTIN/CORNET check

2.0 PURPOSE AND SCOPE:

- 2.1 The purpose of this Letter of Agreement (LOA) is to set out the roles and responsibilities of the parties in relation to the type of enhanced security screening performed, disclosure of information, timelines and fees.

3.0 THE PARTIES AGREE AS FOLLOWS:

- 3.1 The Judiciary will request enhanced security screening services by emailing PSSO@gov.bc.ca. When requesting an initial check, the Judiciary agrees to provide PSSO with proof that there has been a conditional offer of employment and a copy of the applicant's resume. The Judiciary also agrees to provide PSSO with the applicant's full legal name and confirm that 2 pieces of ID have been verified. When requesting a re-check or a check upon promotion, the Judiciary will provide all relevant details regarding the employee, including the resume, if applicable.
- 3.2 PSSO agrees to provide the blank consent form to the applicant. PSSO agrees to obtain the signed consent form from the applicant.
- 3.3 PSSO agrees to conduct the enhanced security screening on an applicant and provide a report, including reasons and recommendation on security screening clearance based strictly on the information PSSO collected. This information is provided for the review of the Judiciary which is responsible for making the final decision on whether or not to grant a security clearance to any individual undergoing enhanced security screening.
- 3.4 PSSO will provide a report to the Director, Human Resource and Support Services (Superior Courts Judiciary) or the Manager, Human Resources (Provincial Courts Judiciary) regarding whether or not to confirm an offer of employment based on the security screening results.
- 3.5 In the event the record search reveals a criminal record, the PSSO will advise the appropriate Executive Director of the type of records found, the details and circumstances of the offence, and how they came to their decision to recommend hiring or not. The appropriate Executive Director will consider the recommendation of the PSSO in the decision to hire or not.
- 3.6 The Judiciary and PSSO acknowledge the necessity to respect the privacy of individuals and to protect the data available through CPIC. The Judiciary and PSSO shall comply with applicable provincial privacy laws.
- 3.7 The information released to the Judiciary shall be used only for the purpose of security screening an individual entering into a position of trust. The final hiring decision is made by the Judiciary, not PSSO. The Judiciary will destroy all copies of the PSSO's report once the hiring decision has been made.

4.0 FINANCIAL ARRANGEMENTS

s.17

s.17

5.0 EFFECTIVE DATE OF AGREEMENT, AMENDMENTS, AND TERMINATION

5.1 This LOA is effective January 1, 2019.

5.4 This LOA may be amended at any time by the written consent of the parties and any such amendments will be dated and signed by both parties and attached to this LOA as a schedule.

Signed on behalf of the Personnel Security Screening Office, the Ministry of Public Safety and Solicitor General



Dianne Small

Director, Security Screening

Security Programs Division, Ministry of Public Safety and Solicitor General

Date

Dec 18/18

Signed on behalf of the Superior Courts Judiciary



Heidi McBride

Executive Director and Senior Counsel, Superior Courts Judiciary

Date:

Jan. 16, 2019

Signed on behalf of the Provincial Court of B.C.



Craig Wilkins

Executive Director of Organizational Services, Provincial Court of B.C.

Date:

Jan 16, 2019

**MINISTRY OF PUBLIC SAFETY AND SOLICITOR GENERAL
POLICING AND SECURITY BRANCH**

ADDENDUM TO PROPOSED BUSINESS MODEL FOR THE CRIMINAL RECORDS REVIEW UNIT (CRRU)

This addendum to the CRRU Business Case signed by ADM Clayton Pecknold on December 10, 2018 is in response to Deputy Commissioner Butterworth-Carr's letter, sent February 25, 2019, supporting the formalization of the Criminal Records Review Unit (CRRU) as a unit of the RCMP Provincial Police Service created under the *Provincial Police Service Agreement* (PPSA).

Staffing of the proposed CRRU positions will be the responsibility of the RCMP and once the Business Case is approved, a letter to the federal government will be sent by the Minister of Public Safety and Solicitor General, requesting the required change to Annex A of the PPSA.

Specific provisions of the above-noted CRRU Business Case are amended as per the following:

3.2 i) Organizational Structure

The CRRU unit will be comprised of 0.5 regular police member supervisory position as well as nine civilian support positions (one Team Coordinator and eight Investigative Officers), as identified in the table below:

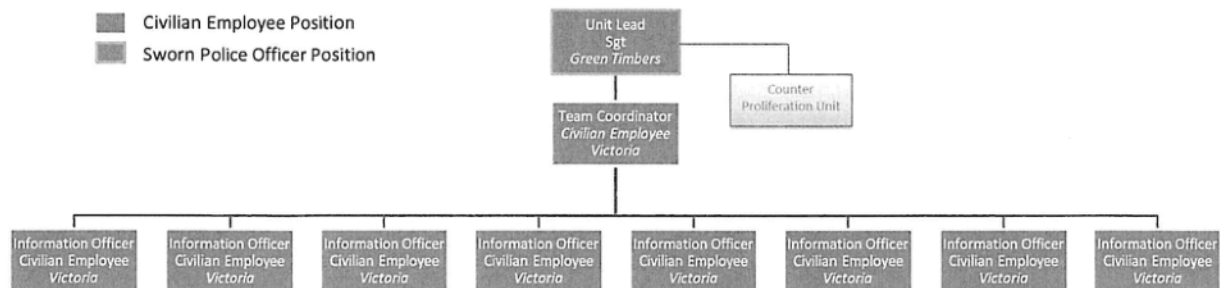
Table 1 (revised):

Proposed Model		FY 19/20	FY 20/21	FY 21/22+
Role	Classification			
Unit Lead	Sgt	0.5	0.5	0.5
CRRU Team Coordinator	civilian employee	1	1	1
Information Officer	civilian employee	8	8	8
Total Unit FTEs		9.5	9.5	9.5

OMIT: SPD employees to fill investigator positions.

CORRECTION: All staffing of the unit will be the responsibility of the RCMP.

The preliminary organization chart has been revised to the following:



3.3 Governance and Reporting

OMIT: The provincial employees will be members of BCGEU and will formally report to the Director, Security Screening at SPD, with a dotted line reporting relationship to the CRRU Team Coordinator.

CORRECTION: Objectives and priorities of the CRRU will be led by the Director, Security Screening at SPD, while the oversight and responsibility for the CRRU and its output will fall under the RCMP. Further details on unit governance and reporting requirements will be built into a Service Level Agreement.

3.4 Unit Costs

Table 2 is revised to reflect the updated costs of the CRRU: *Total estimated costs of updated CRRU*

	#	FY 18/19*	FY 19/20	FY 20/21	FY 21/22 +
Pay & Benefits					
Sgt	0.5	0	60,133	60,133	60,133
Team Coordinator	1.0	0	71,000	71,000	71,000
Information Officers	8.0	0	289,910	496,989	496,989
Allowances & Benefits		0	105,884	157,239	157,239
7 x 7 Information Officer contracts	7.0	0	347,083	0	0
Staffing Subtotal (100%)		\$ -	\$ 874,010	\$ 785,361	\$ 785,361
OT and O&M Costs					
Overtime		0	17,000	20,000	20,000
Travel		0	15,000	15,000	15,000
O&M Costs		0	47,577	30,826	30,826
Training (CPIC, PRIME, etc.)		0	49,500	28,500	28,500
Accommodations (0.5 for Sgt only)		0	7,500	7,500	7,500
OT and O&M Subtotal (100%)		\$ -	\$ 136,577	\$ 101,826	\$ 101,826
Start-up costs					
Workstations		23,300	0	0	0
Desks & fit-up		25,000	20,000	0	0
Start-up Subtotal(100%)		\$ 48,300	\$ 20,000	\$ -	\$ -
Total Cost for Unit (100%)		\$ 48,300	\$ 1,030,587	\$ 887,187	\$ 887,187
Federal Contribution (30%)		\$ 14,490	\$ 309,176	\$ 266,156	\$ 266,156
Cost to Province (70%)		\$ 33,810	\$ 721,411	\$ 621,031	\$ 621,031

5.0 Implementation

OMIT: SPD will work to fill the eight investigator positions

CORRECTION: Hiring and training for the eight investigator positions is the responsibility of the RCMP (CRRU Unit Lead).

Approvals


This business case has been reviewed and is recommended by:



Robyn White, A/ ED Security Programs Division
Policing and Security Branch
Ministry of Public Safety and Solicitor General

April 29, 2019

Date



Brenda Butterworth-Carr; Tr'injã shãr njit dintlãt
Assistant Deputy Minister
And Director of Police Services
Policing and Security Branch

2019-04-30

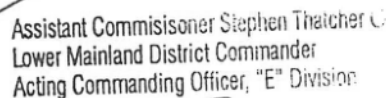
Date

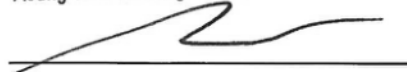


Ward LYMBURNER, C/Supt. O.2222
E Div. Major Crime Section
Assistant Commissioner Kevin Hackett,
Criminal Operations Officer (FISOC)
Royal Canadian Mounted Police

2019-05-06

Date



Assistant Commissioner Stephen Thatcher C.
Lower Mainland District Commander
Acting Commanding Officer, "E" Division

Assistant Commissioner Eric Stubbs
A/Commanding Officer, E – Division
Royal Canadian Mounted Police

2019-05-07

Date



LETTER OF AGREEMENT

INDEPENDENT INVESTIGATIONS OFFICE

Between: **The Personnel Security Screening Office, Ministry of Public Safety and Solicitor General (hereinafter known as PSSO)**

And: **Independent Investigations Office
(hereinafter known as IIO)**

1.0 BACKGROUND:

- 1.1 The BC Public Service Security Screening Policy covers the requirement for criminal record checks and/or enhanced security screening for designated positions within the BC Public Service, facilitated by the PSSO. An enhanced security screening business case was approved for the IIO on January 9, 2012.
- 1.2 Depending on the position within the IIO, the enhanced screening approved in the business case is for one or more of the following enhanced security screening services:
 - ✓ Box 4 police record check
 - ✓ JUSTIN/CORNET check
 - ✓ Certified criminal record check (with or without VS screening)
 - ✓ Security interview with lifestyle questions
 - ✓ Polygraph with lifestyle questions
 - ✓ Character references check
 - ✓ Education check, five year employment history check, credentials check
 - ✓ Driver's abstract
- 1.3 The Public Service Agency's Security Screening Policy mandates that employees subject to enhanced security screening are required to undergo a re-check every five years.
- 1.4 The lifestyle questionnaire with polygraph analysis will be applicable to Investigators and Directors only. Non-investigative and administrative staff will be subject to the lifestyle questionnaire with security interview.

2.0 PURPOSE AND SCOPE:

- 2.1 This purpose of this Letter of Agreement (LOA) is to set out the roles and responsibilities of the parties in relation to the type of criminal record checks performed, disclosure of information, timelines and fees.

3.0 THE PARTIES AGREE AS FOLLOWS:

- 3.1 IIO agrees to provide PSSO with a copy of the ESS letter to the applicant and copy of resume and an email address for the applicant.
- 3.2 The PSSO will send out the consent form and package to all applicants. The applicant will return the completed package directly to PSSO to ensure privacy is maintained. The PSSO will then provide the completed questionnaire to the polygraph/security interview providers in order that they may review them prior to interview.
- 3.3 The PSSO's polygraph provider may liaise directly with the IIO and the applicant in order to set up the time and location of the polygraph. For non-investigative and administrative staff, the PSSO's security interview provider will liaise directly with the applicant in order to set up the security interview.
- 3.4 PSSO agrees to conduct the enhanced security screening on an applicant and provide a report, including an assessment regarding issues related to security to the Chief Civilian Director. The analysis will be based strictly on the information PSSO collected and will outline any concerns regarding security or suitability. A copy of the polygrapher's report will be provided to the Chief Civilian Director, with a request that any hard or electronic copies be destroyed after the hiring decision has been made. Original reports and all other supporting documentation will be maintained by the PSSO.
- 3.5 The IIO has provided written permission for the PSSO to complete and submit reports with educational/employment verification pending. Once outstanding information is received by the PSSO, an addendum outlining the results will be provided to the IIO. Similarly, the PSSO will provide results of certified criminal record check to the Chief Civilian Director, as an addendum, upon receipt (which may take several months, depending on RCMP response time).
- 3.6 IIO and PSSO acknowledge the necessity to respect the privacy of individuals and to protect the data available through CPIC. IIO and PSSO shall comply with applicable provincial privacy laws.
- 3.7 The information released to IIO shall be used only for the purpose of screening an individual entering into a position of trust.

4.0 FINANCIAL ARRANGEMENTS

- 4.1 IIO shall be responsible for compensating PSSO at a cost per service as follows:

OPTIONS

- a) Enhanced security screening, for Investigators and Directors, which includes the collection, analysis and report on the following: box 4 criminal record check (box 4 is the addition of police databases), JUSTIN/CORNET check, certified criminal record check with fingerprinting and vulnerable sector screening, lifestyle questionnaire and polygraph analysis, character references, employment, education and credentials verification, driver's abstract:

Approved Fees by Level of Adjudication			
No Adjudication	Simple	Intermediate	Difficult
\$875 plus travel expenses	\$910 plus travel expenses	\$960 plus travel expenses	\$1,160 plus travel expenses

The PSSO report and polygrapher's report will be returned to Chief Civilian Director within 4-5 weeks.

- b) Enhanced security screening, for non-investigative/administrative staff, which includes the collection, analysis and report on the following: box 4 criminal record check (box 4 is the addition of police databases), JUSTIN/CORNET check, certified criminal record check with fingerprinting, lifestyle questionnaire with interview, character references, employment, education and credential verification, driver's abstract:

Approved Fees by Level of Adjudication			
No Adjudication	Simple	Intermediate	Difficult
\$765 plus travel expenses	\$800 plus travel expenses	\$850 plus travel expenses	\$1,050 plus travel expenses

The PSSO report will be returned to Chief Civilian Director within 4-5 weeks.

- c) 5 year re-checks for all staff (Investigators, Directors and non-investigative/administrative staff), which includes the collection, analysis and report on the following: box 4 criminal record check (box 4 is the addition of police databases), JUSTIN/CORNET check, driver's abstract:

Approved Fees by Level of Adjudication			
No Adjudication	Simple	Intermediate	Difficult
\$135	\$170	\$220	\$420

The PSSO report will be returned to Chief Civilian Director within approximately two weeks.

- 4.2 IIO shall reimburse PSSO by a Journal Voucher, completed on a monthly basis in accordance with the fiscal year defined as April 1 to March 31.

5.0 EFFECTIVE DATE OF AGREEMENT, AMENDMENTS, AND TERMINATION

- 5.1 This LOA is effective on March 1, 2012.
- 5.2 This revised LOA was effective on January 1, 2019.
- 5.3 This newly amended LOA is effective on August 2, 2019.
- 5.4 This LOA may be amended at any time by the written consent of the parties and any such amendments will be dated and signed by both parties and attached to this LOA as a schedule.
- 5.5 This LOA may be terminated by either party upon 30 days written notice.

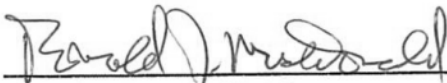
Signed on behalf of the Personnel Security Screening Office, the Ministry of Public Safety and Solicitor General



Dianne Small
Director, Security Screening
Security Programs Division, Ministry of Public Safety and Solicitor General

Date: Aug 2/19

Signed on behalf of the Independent Investigations Office



Ronald J. MacDonald, QC
Chief Civilian Director, Independent Investigations Office

Date: August 26, 2019

GENERAL SERVICE AGREEMENT



<i>For Administrative Purposes Only</i>	
<p><i>Ministry Contract No.: SGPSPB21CS09</i></p> <p><i>Requisition No.: _____</i></p> <p><i>Solicitation No.(if applicable): _____</i></p> <p><i>Commodity Code: _____</i></p> <p>Contractor Information</p> <p><i>Supplier Name: ITV CONSULTING</i></p> <p><i>Supplier No.: 2037404</i></p> <p><i>Telephone No.: (250) 883-5528</i></p> <p><i>E-mail Address: dwitv@shaw.ca</i></p> <p><i>Website: _____</i></p>	<p>Financial Information</p> <p><i>Client: 010</i></p> <p><i>Responsibility Centre: 15408</i></p> <p><i>Service Line: 11710</i></p> <p><i>STOB: 6001</i></p> <p><i>Project: 1500000</i></p> <p>Template version: December 21, 2018</p>

TABLE OF CONTENTS

No.	Heading	Page
1.	Definitions	1
	1.1 General.....	1
	1.2 Meaning of "record"	2
2.	Services	2
	2.1 Provision of services	2
	2.2 Term	2
	2.3 Supply of various items	2
	2.4 Standard of care.....	2
	2.5 Standards in relation to persons performing Services.....	2
	2.6 Instructions by Province	2
	2.7 Confirmation of non-written instructions	2
	2.8 Effectiveness of non-written instructions	2
	2.9 Applicable laws	2
3.	Payment	3
	3.1 Fees and expenses	3
	3.2 Statements of accounts	3
	3.3 Withholding of amounts.....	3
	3.4 Appropriation.....	3
	3.5 Currency	3
	3.6 Non-resident income tax.....	3
	3.7 Prohibition against committing money	3
	3.8 Refunds of taxes	4
4.	Representations and Warranties	4
5.	Privacy, Security and Confidentiality	4
	5.1 Privacy	4
	5.2 Security	4
	5.3 Confidentiality	4
	5.4 Public announcements	5
	5.5 Restrictions on promotion	5
6.	Material and Intellectual Property	5
	6.1 Access to Material	5
	6.2 Ownership and delivery of Material	5
	6.3 Matters respecting intellectual property	5
	6.4 Rights relating to Incorporated Material	5
7.	Records and Reports	6
	7.1 Work reporting.....	6
	7.2 Time and expense records	6
8.	Audit	6

9.	Indemnity and Insurance	6
9.1	Indemnity	6
9.2	Insurance	6
9.3	Workers compensation.....	6
9.4	Personal optional protection	6
9.5	Evidence of coverage.....	7
10.	Force Majeure	7
10.1	Definitions relating to force majeure.....	7
10.2	Consequence of Event of Force Majeure	7
10.3	Duties of Affected Party.....	7
11.	Default and Termination	7
11.1	Definitions relating to default and termination.....	7
11.2	Province's options on default.....	8
11.3	Delay not a waiver	8
11.4	Province's right to terminate other than for default	8
11.5	Payment consequences of termination	8
11.6	Discharge of liability.....	8
11.7	Notice in relation to Events of Default.....	9
12.	Dispute Resolution	9
12.1	Dispute resolution process	9
12.2	Location of arbitration or mediation	9
12.3	Costs of mediation or arbitration.....	9
13.	Miscellaneous	9
13.1	Delivery of notices	9
13.2	Change of address or fax number	10
13.3	Assignment	10
13.4	Subcontracting.....	10
13.5	Waiver.....	10
13.6	Modifications	10
13.7	Entire agreement	10
13.8	Survival of certain provisions	10
13.9	Schedules.....	10
13.10	Independent contractor.....	11
13.11	Personnel not to be employees of Province	11
13.12	Key Personnel.....	11
13.13	Pertinent Information	11
13.14	Conflict of interest.....	11
13.15	Time	11
13.16	Conflicts among provisions.....	11
13.17	Agreement not permit nor fetter.....	11
13.18	Remainder not affected by invalidity	12
13.19	Further assurances	12
13.20	Additional terms	12
13.21	Governing law	12
14.	Interpretation	12
15.	Execution and Delivery of Agreement	12

SCHEDULE A – SERVICES

- Part 1 - Term**
- Part 2 - Services**
- Part 3 - Related Documentation**
- Part 4 - Key Personnel**

SCHEDULE B – FEES AND EXPENSES

- Part 1 - Maximum Amount Payable**
- Part 2 - Fees**
- Part 3 - Expenses**
- Part 4 - Statements of Account**
- Part 5 - Payments Due**

SCHEDULE C – APPROVED SUBCONTRACTOR(S)

SCHEDULE D – INSURANCE

SCHEDULE E – PRIVACY PROTECTION SCHEDULE

SCHEDULE F – ADDITIONAL TERMS

SCHEDULE G – SECURITY SCHEDULE

THIS AGREEMENT is dated for reference the 1st day of April ~~2019~~ 2020

BETWEEN:

ITV Consulting (the "Contractor") with the following specified address and fax number:
577 Delora Drive
Victoria, British Columbia
V9C 3S2

AND:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, as represented by the Minister of Public Safety and Solicitor General (the "Province") with the following specified address and fax number:
Policing and Security Branch
Security Programs Division
PO Box 9217 Stn Prov Govt
Victoria, British Columbia
V8W 9J1

The Province wishes to retain the Contractor to provide the services specified in Schedule A and, in consideration for the remuneration set out in Schedule B, the Contractor has agreed to provide those services, on the terms and conditions set out in this Agreement.

As a result, the Province and the Contractor agree as follows:

1 DEFINITIONS

General

1.1 In this Agreement, unless the context otherwise requires:

- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
- (b) "Incorporated Material" means any material in existence prior to the start of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
- (c) "Material" means the Produced Material and the Received Material;
- (d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced or provided by the Contractor or a Subcontractor and includes the Incorporated Material;
- (e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Province or any other person;
- (f) "Services" means the services described in Part 2 of Schedule A;
- (g) "Subcontractor" means a person described in paragraph (a) or (b) of section 13.4; and
- (h) "Term" means the term of the Agreement described in Part 1 of Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by Province

2.6 The Province may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are carried out.

Confirmation of non-written instructions

2.7 If the Province provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Province in writing, which request the Province must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

3 PAYMENT

Fees and expenses

3.1 If the Contractor complies with this Agreement, then the Province must pay to the Contractor at the times and on the conditions set out in Schedule B:

(a) the fees described in that Schedule;

DW

- (b) the expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Province's opinion, are necessarily incurred by the Contractor in providing the Services; and
- (c) any applicable taxes payable by the Province under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Province is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Province a written statement of account in a form satisfactory to the Province upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

- 3.3 Without limiting section 9.1, the Province may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Province and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Province to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Province.

Appropriation

- 3.4 The Province's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Province during which payment becomes due.

Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are to Canadian dollars.

Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Province may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

- 3.7 Without limiting section 13.10(a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Province to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

- 3.8 The Contractor must:
- (a) apply for, and use reasonable efforts to obtain, any available refund, credit, rebate or remission of federal, provincial or other tax or duty imposed on the Contractor as a result of this Agreement that the Province has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement; and
 - (b) immediately on receiving, or being credited with, any amount applied for under paragraph (a), remit that amount to the Province.

4 REPRESENTATIONS AND WARRANTIES

4.1 As at the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Province as follows:

- (a) except to the extent the Contractor has previously disclosed otherwise in writing to the Province,
 - (i) all information, statements, documents and reports furnished or submitted by the Contractor to the Province in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,
 - (ii) the Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractual or other agreements in place and available to enable the Contractor to fully perform the Services and to grant any licenses under this Agreement, and
 - (iii) the Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and
- (b) if the Contractor is not an individual,
 - (i) the Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and
 - (ii) this Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:

- (a) make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, alteration or disposal; and
- (b) comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Province's prior written consent except:

- (a) as required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
- (b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or
- (c) if it is information in any Incorporated Material.

DW

Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Province and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

- 5.5 The Contractor must not, without the prior written approval of the Province, refer for promotional purposes to the Province being a customer of the Contractor or the Province having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Province, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Province.

Ownership and delivery of Material

- 6.2 The Province exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Province immediately upon the Province's request.

Matters respecting intellectual property

- 6.3 The Province exclusively owns all intellectual property rights, including copyright, in:

- (a) Received Material that the Contractor receives from the Province; and
- (b) Produced Material, other than any Incorporated Material.

Upon the Province's request, the Contractor must deliver to the Province documents satisfactory to the Province that irrevocably waive in the Province's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Province of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Province:
- (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to exercise, in respect of that Incorporated Material, the rights set out in the *Copyright Act* (Canada), including the right to use, reproduce, modify, publish and distribute that Incorporated Material; and
 - (b) the right to sublicense or assign to third-parties any or all of the rights granted to the Province under section 6.4(a).

7 RECORDS AND REPORTS

Work reporting

- 7.1 Upon the Province's request, the Contractor must fully inform the Province of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Province. Unless otherwise specified in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement ends.

8 AUDIT

- 8.1 In addition to any other rights of inspection the Province may have under statute or otherwise, the Province may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Province's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

- 9.1 The Contractor must indemnify and save harmless the Province and the Province's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Province or any of the Province's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "Loss") to the extent the Loss is directly or indirectly caused or contributed to by:

- (a) any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or
- (b) any representation or warranty of the Contractor being or becoming untrue or incorrect.

Insurance

- 9.2 The Contractor must comply with the Insurance Schedule attached as Schedule D.

Workers compensation

- 9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

- 9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- (a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
 - (b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

- 9.5 Within 10 Business Days of being requested to do so by the Province, the Contractor must provide the Province with evidence of the Contractor's compliance with sections 9.3 and 9.4.

DW

10 FORCE MAJEURE

Definitions relating to force majeure

10.1 In this section and sections 10.2 and 10.3:

- (a) "Event of Force Majeure" means one of the following events:
 - (i) a natural disaster, fire, flood, storm, epidemic or power failure,
 - (ii) a war (declared and undeclared), insurrection or act of terrorism or piracy,
 - (iii) a strike (including illegal work stoppage or slowdown) or lockout, or
 - (iv) a freight embargoif the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
- (b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

- (a) "Event of Default" means any of the following:
 - (i) an Insolvency Event,
 - (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
 - (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and
- (b) "Insolvency Event" means any of the following:
 - (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
 - (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency,
 - (iii) a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
 - (iv) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),

- (v) a receiver or receiver-manager is appointed for any of the Contractor's property, or
- (vi) the Contractor ceases, in the Province's reasonable opinion, to carry on business as a going concern.

Province's options on default

- 11.2 On the happening of an Event of Default, or at any time thereafter, the Province may, at its option, elect to do any one or more of the following:
- (a) by written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
 - (b) pursue any remedy or take any other action available to it at law or in equity; or
 - (c) by written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

- 11.3 No failure or delay on the part of the Province to exercise its rights in relation to an Event of Default will constitute a waiver by the Province of such rights.

Province's right to terminate other than for default

- 11.4 In addition to the Province's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Province may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

- 11.5 Unless Schedule B otherwise provides, if the Province terminates this Agreement under section 11.4:
- (a) the Province must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Province's satisfaction before termination of this Agreement; and
 - (b) the Contractor must, within 30 days of such termination, repay to the Province any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Province has notified the Contractor in writing was not completed to the Province's satisfaction before termination of this Agreement.

Discharge of liability

- 11.6 The payment by the Province of the amount described in section 11.5(a) discharges the Province from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

- 11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Province of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

- 12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
- (a) the parties must initially attempt to resolve the dispute through collaborative negotiation;
 - (b) if the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the Mediate BC Society; and
 - (c) if the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Arbitration Act*.

Location of arbitration or mediation

- 12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

- 12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

- 13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
- (a) by fax to the addressee's fax number specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
 - (b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
 - (c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or fax number

- 13.2 Either party may from time to time give notice to the other party of a substitute address or fax number, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or fax number specified for the party giving the notice.

Assignment

- 13.3 The Contractor must not assign any of the Contractor's rights or obligations under this Agreement without the Province's prior written consent. Upon providing written notice to the Contractor, the Province may assign to any person any of the Province's rights under this Agreement and may assign to any "government corporation", as defined in the *Financial Administration Act*, any of the Province's obligations under this Agreement.

Subcontracting

- 13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Province's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
- (a) any person retained by the Contractor to perform obligations under this Agreement; and
 - (b) any person retained by a person described in paragraph (a) to perform those obligations fully complies with this Agreement in performing the subcontracted obligations.

Waiver

- 13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

- 13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

- 13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to performance of the Services.

Survival of certain provisions

- 13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedules

- 13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:

- (a) an employee or partner of the Province; or
- (b) an agent of the Province except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Province

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Province.

Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in Part 4 of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Province otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

13.13 The Province must make available to the Contractor all information in the Province's possession which the Province considers pertinent to the performance of the Services.

Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Province's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Province under this Agreement.

Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:

- (a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
- (b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Province or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Province or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

- 13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

- 13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

- 13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Governing law

- 13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION



14.1 In this Agreement:

- (a) "includes" and "including" are not intended to be limiting;
- (b) unless the context otherwise requires, references to sections by number are to sections of this Agreement;
- (c) the Contractor and the Province are referred to as "the parties" and each of them as a "party";
- (d) "attached" means attached to this Agreement when used in relation to a schedule;
- (e) unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
- (f) the headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
- (g) "person" includes an individual, partnership, corporation or legal entity of any nature; and
- (h) unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

15 EXECUTION AND DELIVERY OF AGREEMENT

- 15.1 This Agreement may be entered into by a separate copy of this Agreement being executed by, or on behalf of, each party and that executed copy being delivered to the other party by a method provided for in section 13.1 or any other method agreed to by the parties.

The parties have executed this Agreement as follows:

<p>SIGNED on the <u>6</u> day of <u>June</u>, 2020 by the Contractor (or, if not an individual, on its behalf by its authorized signatory or signatories):</p> <p></p> <p>_____ Signature(s)</p> <p><u>Don Wiebe</u> _____ Print Name(s)</p> <p><u>Director, ITV Consulting</u> _____ Print Title(s)</p>	<p>SIGNED on the <u>8</u> day of <u>June</u>, 2020 on behalf of the Province by its duly authorized representative:</p> <p></p> <p>_____ Signature</p> <p><u>Jess Gunnarson</u> _____ Print Name</p> <p><u>Executive Director</u> _____ Print Title</p>
---	---

Schedule A – Services

PART 1. TERM:

1. Subject to section 2 of this Part 1, the term of this Agreement commences on April 1, 2020 and ends on March 31, 2022.
2. At the sole discretion of the Province, there is an option to renew this contract for one year from April 1, 2022 to March 31, 2023.

PART 2. SERVICES:

The enhanced screening process is done by the Personnel Security Screening Office (PSSO) at Security Programs Division. In keeping with accepted standards and practices established by the National Institute for Truth Verification (West Palm Beach, Florida, USA), the contractor will perform COMPUTERIZED VOICE STRESS ANALYSIS (CVSA) pre-employment screening analysis with groups or individuals identified by the Personnel Security Screening Office (PSSO).

The objective of the pre-employment screening CVSA is to provide the PSSO with additional and unbiased assessments that candidate(s) being considered for employment in law enforcement positions have apparently represented themselves truthfully in the recruitment and pre-employment processes. British Columbia Conservation Service, Sheriff Service, Ministry of Children and Family Development's Youth Custody Services and Corrections Branch require their employees to complete enhanced security screening (ESS) which includes a computer voice stress analysis (CVSA) test.

Pursuant to their business case and letter of agreement, CVSA is used in conjunction with security interviews to assess employee suitability to work at the client group organizations.

The contractor will:

1. Use standardized questions, approved in advance by PSSO staff, to screen employment candidates in areas such as criminal or undesirable activity, employment, educational and financial history, and personal associations.
2. Conduct Pre-Test Interviews to evaluate the honesty and integrity of answers provided by candidates during the pre-employment selection process, and assist in resolving issues where stress may be detected during the CVSA process.
3. Conduct CVSA examinations which assess the truthfulness of candidate responses through control and analytical or investigative questions in areas such as criminal or undesirable activity, employment, educational and financial history and personal associations.
4. Perform the same security interview/test as set out in some cases without the CVSA being used.
5. Perform character reference checks using standardized questions, approved in advance by PSSO staff.
6. Perform other related security screening services on an hourly basis when requested by the Province.

Reporting requirements

The contractor will provide an oral and written report of the results of each CVSA pre-employment screening analysis to the PSSO, or an authorized delegate, within two (2) business days upon completion of each such CVSA examination.

PART 3. RELATED DOCUMENTATION:

Not applicable

PART 4. KEY PERSONNEL:

1. The Key Personnel of the Contractor are as follows:
 - a) Robert Wall
 - b) Don Wiebe

DW

- c) Ross Poulton
- d) Lisa Wiebe
- e) Rob McColl
- f) Doug Newman

Schedule B – Fees and Expenses

1. MAXIMUM AMOUNT PAYABLE:

Maximum Amount: Despite sections 2 and 3 of this Schedule, \$440,000.00 is the maximum amount over two years, from April 1, 2020 to March 31, 2022, which the Province is obliged to pay to the Contractor for fees and expenses under this Agreement (exclusive of any applicable taxes described in section 3.1(c) of this Agreement).

The maximum amount for each fiscal year of the Agreement (2020/21, 2021/22) is \$220,000 and, if the Agreement is renewed, the maximum for 2022/23 will be \$220,000.

2. Rate Per Unit/Candidate:

Service to be provided by the Contractor under the terms of this Agreement,	Fee rate
Computer voice stress analysis (CVSA) test	\$275
Reference check (three references)	\$200
Cancellation Fees	
Cancellation fee when the Province cancels a scheduled test upon providing 10 business days' notice or more.	\$0
Cancellation fee when the Province cancels a scheduled test with notice provided more than 24 hours but less than 10 business days before the scheduled test and without providing a replacement candidate.	\$100
Cancellation fee when the Province cancels a scheduled test with less than 24 hours' notice and without providing a replacement candidate.	\$275
Cancellation fee when the Province cancels work that the contractor has started in respect of a candidate (administrative services, request for references). The Province may seek confirmation of the contractor's work.	\$100
Hourly rate for any additional security screening services (e.g. further reference checks) requested by the Province.	\$100 per hour

3. EXPENSES:

Expenses:

- travel, accommodation and meal expenses for travel greater than 32 kilometers away from Victoria, British Columbia on the same basis as the Province pays its Group II employees when they are on travel status; and
- the Contractor's actual long distance telephone, fax, postage and other identifiable communication expenses.

excluding goods and services tax ("GST") or other applicable tax paid or payable by the Contractor on expenses described in (a) and (b) above to the extent that the Contractor is entitled to claim credits (including GST input tax credits), rebates, refunds or remissions of the tax from the relevant taxation authorities.

\$70,000.00 is the maximum amount of expenses payable annually for each fiscal year of the Province under this Agreement.

4. STATEMENTS OF ACCOUNT:

Statements of Account: In order to obtain payment of any fees and expenses under this Agreement for a period from and including the 1st day of a month to and including the last day of that month (each, a Billing Period”), the Contractor must deliver to the Province on a billing date after the Billing Period a written statement of account in a form satisfactory to the Province, without errors, containing:

- (a) the Contractor’s legal name and address;
- (b) the date of the invoice statement and supporting documents, and the Billing Period to which the statement pertains;
- (c) the Contractor’s calculation of all fees claimed under this Agreement for that Billing Period, including the number of CVSAs, reference checks, cancellation notices by the Province or candidate, candidate’s name, client organization and location, if applicable;
- (d) a chronological listing, in reasonable detail, of any travel expenses claimed by the Contractor for the Billing Period with receipts attached, if applicable, and, if the Contractor is claiming reimbursement of any GST or other applicable taxes paid or payable by the Contractor in relation to those expenses, a description of any credits, rebates, refunds or remissions the Contractor is entitled to from the relevant taxation authorities in relation to those taxes;
- (e) the Contractor’s calculation of any applicable taxes payable by the Province in relation to the Services for the Billing Period;
- (f) a description of this Agreement to which the statement relates; and
- (g) any other billing information reasonably requested by the Province.

5. PAYMENTS DUE:

Payments Due: Within 30 days of the Province’s receipt of the Contractor’s written statement of account delivered in accordance with this Schedule, the Province must pay the Contractor the fees and expenses (plus all applicable taxes) claimed in the statement if they are in accordance with this Schedule. Statements of account or contract invoices offering an early payment discount may be paid by the Province as required to obtain the discount.

DW

Schedule C – Approved Subcontractor(s)

Not applicable

De

Schedule D – Insurance

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Province:
 - (a) Commercial General Liability in an amount not less than \$2,000,000.00 inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
 - (i) include the Province as an additional insured,
 - (ii) be endorsed to provide the Province with 30 days advance written notice of cancellation or material change, and
 - (iii) include a cross liability clause.
2. All insurance described in section 1 of this Schedule must:
 - (a) be primary; and
 - (b) not require the sharing of any loss by any insurer of the Province.
3. The Contractor must provide the Province with evidence of all required insurance as follows:
 - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Province evidence of all required insurance in the form of a completed Province of British Columbia Certificate of Insurance;
 - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Province within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
 - (c) despite paragraph (a) or (b) above, if requested by the Province at any time, the Contractor must provide to the Province certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Schedule E – Privacy Protection Schedule

Definitions

1. In this Schedule,
 - (a) “**access**” means disclosure by the provision of access;
 - (b) “**Act**” means the *Freedom of Information and Protection of Privacy Act*;
 - (c) “**contact information**” means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
 - (d) “**personal information**” means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Province and the Contractor dealing with the same subject matter as the Agreement but excluding any such information that, if this Schedule did not apply to it, would not be under the “control of a public body” within the meaning of the Act; and
 - (e) “**privacy course**” means the Province’s online privacy and information sharing training course.

Purpose

2. The purpose of this Schedule is to:
 - (a) enable the Province to comply with the Province's statutory obligations under the Act with respect to personal information; and
 - (b) ensure that, as a service provider, the Contractor is aware of and complies with the Contractor's statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor’s obligations, or the exercise of the Contractor’s rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
 - (a) the purpose for collecting it;
 - (b) the legal authority for collecting it; and
 - (c) the title, business address and business telephone number of the person designated by the Province to answer questions about the Contractor’s collection of personal information.

Privacy Training

6. The Contractor must ensure that each person who will provide services under the Agreement that involve the collection or creation of personal information will complete, at the Contractor’s expense, the privacy course prior to that person providing those services.

DW

7. The requirement in section 6 will only apply to persons who have not previously completed the privacy course.

Accuracy of personal information

8. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Province to make a decision that directly affects the individual the information is about.

Requests for access to personal information

9. If the Contractor receives a request for access to personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province unless the Agreement expressly requires the Contractor to provide such access and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

10. Within 5 Business Days of receiving a written direction from the Province to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
11. When issuing a written direction under section 10, the Province must advise the Contractor of the date the correction request to which the direction relates was received by the Province in order that the Contractor may comply with section 12.
12. Within 5 Business Days of correcting or annotating any personal information under section 10, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Province, the Contractor disclosed the information being corrected or annotated.
13. If the Contractor receives a request for correction of personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

14. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

15. Unless the Province otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

16. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

17. Unless the Province otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of personal information

18. Unless the Province otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Province if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
19. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

20. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.2 of the Act, if in relation to personal information in the custody or under the control of the Contractor, the Contractor:
- (a) receives a foreign demand for disclosure;
 - (b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or
 - (c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure

the Contractor must immediately notify the Province and, in so doing, provide the information described in section 30.2(3) of the Act. In this section, the phrases "foreign demand for disclosure" and "unauthorized disclosure of personal information" will bear the same meanings as in section 30.2 of the Act.

Notice of unauthorized disclosure

21. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information in the custody or under the control of the Contractor, the Contractor must immediately notify the Province. In this section, the phrase "unauthorized disclosure of personal information" will bear the same meaning as in section 30.5 of the Act.

Inspection of personal information

22. In addition to any other rights of inspection the Province may have under the Agreement or under statute, the Province may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to the Contractor's management of personal information or the Contractor's compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

23. The Contractor must in relation to personal information comply with:
- (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
 - (b) any direction given by the Province under this Schedule.
24. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

25. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

26. In addition to any other rights of termination which the Province may have under the Agreement or otherwise at law, the Province may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

27. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
28. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
29. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
30. If a provision of the Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
31. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 32, the law of any jurisdiction outside Canada.
32. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

Schedule F – Additional Terms

Not applicable

DW

Schedule G – Security Schedule

Definitions

1. In this Schedule:

- (a) **“Device”** means any device to manage, operate or provide the Services or to connect to any Systems or any Province system or network, or that is capable of storing any Protected Information, and includes any workstation or handheld device the Contractor authorizes Personnel to use in relation to this Agreement;
- (b) **“Facilities”** means the physical locations (excluding those of the Province) the Contractor uses to provide the Services, or to house Systems or records containing Protected Information;
- (c) **“Least Privilege”** means the principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks so as to limit the damage that can result from accident, error or unauthorized use;
- (d) **“Need-to-Know”** means the principle where access is restricted to authorized individuals whose duties require such access and not merely because of status, rank or office;
- (e) **“Personnel”** means all individuals hired or used by the Contractor and Subcontractors to perform the Contractor’s obligations under this Agreement, including unpaid volunteers and the Contractor or a Subcontractor if an individual;
- (f) **“Policies”** means the intentions and directions of an organization or part of it, as expressed in record form by its top management (including, for example, policies, directions, standards, practices, procedures and guidelines);
- (g) **“Protected Information”** means any and all:
 - (i) “personal information” as defined in the Privacy Protection Schedule if attached;
 - (ii) information and records of information the Contractor is required to treat as confidential under this Agreement; and
 - (iii) records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked or instructed by the Province to be so preserved or otherwise treated as “Protected Information” under this Agreement;
- (h) **“Security Event Logs”** means any logs (also known as audit records) of events, notifications or alerts that any component of any Device or other device (not limited to security device), or any Systems or other system or software is technically capable of producing in relation to its status, functions and activities that may be used for such purposes as security investigations, auditing, monitoring and determining security incidents (examples of components capable of producing such logs include firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, dynamic host configuration protocols, dynamic naming services, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application firewalls);
- (i) **“Systems”** means any systems, subsystems, equipment, infrastructure, networks, management networks, servers, hardware and software the Contractor uses in relation to this Agreement, including for managing, operating or providing the Services, but excluding any the Province owns or makes available to the Contractor for the Contractor to use in relation to this Agreement;

- (j) **"Tenancy"** means those components of the Systems that:
 - (i) directly access and store Protected Information,
 - (ii) relate to Protected Information or the Province's tenancy activities, or
 - (iii) are customer facing and managed by the Province in its use of the Services; and
- (k) **"Tenancy Security Event Logs"** means Security Event Logs that relate to Tenancy, including:
 - (i) log-on/log-off information about Province user activities, and
 - (ii) application logs, web server log, file server logs, database logs of applications, web servers, file servers or database servers or any other logs that directly store, access or contain Protected Information.

Additional obligations

- 2. The Contractor must comply with Appendix G1 if attached.

PERSONNEL

Confidentiality agreements

- 3. The Contractor must not permit any person the Contractor hires or uses to access or obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under this Agreement.

Personnel security screening

- 4. The Contractor may only permit individual Personnel to have access to any Protected Information or other asset of the Province (including to any system, network or device the Province makes available to the Contractor) in relation to this Agreement, if, after:
 - (a) verifying their identity and relevant education, professional qualifications and employment history;
 - (b) completing a criminal record check that is updated at least every five years;
 - (c) requiring Personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law;
 - (d) performing any additional screening this Agreement or applicable law may require; and
 - (e) performing any additional background checks the Contractor considers appropriate,

the Contractor is satisfied that the individual does not constitute an unreasonable security risk.

- 5. If any criminal record check or proactive disclosure reveals a prior criminal offence or pending criminal matter, the Contractor must make a reasonable determination of whether the applicable person constitutes an unreasonable security risk, taking into consideration the duties of the individual and the type and sensitivity of information to which the individual may be exposed.

6. If the Contractor is an individual, the Province may subject the Contractor to the screening requirements in this Schedule.

Personnel information security training

7. Unless otherwise specified in this Agreement, the Contractor must ensure all Personnel complete any relevant information security training, at the Contractor's expense, before they provide any Services, or receive or are given access to any Protected Information or any system, device or secure facility of the Province, and thereafter at least annually.

Security contact

8. If not set out elsewhere in this Agreement, the Contractor (but not a Subcontractor) must provide in writing to the Province the contact information for the individual who will coordinate compliance by the Contractor and all Subcontractors and act as a direct contact for the Province on matters relating to this Schedule.

Supply chain

9. The Contractor must ensure that the security requirements of those in its upstream and downstream supply chain are documented, followed, reviewed, and updated on an ongoing basis as applicable to this Agreement.

GENERAL POLICIES AND PRACTICES

Information security policy

10. The Contractor must have an information security Policy that is:
 - (a) based on recognized industry standards; and
 - (b) reviewed and updated at least every three years.

Compliance and Standard for Security Controls

11. Unless this Agreement otherwise specifies, the Contractor must apply controls and security management practices to manage or operate Protected Information and Systems, Devices, and Facilities that are compliant with or equivalent to the following Province's Policies accessible at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>:
 - (a) "Information Security Policy";
 - (b) government wide IM/IT Standards; and
 - (c) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.

Contractor security risk assessments

12. The Contractor must undertake a security threat and risk assessment against an industry security standard before placing any new or materially changed Systems or services into production.

Change control and management

13. The Contractor must:

DW

- (a) implement and maintain change control processes for Facilities, Systems and Devices in line with applicable security best practices to reduce security-related risks with respect to implemented significant changes; and
- (b) ensure that adequate testing of any change is completed before the change is put into production.

Backups and restores

- 14. The Contractor must ensure that:
 - (a) it has a backup Policy that is followed and is reviewed, updated and tested at least annually;
 - (b) backups are taken and tested in accordance with the Contractor's backup Policy, but in any event at least annually; and
 - (c) frequency and completeness of backups is based on reasonable industry practice.

Business continuity plan and disaster recovery plan

- 15. The Contractor must ensure that it has a documented business continuity plan and a disaster recovery plan that is reviewed at least annually.
- 16. The Contractor must ensure that Facilities and Systems are protected from loss, damage or other occurrence, including fire and environmental hazards and power interruptions, that may result in any of those Facilities and Systems being unavailable when required to provide the Services.

Security Incident Response and Management

- 17. The Contractor must ensure that it has a security incident management Policy and response plan that is reviewed at least annually.

PROTECTED INFORMATION AND DATA SECURITY

Encryption

- 18. The Contractor must ensure that:
 - (a) encryption of data at rest is implemented and is maintained in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, for all Protected Information stored on Systems and Devices; and
 - (b) encryption end-to-end is implemented for all Protected Information in transit.

No storage on unencrypted portable media

- 19. The Contractor must ensure that no Protected Information is stored on portable media for transport outside of the Facilities or Systems without both the prior written approval of the Province and ensuring that the portable media and the Protected Information are encrypted.

Encryption standard

- 20. For sections 18 and 19, encryption must comply with the Province's "Cryptographic Standards for Information Protection" accessible at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>.

Isolation controls and logical isolation of data

21. The Contractor must implement and maintain the logical isolation of Protected Information, in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure.

ACCESS AND AUTHENTICATION

User Identifiers

22. The Contractor must assign and ensure that user identifiers are unique and personal for log in to Systems and Devices.

Access

23. The Contractor must implement, follow, and regularly review and update, access control Policies that address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts for Facilities, Systems and Devices within the Contractor's control.
24. The Contractor must ensure that all access to Protected Information and to Facilities, Systems and Devices is based Least Privilege and Need-to-Know" based on role and responsibilities. The Contractor must identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse.
25. The Contractor must verify an individual's identity before assigning the individual a unique identifier that would give them access to Facilities, Systems or Devices.
26. The Contractor must implement a formal user registration process for Personnel that includes:
 - (a) verification of access levels;
 - (b) creating and maintaining records of access privileges;
 - (c) audit processes; and
 - (d) actions to ensure access is not given before approval is granted by the Contractor.
27. The Contractor must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts.
28. The Contractor must implement a monitoring process to oversee, manage and review Personnel access rights and roles at regular intervals.
29. The Contractor must ensure that all Systems and Devices:
 - (a) are configured in alignment with industry standards;
 - (b) enforce a limit of consecutive invalid logon attempts by a user during a predetermined time period;
 - (c) automatically lock the applicable account and Systems after failed logon failures;
 - (d) limit the number of concurrent sessions;
 - (e) prevent further access to Systems by initiating a session lock; and
 - (f) provide the capability of disconnecting or disabling remote access to the Systems.

Authentication

30. The Contractor must use or require complex passwords or personal identification numbers (PINs) that are not shared, default or blank and that are encrypted (not displayed) when entered, biometric accesses, keys, smart cards, other logical or access controls, or combinations of them, to control access to Protected Information and to Systems and Devices.
31. The Contractor must ensure that Systems for password-based authentication:
 - (a) enforce minimum password complexity, including requiring passwords to be case sensitive, contain a minimum of eight characters and a combination of upper-case letters, lower-case letters, numbers, and/or special characters;
 - (b) change authentication passwords regularly at predetermined intervals, but at a minimum semi-annually;
 - (c) store and transmit only encrypted representations of passwords;
 - (d) enforce password minimum and maximum lifetime restrictions;
 - (e) prohibit password reuse;
 - (f) prevent reuse of identifiers; and
 - (g) disable the identifier after ninety days of inactivity.

Highly sensitive Protected Information

32. If this Agreement or the Province under this Agreement indicates that any Protected Information is highly sensitive, the Contractor must also ensure that Systems enforce with respect to that Protected Information:
 - (a) two-factor authentication for access;
 - (b) enhanced logging that logs all accesses;
 - (c) request based access; and
 - (d) no standing access rights.

SECURITY EVENT LOGS

Log generation, log retention and monitoring

33. The Contractor must ensure that logging of Security Event Logs is enabled on all applicable Systems components
34. The Contractor must retain Security Event Logs for the Systems online for a minimum of 90 days and either online or off-line for an additional period of time adequate to enable the Contractor to conduct effective security investigations into suspected or actual security incidents.
35. The Contractor must retain Tenancy Security Event Logs online for a minimum of 90 days and either:
 - (a) such additional period of time as the Province may instruct; or
 - (b) ensure that the Tenancy offers the technical capability for the Province to retain the Tenancy Security Event Logs,

to enable the Province to comply with an information schedule approved under the *Information Management Act* or other retention period required by law.

36. Upon the Province's request, the Contractor must ensure that the Tenancy offers the technical capability for the Province to enable or configure the forwarding, extraction, backup of Tenancy Security Event Logs from the Tenancy to the Province's security information and event management system or to an external log storage and retention system.
37. The Contractor must review Security Event Logs regularly to detect potential security incidents, using automated tools or equivalent processes for the monitoring, review, correlating and alerting of Security Event Logs.

PROVINCE PROPERTY

Access to Province facilities, systems or networks

38. If the Province makes available any facilities, systems, networks or devices for use of the Contractor in relation to this Agreement, the Contractor must comply with, and permit access on its behalf only by those authorized Personnel who have been instructed to comply with, the Province's Policies then applicable to their acceptable use, access and protection accessible at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>, including:
 - (a) "Appropriate Use Policy" (as also referenced in chapter 12 of the Province's "Core Policy and Procedures Manual");
 - (b) "Information Security Policy";
 - (c) government wide IM/IT Standards; and
 - (d) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.
39. The Province has the rights to:
 - (a) not make any particular Province facility, system, network or device available before the Contractor or individual Personnel or both agree to a form of agreement acceptable to the Province on acceptable use, protection of, and access to, such facility, system, network or device, or at all;
 - (b) not permit connection to any particular Province system or network until satisfied with the controls applied and the security status of the Device to be connected;
 - (c) keep facilities access logs and Security Event Logs, and to otherwise monitor and analyze use of Province facilities, systems and networks to verify compliance, investigate suspected or actual breaches or information incidents and protect the Province's assets, including records, in compliance with applicable laws, including the *Freedom of Information and Protection of Privacy Act* and *Information Management Act*, and the Province's Policies; and
 - (d) limit or revoke access to any Province systems, facility or device at its discretion.

Application development

40. If the Services include software development, the Contractor must ensure that the applications and programming interfaces are developed according to industry standards and Province's Policies applicable to application development standards. The Contractor must use secure application development practices for the development of the software.

FACILITIES, SYSTEMS, DATABASE AND DEVICE SECURITY

Physical security

41. The Contractor must ensure that adequate physical controls and processes are implemented to ensure that only authorized persons have physical access to the Facilities and Systems.
42. The Contractor must develop, document, and disseminate a physical and environmental protection Policy that it reviews at least annually.
43. The Contractor must review physical access logs at least once monthly.
44. The Contractor must ensure that physical security of any Systems or Facilities being used or capable of being used to house Protected Information meets a standard as would be reasonably expected to provide adequate protection based on the value of the data being protected and the environment in which the Systems or Facilities are located. At a minimum, this should include:
 - (a) hardening of the perimeter of the Facilities;
 - (b) physical separation of public and restricted spaces;
 - (c) Intrusion Alarm System (IAS) partitioned to ensure areas containing Protected Information are protected at all times;
 - (d) Access Control Systems (ACS) and/or Key Management processes; and
 - (e) visitor and identity management processes – including access logs and identification badges.

Separation of production from test environments

45. The Contractor must not use any production data in any development, test or training environments used for the Services without the Province's prior written consent. If the Province gives such consent, the production data must, at minimum, be obfuscated (for example, by using data masking functionality).
46. The Contractor must keep its development, test and training environments separate from its production environments used for the Services at all times, even in case of failure.

Systems (including servers) hardening

47. The Contractor must:
 - (a) harden all Systems against attack and misuse, using appropriate security best practices for the hardening of the specific deployed platform, before placing those Systems into production;
 - (b) ensure that all unsecured and unneeded ports, services, applications, protocols and network communicating applications are uninstalled or disabled on all Systems;
 - (c) applying Least Privilege, ensure that the Contractor only configures and makes operational ports, services, applications, protocols and network communicating applications based on the functional requirements of the respective Systems;
 - (d) ensure that default passwords and shared accounts are not used for any Systems; and

- (e) in relation to Systems, implement server hardening using configuration security best practices (for example, Center for Internet Security, Inc. (CIS) Benchmarks or equivalent) for any server operating systems, server virtualization, server middleware (for example, web servers and database servers) and application servers.

Perimeter controls (firewall and intrusion prevention system) and network security

48. The Contractor must:

- (a) implement stateful packet inspection firewalls to control traffic flow to and from Systems and Tenancy at all times, and configure the stateful packet inspection firewalls applying security best practices and Least Privilege;
- (b) implement an intrusion prevention System to control and filter traffic flow leaving and entering Systems and Tenancy at all times, and configure the intrusion prevention System applying security best practices; and
- (c) implement a secure network perimeter and network segmentation for Systems, with ingress and egress points that are known and controlled.

Application firewall

49. The Contractor must implement application layer firewalls on Systems:

- (a) at such level of protection as the Province may instruct ; and
- (b) to detect and mitigate application attacks (for example, brute force, OWASP Top 10, SQL injection, cross site scripting).

Management network

50. The Contractor must ensure that for any Systems:

- (a) the management network remains logically separated from any other zone and is not directly accessible from the Internet;
- (b) the management network is internally segmented, with each server's dedicated network interface on its own segmented network and that interfaces on the management network do not have visibility to each other; and
- (c) all access to the management network is strictly controlled and exclusively enforced through a secure access gateway, bastion host or equivalent.

Remote management and secure access gateway

51. The Contractor must perform any remote management of Systems or Devices in a secure manner, using encrypted communication channels and adequate access controls.

Database security

52. The Contractor must ensure that for any Systems:

- (a) database maintenance utilities that bypass controls are restricted and monitored;

- (b) there is a formal approval process in place for handling requests for disclosure of database contents or for database access, including steps to evaluate privacy impacts and security risks of such requests; and
 - (c) methods to check and maintain the integrity of the data are implemented (for example, consistency checks and checksums).
53. For database security, the Contractor must implement logical isolation and encryption of Protected Information.

Device security and antivirus scanning

54. The Contractor must ensure all Devices:
- (a) have antivirus and malware protection as appropriate for the particular Device active at all times;
 - (b) are configured to perform antivirus scans at least once per week;
 - (c) have host based firewall configured, enabled and active at all times; and
 - (d) have all patches and appropriate security updates installed for the operating system and all installed software.

VULNERABILITY PREVENTION, SCANNING AND MANAGEMENT

Proactive management

55. The Contractor must:
- (a) obtain information in a timely basis about technical vulnerabilities relating to Systems and Devices; and
 - (b) implement processes to stay current with security threats.

Patching

56. The Contractor must patch all Systems regularly in line with security best practices and ensure that current software, operating systems and application patching levels are maintained.
57. The Contractor must ensure that all Systems have all patches installed on a regular schedule, within the time frame recommended by the manufacturer unless the Province otherwise consents in writing.
58. The Contractor must ensure that vulnerabilities are remedied and patches installed on an accelerated basis for zero-day, critical and high vulnerabilities. For zero-day vulnerabilities, the Contractor must implement appropriate mitigation measures promptly on notification of the zero-day vulnerability. The Contractor must remediate zero-day, high and critical vulnerabilities through patching, decommission, or compensating controls.
59. The Contractor must patch high vulnerabilities within 30 days or less of discovery and patch medium vulnerabilities within 90 days or less of discovery.

Vulnerability Scanning

60. The Contractor must ensure that a vulnerability scan is completed on components of all Systems:
- (a) with any identified vulnerabilities remedied, before being placed into production; and

DW

- (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Web application vulnerability scanning

- 61. The Contractor must ensure that a vulnerability scan is completed on any web applications used for Tenancy or in any other Systems:
 - (a) and on any major changes to such web applications, with any identified vulnerabilities remedied, before being placed into production; and
 - (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Antivirus and malware scanning

- 62. The Contractor must ensure that all Systems servers:
 - (a) have antivirus and malware protection configured, active and enabled at all times;
 - (b) have antivirus and malware definitions updated at least once a day; and
 - (c) are configured to undergo a full anti-virus scan for latent infections (to detect infections missed by the real-time agent) at least once a week.

DISPOSALS

Asset disposal

- 63. The Contractor must ensure that all disposals of assets used in providing or relating to the Services are done in a secure manner that ensures that Protected Information cannot be recovered.

Asset management

- 64. The Contractor must have asset management and disposal Policies that are followed, and reviewed and updated regularly in line with security best practices, and that address hardware, software and other critical business assets.
- 65. The Contractor must keep an asset management inventory that includes the name of the System, location, purpose, owner, and criticality, with assets added to inventory on commission and removed on decommission.

Information destruction and disposal

- 66. The Contractor must retain all records containing Protected Information in the Contractor's possession for one year minimum unless otherwise instructed by the Province in writing to dispose or deliver them.
- 67. The Contractor must securely erase:
 - (a) records that contain Protected Information and Tenancy Security Event Logs when instructed in writing by the Province; and
 - (b) any backup, transitory and extra copies of records that contain Protected Information or Tenancy Security Event Logs when no longer needed in relation to this Agreement.

68. The Contractor must ensure that Protected Information and Tenancy Security Event Logs on magnetic media are securely wiped by overwriting using procedures and adequate media wiping solutions, degaussing, or other method in line with security best practices for disposal of media.

NOTICES, INCIDENTS AND INVESTIGATIONS

Notice of demands for disclosure

69. In addition to any obligation the Contractor may have to notify or assist the Province under applicable law or this Agreement, including the Privacy Protection Schedule if attached, if the Contractor is required (including under an enactment or a subpoena, warrant, order, demand or other request from a court, government agency or other legal authority) to produce, provide access to or otherwise disclose any Protected Information, the Contractor must, unless prohibited by applicable law, immediately notify and provide reasonable assistance to the Province so the Province may seek a protective order or other remedy to prevent or limit the disclosure.

E-discovery and legal holds

70. The Contractor must fully co-operate with the Province to enable the Province to comply with e-discovery and legal hold obligations.

Incidents

71. In addition to any obligation the Contractor may have under applicable law, including the *Freedom of Information and Protection of Privacy Act*, or this Agreement, if, during or after the Term, the Contractor discovers a suspected or actual unwanted or unexpected event or series of events that threaten the privacy or security of Protected Information (including its unauthorized access, collection, use, disclosure, alteration, storage or disposal) or Tenancy, whether accidental or deliberate, the Contractor must:
- (a) immediately report the particulars of such incident to, and follow the instructions of, the Province, confirming any oral report with a notice in writing to the Province as soon as reasonably practicable (if unable to contact the Province's contract manager or other designated contact for this Agreement, the Contractor must follow the procedure for reporting and managing information incidents on the Province's website at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents>; and
 - (b) make every reasonable effort to recover the records containing Protected Information and contain and remediate such incident, following such reasonable instructions as the Province may give.

Investigations support and security investigations

72. The Contractor must:
- (a) conduct security investigations in the case of incidents (including any security breach or compromise) affecting Devices, Facilities, Systems, Tenancy or Protected Information, collecting evidence, undertaking forensic activities and taking such other actions as needed;
 - (b) provide the Province with any related investigation reports, which the Contractor may sanitize first;
 - (c) upon the Province's request, provide the Province with any logs relating to such investigation reports as validation/confirmation of such investigation, which the Contractor may sanitize first; and
 - (d) maintain a chain of custody in all such security investigations it undertakes.

73. Upon the Province's request, the Contractor must:
- (a) provide investigative support to the Province to enable the Province to conduct its own security investigations into incidents (including security breaches or compromises) affecting the Tenancy or Protected Information;
 - (b) provide the Province with timely access via an on-line, real-time GUI (Graphic User Interface) facility to any Tenancy Security Event Logs and to other Security Event Logs for Systems (the latter of which the Contractor may sanitize first to mask or remove, for example, data pertaining to the Contractor's customers) to assist the Province in conducting the Province's security investigations, or in case of technical limitations, other method acceptable to the Province (for example, on-site visits to enable direct access to those Security Event Logs).
74. The Contractor must work with and support the Province if the Province needs assistance in legal proceedings in relation to security investigations related to Protected Information or Tenancy.

Province Security Threat and Risk Assessment ("STRA") support

75. The Contractor must, via its technical and security resources, support the Province in completing a STRA for the Services and to otherwise assess the risks associated with the Services, including by providing all information and documentation (for example, architecture diagrams, service architecture, controls architecture and technical information), which the Contractor may sanitize first and that the Province may reasonably require for such purpose.

Notification of changes

76. The Contractor must notify the Province of any changes to its security Policies, management practices and security controls described in this Agreement that may potentially negatively impact the security of Tenancy, Protected Information, or those Systems providing the Services.

Compliance verification

77. Upon the Province's request, the Contractor must provide, at no additional cost, the following security reports to the Province at least every six months during the Term:
- (a) vulnerability scan reports of those Systems providing the Services; and
 - (b) patch status reports for those Systems providing the Services.
78. In addition to any other rights of inspection the Province may have under this Agreement or under statute, the Province has the rights, at any reasonable time and on reasonable notice to the Contractor, to:
- (a) request the Contractor to verify compliance with this Schedule and to keep security controls documentation or records to support compliance; and
 - (b) enter on the Contractor premises and Facilities to inspect and to validate the Contractor's compliance with the security obligations under this Agreement
79. The Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province's rights under this section. If any non-compliance or deficiency is found, the Province may (in addition to any other rights it may have) require the Contractor, at the Contractor's expense, to develop and implement a corrective action plan within a reasonable time.

Notice of non-compliance

80. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

MISCELLANEOUS

Interpretation

81. In this Schedule, unless otherwise specified, references to sections by number are to sections of this Schedule.
82. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under this Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
83. Any reference to a specified Policy refers to it as may be revised or replaced from time to time.
84. If a provision of this Schedule conflicts with a documented process required by this Schedule to be created or maintained by the Contractor, the provision of the Schedule will prevail to the extent of the conflict.

Referenced documents

85. Policies and other documents of the Province referenced in this Schedule may be updated or replaced by the Province from time to time without notice, and if not found at the hyperlink or URL provided or via the Province's main website at <http://www.gov.bc.ca>, be obtained from the Province's contact for this Agreement.

Survival

86. Sections 63, 66, 67, 68, 69, 70, and 71 and other obligations of the Contractor in this Schedule which, by their terms or nature, are intended to survive the completion of the Services or the termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedule G – Appendix G1 – Additional Security Obligations

The personnel security screening requirements set out in this Appendix G1 are for the purpose of assisting the Contractor determine whether or not a candidate constitutes an unreasonable security risk.

Verification of name, date of birth and address

1. The Contractor must verify the name, date of birth and current address of a candidate by viewing at least one piece of “primary identification” of the candidate and at least one piece of “secondary identification” of the candidate,* as described in the table following this section. The Contractor must obtain or create, as applicable, Records of all such verifications and retain a copy of those Records. For a candidate from another province or jurisdiction, reasonably equivalent identification documents are acceptable.

Primary Identification	Secondary Identification
<p>Issued by ICBC:</p> <ul style="list-style-type: none"> ▪ B.C. driver’s licence or learner’s licence (must have photo) ▪ B.C. Identification (BCID) card <p>Issued by provincial or territorial government:</p> <ul style="list-style-type: none"> ▪ Canadian birth certificate <p>Issued by Government of Canada:</p> <ul style="list-style-type: none"> • Canadian Citizenship Card • Permanent Resident Card • Canadian Record of Landing/Canadian Immigration Identification Record 	<ul style="list-style-type: none"> • School ID card (student card) • Bank card (only if holder’s name is on card) • Credit card (only if holder’s name is on card) • Passport • Foreign birth certificate (a baptismal certificate is not acceptable) • Canadian or U.S. driver’s licence • Naturalization certificate • Canadian Forces identification • Police identification • Foreign Affairs Canada or consular identification • Vehicle registration (only if owner’s signature is shown) • Picture employee ID card • Firearms Acquisition Certificate • Social Insurance Card (only if has signature strip) • B.C. CareCard • Native Status Card • Parole Certificate ID • Correctional Service Conditional Release Card

*It is not necessary that each piece of identification viewed by the Contractor contains the name, date of birth and current address of the candidate. It is sufficient that, in combination, the identification viewed contains that information.

Verification of education and professional qualifications

2. The Contractor must verify, by reasonable means, any relevant education and professional qualifications of a candidate, obtain or create, as applicable, Records of all such verifications, and retain a copy of those Records.

Verification of employment history and reference checks

3. The Contractor must verify, by reasonable means, any relevant employment history of a candidate, which will generally consist of the Contractor requesting that a candidate provide employment references and the Contractor contacting those references. If a candidate has no relevant employment history, the Contractor must seek to verify the character or other relevant personal characteristics of the candidate by requesting the candidate to provide one or more personal references and contacting those references. The Contractor must obtain or create, as applicable, Records of all such verifications and retain a copy of those Records.

Security interview

4. The Contractor must allow the Province to conduct a security-focused interview with a candidate if the Province identifies a reasonable security concern and notifies the Contractor it wishes to do so.

DW

GENERAL SERVICE AGREEMENT



For Administrative Purposes Only

Ministry Contract No.: SGPSB21C503

Requisition No.: _____

Solicitation No.(if applicable): _____

Commodity Code: _____

Contractor Information

Supplier Name: LorDen Consulting

Supplier No.: _____

Telephone No.: 604-319-7789

E-mail Address: lordenconsulting@gmail.com

Website: _____

Financial Information

Client: 010

Responsibility Centre: 15408

Service Line: 11710

STOB: 6001

Project: 1500000

Template version: February 20, 2020

TABLE OF CONTENTS

No.	Heading	Page
1.	Definitions	1
1.1	General	1
1.2	Meaning of "record"	2
2.	Services	2
2.1	Provision of services.....	2
2.2	Term.....	2
2.3	Supply of various items.....	2
2.4	Standard of care.....	2
2.5	Standards in relation to persons performing Services	2
2.6	Instructions by Province	2
2.7	Confirmation of non-written instructions	2
2.8	Effectiveness of non-written instructions.....	2
2.9	Applicable laws	2
3.	Payment	3
3.1	Fees and expenses	3
3.2	Statements of accounts.....	3
3.3	Withholding of amounts.....	3
3.4	Appropriation.....	3
3.5	Currency.....	3
3.6	Non-resident income tax.....	3
3.7	Prohibition against committing money	3
3.8	Refunds of taxes	4
4.	Representations and Warranties	4
5.	Privacy, Security and Confidentiality	4
5.1	Privacy.....	4
5.2	Security.....	4
5.3	Confidentiality.....	4
5.4	Public announcements	5
5.5	Restrictions on promotion	5
6.	Material and Intellectual Property	5
6.1	Access to Material	5
6.2	Ownership and delivery of Material	5
6.3	Matters respecting intellectual property	5
6.4	Rights relating to Incorporated Material.....	5
7.	Records and Reports	6
7.1	Work reporting	6
7.2	Time and expense records	6
8.	Audit	6

9.	Indemnity and Insurance	6
9.1	Indemnity	6
9.2	Insurance	6
9.3	Workers compensation	6
9.4	Personal optional protection	6
9.5	Evidence of coverage	7
10.	Force Majeure	7
10.1	Definitions relating to force majeure	7
10.2	Consequence of Event of Force Majeure	7
10.3	Duties of Affected Party	7
11.	Default and Termination	7
11.1	Definitions relating to default and termination	7
11.2	Province's options on default	8
11.3	Delay not a waiver	8
11.4	Province's right to terminate other than for default	8
11.5	Payment consequences of termination	8
11.6	Discharge of liability	8
11.7	Notice in relation to Events of Default	9
12.	Dispute Resolution	9
12.1	Dispute resolution process	9
12.2	Location of arbitration or mediation	9
12.3	Costs of mediation or arbitration	9
13.	Miscellaneous	9
13.1	Delivery of notices	9
13.2	Change of address or fax number	10
13.3	Assignment	10
13.4	Subcontracting	10
13.5	Waiver	10
13.6	Modifications	10
13.7	Entire agreement	10
13.8	Survival of certain provisions	10
13.9	Schedules	10
13.10	Independent contractor	11
13.11	Personnel not to be employees of Province	11
13.12	Key Personnel	11
13.13	Pertinent Information	11
13.14	Conflict of interest	11
13.15	Time	11
13.16	Conflicts among provisions	11
13.17	Agreement not permit nor fetter	11
13.18	Remainder not affected by invalidity	12
13.19	Further assurances	12
13.20	Additional terms	12
13.21	Tax Verification	12
13.22	Governing law	12
14.	Interpretation	12
15.	Execution and Delivery of Agreement	12

SCHEDULE A – SERVICES

- Part 1 - Term**
- Part 2 - Services**
- Part 3 - Related Documentation**
- Part 4 - Key Personnel**

SCHEDULE B – FEES AND EXPENSES

- Part 1 - Maximum Amount Payable**
- Part 2 - Fees**
- Part 3 - Expenses**
- Part 4 - Statements of Account**
- Part 5 - Payments Due**

SCHEDULE C – APPROVED SUBCONTRACTOR(S)

SCHEDULE D – INSURANCE

SCHEDULE E – PRIVACY PROTECTION SCHEDULE

SCHEDULE F – ADDITIONAL TERMS

SCHEDULE G – SECURITY SCHEDULE

SCHEDULE H – TAX VERIFICATION

THIS AGREEMENT is dated for reference the 22nd day of January 2021.

BETWEEN:

LorDen Consulting (the "Contractor") with the following specified address and phone number:
PO Box 26074 Langley Mall PO
Langley BC
V3A 8J2
604-319-7789

AND:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, as represented by the Minister of Public Safety and Solicitor General (the "Province") with the following specified address and fax number:

Policing and Security Branch
Security Programs Division
PO Box 9285 Stn Prov Govt
3350 Douglas Street
Victoria, British Columbia
V8Z3L1
FAX: (250) 356-5987

The Province wishes to retain the Contractor to provide the services specified in Schedule A and, in consideration for the remuneration set out in Schedule B, the Contractor has agreed to provide those services, on the terms and conditions set out in this Agreement.

As a result, the Province and the Contractor agree as follows:

1 DEFINITIONS

General

1.1 In this Agreement, unless the context otherwise requires:

- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
- (b) "Incorporated Material" means any material in existence prior to the start of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
- (c) "Material" means the Produced Material and the Received Material;
- (d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced or provided by the Contractor or a Subcontractor and includes the Incorporated Material;
- (e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Province or any other person;
- (f) "Services" means the services described in Part 2 of Schedule A;
- (g) "Subcontractor" means a person described in paragraph (a) or (b) of section 13.4; and
- (h) "Term" means the term of the Agreement described in Part 1 of Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of “record”

- 1.2 The definition of “record” in the *Interpretation Act* is incorporated into this Agreement and “records” will bear a corresponding meaning.

2 SERVICES

Provision of services

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor’s obligations under this Agreement, including the license under section 6.4.

Standard of care

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by Province

- 2.6 The Province may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are carried out.

Confirmation of non-written instructions

- 2.7 If the Province provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Province in writing, which request the Province must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

- 2.9 In the performance of the Contractor’s obligations under this Agreement, the Contractor must comply with all applicable laws.

3 PAYMENT

Fees and expenses

- 3.1 If the Contractor complies with this Agreement, then the Province must pay to the Contractor at the times and on the conditions set out in Schedule B:
- (a) the fees described in that Schedule;
 - (b) the expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Province's opinion, are necessarily incurred by the Contractor in providing the Services; and
 - (c) any applicable taxes payable by the Province under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Province is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Province a written statement of account in a form satisfactory to the Province upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

- 3.3 Without limiting section 9.1, the Province may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Province and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Province to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Province.

Appropriation

- 3.4 The Province's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Province during which payment becomes due.

Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are to Canadian dollars.

Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Province may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

- 3.7 Without limiting section 13.10(a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Province to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

- 3.8 The Contractor must:
- (a) apply for, and use reasonable efforts to obtain, any available refund, credit, rebate or remission of federal, provincial or other tax or duty imposed on the Contractor as a result of this Agreement that

the Province has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement; and

- (b) immediately on receiving, or being credited with, any amount applied for under paragraph (a), remit that amount to the Province.

4 REPRESENTATIONS AND WARRANTIES

4.1 As at the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Province as follows:

- (a) except to the extent the Contractor has previously disclosed otherwise in writing to the Province,
 - (i) all information, statements, documents and reports furnished or submitted by the Contractor to the Province in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,
 - (ii) the Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractual or other agreements in place and available to enable the Contractor to fully perform the Services and to grant any licenses under this Agreement, and
 - (iii) the Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and
- (b) if the Contractor is not an individual,
 - (i) the Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and
 - (ii) this Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:

- (a) make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, alteration or disposal; and
- (b) comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Province's prior written consent except:

- (a) as required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
- (b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or

- (c) if it is information in any Incorporated Material.

Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Province and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

- 5.5 The Contractor must not, without the prior written approval of the Province, refer for promotional purposes to the Province being a customer of the Contractor or the Province having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Province, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Province.

Ownership and delivery of Material

- 6.2 The Province exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Province immediately upon the Province's request.

Matters respecting intellectual property

- 6.3 The Province exclusively owns all intellectual property rights, including copyright, in:
 - (a) Received Material that the Contractor receives from the Province; and
 - (b) Produced Material, other than any Incorporated Material.

Upon the Province's request, the Contractor must deliver to the Province documents satisfactory to the Province that irrevocably waive in the Province's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Province of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Province:
 - (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to exercise, in respect of that Incorporated Material, the rights set out in the *Copyright Act* (Canada), including the right to use, reproduce, modify, publish and distribute that Incorporated Material; and
 - (b) the right to sublicense or assign to third-parties any or all of the rights granted to the Province under section 6.4(a).

7 RECORDS AND REPORTS

Work reporting

- 7.1 Upon the Province's request, the Contractor must fully inform the Province of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Province. Unless otherwise specified in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement ends.

8 AUDIT

- 8.1 In addition to any other rights of inspection the Province may have under statute or otherwise, the Province may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Province's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

- 9.1 The Contractor must indemnify and save harmless the Province and the Province's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Province or any of the Province's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "Loss") to the extent the Loss is directly or indirectly caused or contributed to by:
- (a) any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or
 - (b) any representation or warranty of the Contractor being or becoming untrue or incorrect.

Insurance

- 9.2 The Contractor must comply with the Insurance Schedule attached as Schedule D.

Workers compensation

- 9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

- 9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- (a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
 - (b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

- 9.5 Within 10 Business Days of being requested to do so by the Province, the Contractor must provide the Province with evidence of the Contractor's compliance with sections 9.3 and 9.4.

10 FORCE MAJEURE

Definitions relating to force majeure

10.1 In this section and sections 10.2 and 10.3:

- (a) “Event of Force Majeure” means one of the following events:
 - (i) a natural disaster, fire, flood, storm, epidemic or power failure,
 - (ii) a war (declared and undeclared), insurrection or act of terrorism or piracy,
 - (iii) a strike (including illegal work stoppage or slowdown) or lockout, or
 - (iv) a freight embargoif the event prevents a party from performing the party’s obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
- (b) “Affected Party” means a party prevented from performing the party’s obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party’s obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party’s obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

- (a) “Event of Default” means any of the following:
 - (i) an Insolvency Event,
 - (ii) the Contractor fails to perform any of the Contractor’s obligations under this Agreement, or
 - (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and
- (b) “Insolvency Event” means any of the following:
 - (i) an order is made, a resolution is passed or a petition is filed, for the Contractor’s liquidation or winding up,
 - (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor’s creditors or otherwise acknowledges the Contractor’s insolvency,
 - (iii) a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
 - (iv) a compromise or arrangement is proposed in respect of the Contractor under the *Companies’ Creditors Arrangement Act* (Canada),
 - (v) a receiver or receiver-manager is appointed for any of the Contractor’s property, or
 - (vi) the Contractor ceases, in the Province’s reasonable opinion, to carry on business as a going concern.

Province's options on default

- 11.2 On the happening of an Event of Default, or at any time thereafter, the Province may, at its option, elect to do any one or more of the following:
- (a) by written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
 - (b) pursue any remedy or take any other action available to it at law or in equity; or
 - (c) by written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

- 11.3 No failure or delay on the part of the Province to exercise its rights in relation to an Event of Default will constitute a waiver by the Province of such rights.

Province's right to terminate other than for default

- 11.4 In addition to the Province's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Province may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

- 11.5 Unless Schedule B otherwise provides, if the Province terminates this Agreement under section 11.4:
- (a) the Province must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Province's satisfaction before termination of this Agreement; and
 - (b) the Contractor must, within 30 days of such termination, repay to the Province any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Province has notified the Contractor in writing was not completed to the Province's satisfaction before termination of this Agreement.

Discharge of liability

- 11.6 The payment by the Province of the amount described in section 11.5(a) discharges the Province from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

- 11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Province of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

- 12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
- (a) the parties must initially attempt to resolve the dispute through collaborative negotiation;

- (b) if the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the Mediate BC Society; and
- (c) if the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Arbitration Act*.

Location of arbitration or mediation

- 12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

- 12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

- 13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
- (a) by fax to the addressee's fax number specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
 - (b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
 - (c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or fax number

- 13.2 Either party may from time to time give notice to the other party of a substitute address or fax number, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or fax number specified for the party giving the notice.

Assignment

- 13.3 The Contractor must not assign any of the Contractor's rights or obligations under this Agreement without the Province's prior written consent. Upon providing written notice to the Contractor, the Province may assign to any person any of the Province's rights under this Agreement and may assign to any "government corporation", as defined in the *Financial Administration Act*, any of the Province's obligations under this Agreement.

Subcontracting

- 13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Province's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
- (a) any person retained by the Contractor to perform obligations under this Agreement; and
 - (b) any person retained by a person described in paragraph (a) to perform those obligations fully complies with this Agreement in performing the subcontracted obligations.

Waiver

- 13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

- 13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

- 13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to performance of the Services.

Survival of certain provisions

- 13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedules

- 13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

- 13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:
- (a) an employee or partner of the Province; or
 - (b) an agent of the Province except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Province

- 13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Province.

Key Personnel

- 13.12 If one or more individuals are specified as “Key Personnel” of the Contractor in Part 4 of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor’s behalf, unless the Province otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

- 13.13 The Province must make available to the Contractor all information in the Province’s possession which the Province considers pertinent to the performance of the Services.

Conflict of interest

- 13.14 The Contractor must not provide any services to any person in circumstances which, in the Province’s reasonable opinion, could give rise to a conflict of interest between the Contractor’s duties to that person and the Contractor’s duties to the Province under this Agreement.

Time

- 13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

- 13.16 Conflicts among provisions of this Agreement will be resolved as follows:
- (a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
 - (b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

- 13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Province or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Province or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

- 13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

- 13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

- 13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Tax Verification

13.21 Any terms set out in the attached Schedule H apply to this Agreement.

Governing law

13.22 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION


14.1 In this Agreement:

- (a) "includes" and "including" are not intended to be limiting;
- (b) unless the context otherwise requires, references to sections by number are to sections of this Agreement;
- (c) the Contractor and the Province are referred to as "the parties" and each of them as a "party";
- (d) "attached" means attached to this Agreement when used in relation to a schedule;
- (e) unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
- (f) the headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
- (g) "person" includes an individual, partnership, corporation or legal entity of any nature; and
- (h) unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

15 EXECUTION AND DELIVERY OF AGREEMENT

15.1 This Agreement may be entered into by a separate copy of this Agreement being executed by, or on behalf of, each party and that executed copy being delivered to the other party by a method provided for in section 13.1 or any other method agreed to by the parties.

The parties have executed this Agreement as follows:

<p>SIGNED on the <u>23</u> day of <u>JANUARY</u>, 2021 by the Contractor (or, if not an individual, on its behalf by its authorized signatory or signatories):</p> <p> _____ Signature(s)</p> <p><u>Dennis Paulson</u> _____ Print Name(s)</p> <p><u>OWNER/OPERATOR of LONDON</u> _____ Print Title(s) <u>CONSULTING</u></p>	<p>SIGNED on the ____ day of _____, 2021 on behalf of the Province by its duly authorized representative:</p> <p>_____ Signature</p> <p><u>Jess Gunnarson</u> _____ Print Name</p> <p><u>Executive Director, Security Programs</u> _____ Print Title</p>
---	--

Schedule A – Services

PART 1. TERM:

- The Term of this Agreement commences on February 1, 2021 and ends on March 31, 2023.
- This Agreement may be renewed for one additional Term of 24 months at the sole discretion of the Province, subject to satisfactory performance by the Contractor and the availability of funding by the Province.

PART 2. SERVICES:

- The enhanced security screening process is completed by the Personnel Security Screening Office (PSSO) at Security Programs Division on behalf of client organizations.
- Polygraph examinations are used in conjunction with security interviews to assess employees' risk to work at and/or with a client group organization.

The Contractor must:

- Have their own polygraph examination equipment;
- Have the staffing resources to ensure that they can provide the polygraph examinations required by the client group;
- Be able to provide polygraph examinations at the client group's location;
- Have certification confirming all polygraph examination providers have been trained in providing polygraphs;
- Ensure all polygraph examination providers have at least five years of experience providing polygraph examinations;
- Work with the PSSO to schedule polygraph examinations with the client groups identified by the PSSO at the location specified by the client group;
- Reliably and professionally attend, conduct, and complete scheduled polygraph examinations in person with groups or individuals identified by the PSSO;
- Conduct pre-test interviews using standardized questions based on a "lifestyle questionnaire" created by the PSSO to evaluate the honesty and integrity of the answers provided by candidates during the pre-employment selection process; and,
- Following pre-test interviews, conduct polygraph examinations which assess the truthfulness of candidate responses through control and analytical or investigative questions in areas such as criminal or undesirable activity, employment, education and financial history, and personal associations.

Reporting requirements

The Contractor must:

- Provide a written report of the results of each polygraph examination to the PSSO, or an authorized delegate, within two (2) business days following completion of the polygraph examination.
- The contractor will audio record all polygraph examinations and will enable the PSSO, or an authorized delegate, access to the audio recording upon request up to two (2) years from the date the polygraph examination was conducted. Records must be maintained during this period in a way consistent with Schedule E and G.

PART 3. RELATED DOCUMENTATION:

1. The Contractor must perform the Services in accordance with the obligations set out in this Schedule A including any engagement letter, Solicitation document excerpt, proposal excerpt or other documentation attached as an Appendix to, or specified as being incorporated by reference in, this Schedule.

PART 4. KEY PERSONNEL:

1. The Key Personnel of the Contractor are as follows:

Dennis Paulson

Schedule B – Fees and Expenses

1. MAXIMUM AMOUNT PAYABLE:

Maximum Amount:

Despite sections 2 and 3 of this Schedule, \$20,000.00 is the maximum amount which the Province is obliged to pay to the Contractor for fees and expenses under this Agreement (exclusive of any applicable taxes described in section 3.1(c) of this Agreement).

2. FEES:

Rate per Unit/Deliverable

Fees: at a rate of \$500 for each unit provided by the Contractor as Services during the Term up to 40 units. A unit means each complete polygraph examination and associated polygraph examination report.

3. EXPENSES:

Not Applicable

4. STATEMENTS OF ACCOUNT:

Statements of Account: In order to obtain payment of any fees and expenses under this Agreement for a period from and including the 1st day of a month to and including the last day of that month (each a "Billing Period"), the Contractor must deliver to the Province on a date after the Billing Period (each a "Billing Date"), a written statement of account in a form satisfactory to the Province containing:

- (a) the Contractor's legal name and address;
- (b) the date of the statement, and the Billing Period to which the statement pertains;
- (c) the Contractor's calculation of all fees claimed for that Billing Period, including a declaration by the Contractor of all (units/deliverables) provided during the Billing Period for which the Contractor claims fees and a description of the applicable fee rates;
- (d) a chronological listing, in reasonable detail, of any expenses claimed by the Contractor for the Billing Period with receipts attached, if applicable, and, if the Contractor is claiming reimbursement of any GST or other applicable taxes paid or payable by the Contractor in relation to those expenses, a description of any credits, rebates, refunds or remissions the Contractor is entitled to from the relevant taxation authorities in relation to those taxes;
- (e) the Contractor's calculation of any applicable taxes payable by the Province in relation to the Services for the Billing Period;
- (f) a description of this Agreement;
- (g) a statement number for identification; and
- (h) any other billing information reasonably requested by the Province.

5. PAYMENTS DUE:

Payments Due: Within 30 days of the Province's receipt of the Contractor's written statement of account delivered in accordance with this Schedule, the Province must pay the Contractor the fees and expenses (plus all applicable taxes) claimed in the statement if they are in accordance with this Schedule. Statements of account or contract invoices offering an early payment discount may be paid by the Province as required to obtain the discount.

Schedule C – Approved Subcontractor(s)

Not Applicable

Schedule D – Insurance

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Province:
 - (a) Commercial General Liability in an amount not less than \$2,000,000.00 inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
 - (i) include the Province as an additional insured,
 - (ii) be endorsed to provide the Province with 30 days advance written notice of cancellation or material change, and
 - (iii) include a cross liability clause.
2. All insurance described in section 1 of this Schedule must:
 - (a) be primary; and
 - (b) not require the sharing of any loss by any insurer of the Province.
3. The Contractor must provide the Province with evidence of all required insurance as follows:
 - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Province evidence of all required insurance in the form of a completed Province of British Columbia Certificate of Insurance;
 - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Province within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
 - (c) despite paragraph (a) or (b) above, if requested by the Province at any time, the Contractor must provide to the Province certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Schedule E – Privacy Protection Schedule

Definitions

1. In this Schedule,
 - (a) “**access**” means disclosure by the provision of access;
 - (b) “**Act**” means the *Freedom of Information and Protection of Privacy Act*;
 - (c) “**contact information**” means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
 - (d) “**personal information**” means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Province and the Contractor dealing with the same subject matter as the Agreement but excluding any such information that, if this Schedule did not apply to it, would not be under the “control of a public body” within the meaning of the Act; and
 - (e) “**privacy course**” means the Province’s online privacy and information sharing training course.

Purpose

2. The purpose of this Schedule is to:
 - (a) enable the Province to comply with the Province's statutory obligations under the Act with respect to personal information; and
 - (b) ensure that, as a service provider, the Contractor is aware of and complies with the Contractor's statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor’s obligations, or the exercise of the Contractor’s rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
 - (a) the purpose for collecting it;
 - (b) the legal authority for collecting it; and
 - (c) the title, business address and business telephone number of the person designated by the Province to answer questions about the Contractor’s collection of personal information.

Privacy Training

6. The Contractor must ensure that each person who will provide services under the Agreement that involve the collection or creation of personal information will complete, at the Contractor’s expense, the privacy course prior to that person providing those services.
7. The requirement in section 6 will only apply to persons who have not previously completed the privacy course.

Accuracy of personal information

8. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Province to make a decision that directly affects the individual the information is about.

Requests for access to personal information

9. If the Contractor receives a request for access to personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province unless the Agreement expressly requires the Contractor to provide such access and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

10. Within 5 Business Days of receiving a written direction from the Province to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
11. When issuing a written direction under section 10, the Province must advise the Contractor of the date the correction request to which the direction relates was received by the Province in order that the Contractor may comply with section 12.
12. Within 5 Business Days of correcting or annotating any personal information under section 10, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Province, the Contractor disclosed the information being corrected or annotated.
13. If the Contractor receives a request for correction of personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

14. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

15. Unless the Province otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

16. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

17. Unless the Province otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of personal information

18. Unless the Province otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Province if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
19. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

20. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.2 of the Act, if in relation to personal information in the custody or under the control of the Contractor, the Contractor:
- (a) receives a foreign demand for disclosure;
 - (b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or
 - (c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure

the Contractor must immediately notify the Province and, in so doing, provide the information described in section 30.2(3) of the Act. In this section, the phrases "foreign demand for disclosure" and "unauthorized disclosure of personal information" will bear the same meanings as in section 30.2 of the Act.

Notice of unauthorized disclosure

21. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information in the custody or under the control of the Contractor, the Contractor must immediately notify the Province. In this section, the phrase "unauthorized disclosure of personal information" will bear the same meaning as in section 30.5 of the Act.

Inspection of personal information

22. In addition to any other rights of inspection the Province may have under the Agreement or under statute, the Province may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to the Contractor's management of personal information or the Contractor's compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

23. The Contractor must in relation to personal information comply with:
- (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
 - (b) any direction given by the Province under this Schedule.

24. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

25. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

26. In addition to any other rights of termination which the Province may have under the Agreement or otherwise at law, the Province may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

27. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
28. Any reference to the “Contractor” in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
29. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
30. If a provision of the Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
31. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 32, the law of any jurisdiction outside Canada.
32. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

Schedule F – Additional Terms

Not Applicable

Schedule G – Security Schedule

Definitions

1. In this Schedule:

- (a) **“Device”** means any device to manage, operate or provide the Services or to connect to any Systems or any Province system or network, or that is capable of storing any Protected Information, and includes any workstation or handheld device the Contractor authorizes Personnel to use in relation to this Agreement;
- (b) **“Facilities”** means the physical locations (excluding those of the Province) the Contractor uses to provide the Services, or to house Systems or records containing Protected Information;
- (c) **“Least Privilege”** means the principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks so as to limit the damage that can result from accident, error or unauthorized use;
- (d) **“Need-to-Know”** means the principle where access is restricted to authorized individuals whose duties require such access and not merely because of status, rank or office;
- (e) **“Personnel”** means all individuals hired or used by the Contractor and Subcontractors to perform the Contractor’s obligations under this Agreement, including unpaid volunteers and the Contractor or a Subcontractor if an individual;
- (f) **“Policies”** means the intentions and directions of an organization or part of it, as expressed in record form by its top management (including, for example, policies, directions, standards, practices, procedures and guidelines);
- (g) **“Protected Information”** means any and all:
 - (i) “personal information” as defined in the Privacy Protection Schedule if attached;
 - (ii) information and records of information the Contractor is required to treat as confidential under this Agreement; and
 - (iii) records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked or instructed by the Province to be so preserved or otherwise treated as “Protected Information” under this Agreement;
- (h) **“Security Event Logs”** means any logs (also known as audit records) of events, notifications or alerts that any component of any Device or other device (not limited to security device), or any Systems or other system or software is technically capable of producing in relation to its status, functions and activities that may be used for such purposes as security investigations, auditing, monitoring and determining security incidents (examples of components capable of producing such logs include firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, dynamic host configuration protocols, dynamic naming services, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application firewalls);
- (i) **“Systems”** means any systems, subsystems, equipment, infrastructure, networks, management networks, servers, hardware and software the Contractor uses in relation to this Agreement, including for managing, operating or providing the Services, but excluding any the Province owns or makes available to the Contractor for the Contractor to use in relation to this Agreement;
- (j) **“Tenancy”** means those components of the Systems that:
 - (i) directly access and store Protected Information,

- (ii) relate to Protected Information or the Province's tenancy activities, or
- (iii) are customer facing and managed by the Province in its use of the Services; and
- (k) **"Tenancy Security Event Logs"** means Security Event Logs that relate to Tenancy, including:
 - (i) log-on/log-off information about Province user activities, and
 - (ii) application logs, web server log, file server logs, database logs of applications, web servers, file servers or database servers or any other logs that directly store, access or contain Protected Information.

Additional obligations

2. The Contractor must comply with Appendix G1 if attached.

PERSONNEL

Confidentiality agreements

3. The Contractor must not permit any person the Contractor hires or uses to access or obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under this Agreement.

Personnel security screening

4. The Contractor may only permit individual Personnel to have access to any Protected Information or other asset of the Province (including to any system, network or device the Province makes available to the Contractor) in relation to this Agreement, if, after:
 - (a) verifying their identity and relevant education, professional qualifications and employment history;
 - (b) completing a criminal record check that is updated at least every five years;
 - (c) requiring Personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law;
 - (d) performing any additional screening this Agreement or applicable law may require; and
 - (e) performing any additional background checks the Contractor considers appropriate,

the Contractor is satisfied that the individual does not constitute an unreasonable security risk.

5. If any criminal record check or proactive disclosure reveals a prior criminal offence or pending criminal matter, the Contractor must make a reasonable determination of whether the applicable person constitutes an unreasonable security risk, taking into consideration the duties of the individual and the type and sensitivity of information to which the individual may be exposed.
6. If the Contractor is an individual, the Province may subject the Contractor to the screening requirements in this Schedule.

Personnel information security training

7. Unless otherwise specified in this Agreement, the Contractor must ensure all Personnel complete any relevant information security training, at the Contractor's expense, before they provide any Services, or receive or are given access to any Protected Information or any system, device or secure facility of the Province, and thereafter at least annually.

Security contact

8. If not set out elsewhere in this Agreement, the Contractor (but not a Subcontractor) must provide in writing to the Province the contact information for the individual who will coordinate compliance by the Contractor and all Subcontractors and act as a direct contact for the Province on matters relating to this Schedule.

Supply chain

9. The Contractor must ensure that the security requirements of those in its upstream and downstream supply chain are documented, followed, reviewed, and updated on an ongoing basis as applicable to this Agreement.

GENERAL POLICIES AND PRACTICES

Information security policy

10. The Contractor must have an information security Policy that is:
 - (a) based on recognized industry standards; and
 - (b) reviewed and updated at least every three years.

Compliance and Standard for Security Controls

11. Unless this Agreement otherwise specifies, the Contractor must apply controls and security management practices to manage or operate Protected Information and Systems, Devices, and Facilities that are compliant with or equivalent to the following Province's Policies accessible at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>:
 - (a) "Information Security Policy";
 - (b) government wide IM/IT Standards; and
 - (c) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.

Contractor security risk assessments

12. The Contractor must undertake a security threat and risk assessment against an industry security standard before placing any new or materially changed Systems or services into production.

Change control and management

13. The Contractor must:
 - (a) implement and maintain change control processes for Facilities, Systems and Devices in line with applicable security best practices to reduce security-related risks with respect to implemented significant changes; and
 - (b) ensure that adequate testing of any change is completed before the change is put into production.

Backups and restores

14. The Contractor must ensure that:
 - (a) it has a backup Policy that is followed and is reviewed, updated and tested at least annually;
 - (b) backups are taken and tested in accordance with the Contractor's backup Policy, but in any event at least annually; and
 - (c) frequency and completeness of backups is based on reasonable industry practice.

Business continuity plan and disaster recovery plan

15. The Contractor must ensure that it has a documented business continuity plan and a disaster recovery plan that is reviewed at least annually.
16. The Contractor must ensure that Facilities and Systems are protected from loss, damage or other occurrence, including fire and environmental hazards and power interruptions, that may result in any of those Facilities and Systems being unavailable when required to provide the Services.

Security Incident Response and Management

17. The Contractor must ensure that it has a security incident management Policy and response plan that is reviewed at least annually.

PROTECTED INFORMATION AND DATA SECURITY

Encryption

18. The Contractor must ensure that:
 - (a) encryption of data at rest is implemented and is maintained in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, for all Protected Information stored on Systems and Devices; and
 - (b) encryption end-to-end is implemented for all Protected Information in transit.

No storage on unencrypted portable media

19. The Contractor must ensure that no Protected Information is stored on portable media for transport outside of the Facilities or Systems without both the prior written approval of the Province and ensuring that the portable media and the Protected Information are encrypted.

Encryption standard

20. For sections 18 and 19, encryption must comply with the Province's "Cryptographic Standards for Information Protection" accessible at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>.

Isolation controls and logical isolation of data

21. The Contractor must implement and maintain the logical isolation of Protected Information, in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure.

ACCESS AND AUTHENTICATION

User Identifiers

22. The Contractor must assign and ensure that user identifiers are unique and personal for log in to Systems and Devices.

Access

23. The Contractor must implement, follow, and regularly review and update, access control Policies that address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts for Facilities, Systems and Devices within the Contractor's control.
24. The Contractor must ensure that all access to Protected Information and to Facilities, Systems and Devices is based Least Privilege and Need-to-Know" based on role and responsibilities. The Contractor must identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse.
25. The Contractor must verify an individual's identity before assigning the individual a unique identifier that would give them access to Facilities, Systems or Devices.
26. The Contractor must implement a formal user registration process for Personnel that includes:
 - (a) verification of access levels;
 - (b) creating and maintaining records of access privileges;
 - (c) audit processes; and
 - (d) actions to ensure access is not given before approval is granted by the Contractor.
27. The Contractor must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts.
28. The Contractor must implement a monitoring process to oversee, manage and review Personnel access rights and roles at regular intervals.
29. The Contractor must ensure that all Systems and Devices:
 - (a) are configured in alignment with industry standards;
 - (b) enforce a limit of consecutive invalid logon attempts by a user during a predetermined time period;
 - (c) automatically lock the applicable account and Systems after failed logon failures;
 - (d) limit the number of concurrent sessions;
 - (e) prevent further access to Systems by initiating a session lock; and
 - (f) provide the capability of disconnecting or disabling remote access to the Systems.

Authentication

30. The Contractor must use or require complex passwords or personal identification numbers (PINs) that are not shared, default or blank and that are encrypted (not displayed) when entered, biometric accesses, keys,

smart cards, other logical or access controls, or combinations of them, to control access to Protected Information and to Systems and Devices.

31. The Contractor must ensure that Systems for password-based authentication:
 - (a) enforce minimum password complexity, including requiring passwords to be case sensitive, contain a minimum of eight characters and a combination of upper-case letters, lower-case letters, numbers, and/or special characters;
 - (b) change authentication passwords regularly at predetermined intervals, but at a minimum semi-annually;
 - (c) store and transmit only encrypted representations of passwords;
 - (d) enforce password minimum and maximum lifetime restrictions;
 - (e) prohibit password reuse;
 - (f) prevent reuse of identifiers; and
 - (g) disable the identifier after ninety days of inactivity.

Highly sensitive Protected Information

32. If this Agreement or the Province under this Agreement indicates that any Protected Information is highly sensitive, the Contractor must also ensure that Systems enforce with respect to that Protected Information:
 - (a) two-factor authentication for access;
 - (b) enhanced logging that logs all accesses;
 - (c) request based access; and
 - (d) no standing access rights.

SECURITY EVENT LOGS

Log generation, log retention and monitoring

33. The Contractor must ensure that logging of Security Event Logs is enabled on all applicable Systems components
34. The Contractor must retain Security Event Logs for the Systems online for a minimum of 90 days and either online or off-line for an additional period of time adequate to enable the Contractor to conduct effective security investigations into suspected or actual security incidents.
35. The Contractor must retain Tenancy Security Event Logs online for a minimum of 90 days and either:
 - (a) such additional period of time as the Province may instruct; or
 - (b) ensure that the Tenancy offers the technical capability for the Province to retain the Tenancy Security Event Logs,
to enable the Province to comply with an information schedule approved under the *Information Management Act* or other retention period required by law.
36. Upon the Province's request, the Contractor must ensure that the Tenancy offers the technical capability for the Province to enable or configure the forwarding, extraction, backup of Tenancy Security Event Logs from the Tenancy to the Province's security information and event management system or to an external log storage and retention system.

37. The Contractor must review Security Event Logs regularly to detect potential security incidents, using automated tools or equivalent processes for the monitoring, review, correlating and alerting of Security Event Logs.

PROVINCE PROPERTY

Access to Province facilities, systems or networks

38. If the Province makes available any facilities, systems, networks or devices for use of the Contractor in relation to this Agreement, the Contractor must comply with, and permit access on its behalf only by those authorized Personnel who have been instructed to comply with, the Province's Policies then applicable to their acceptable use, access and protection accessible at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>, including:
- (a) "Appropriate Use Policy" (as also referenced in chapter 12 of the Province's "Core Policy and Procedures Manual");
 - (b) "Information Security Policy";
 - (c) government wide IM/IT Standards; and
 - (d) sector or ministry specific IM/IT Standards, if any applicable to the Province ministry, agency or other representative receiving the Services.
39. The Province has the rights to:
- (a) not make any particular Province facility, system, network or device available before the Contractor or individual Personnel or both agree to a form of agreement acceptable to the Province on acceptable use, protection of, and access to, such facility, system, network or device, or at all;
 - (b) not permit connection to any particular Province system or network until satisfied with the controls applied and the security status of the Device to be connected;
 - (c) keep facilities access logs and Security Event Logs, and to otherwise monitor and analyze use of Province facilities, systems and networks to verify compliance, investigate suspected or actual breaches or information incidents and protect the Province's assets, including records, in compliance with applicable laws, including the *Freedom of Information and Protection of Privacy Act* and *Information Management Act*, and the Province's Policies; and
 - (d) limit or revoke access to any Province systems, facility or device at its discretion.

Application development

40. If the Services include software development, the Contractor must ensure that the applications and programming interfaces are developed according to industry standards and Province's Policies applicable to application development standards. The Contractor must use secure application development practices for the development of the software.

FACILITIES, SYSTEMS, DATABASE AND DEVICE SECURITY

Physical security

41. The Contractor must ensure that adequate physical controls and processes are implemented to ensure that only authorized persons have physical access to the Facilities and Systems.
42. The Contractor must develop, document, and disseminate a physical and environmental protection Policy that it reviews at least annually.

43. The Contractor must review physical access logs at least once monthly.
44. The Contractor must ensure that physical security of any Systems or Facilities being used or capable of being used to house Protected Information meets a standard as would be reasonably expected to provide adequate protection based on the value of the data being protected and the environment in which the Systems or Facilities are located. At a minimum, this should include:
 - (a) hardening of the perimeter of the Facilities;
 - (b) physical separation of public and restricted spaces;
 - (c) Intrusion Alarm System (IAS) partitioned to ensure areas containing Protected Information are protected at all times;
 - (d) Access Control Systems (ACS) and/or Key Management processes; and
 - (e) visitor and identity management processes – including access logs and identification badges.

Separation of production from test environments

45. The Contractor must not use any production data in any development, test or training environments used for the Services without the Province's prior written consent. If the Province gives such consent, the production data must, at minimum, be obfuscated (for example, by using data masking functionality).
46. The Contractor must keep its development, test and training environments separate from its production environments used for the Services at all times, even in case of failure.

Systems (including servers) hardening

47. The Contractor must:
 - (a) harden all Systems against attack and misuse, using appropriate security best practices for the hardening of the specific deployed platform, before placing those Systems into production;
 - (b) ensure that all unsecured and unneeded ports, services, applications, protocols and network communicating applications are uninstalled or disabled on all Systems;
 - (c) applying Least Privilege, ensure that the Contractor only configures and makes operational ports, services, applications, protocols and network communicating applications based on the functional requirements of the respective Systems;
 - (d) ensure that default passwords and shared accounts are not used for any Systems; and
 - (e) in relation to Systems, implement server hardening using configuration security best practices (for example, Center for Internet Security, Inc. (CIS) Benchmarks or equivalent) for any server operating systems, server virtualization, server middleware (for example, web servers and database servers) and application servers.

Perimeter controls (firewall and intrusion prevention system) and network security

48. The Contractor must:
 - (a) implement stateful packet inspection firewalls to control traffic flow to and from Systems and Tenancy at all times, and configure the stateful packet inspection firewalls applying security best practices and Least Privilege;

- (b) implement an intrusion prevention System to control and filter traffic flow leaving and entering Systems and Tenancy at all times, and configure the intrusion prevention System applying security best practices; and
- (c) implement a secure network perimeter and network segmentation for Systems, with ingress and egress points that are known and controlled.

Application firewall

49. The Contractor must implement application layer firewalls on Systems:

- (a) at such level of protection as the Province may instruct ; and
- (b) to detect and mitigate application attacks (for example, brute force, OWASP Top 10, SQL injection, cross site scripting).

Management network

50. The Contractor must ensure that for any Systems:

- (a) the management network remains logically separated from any other zone and is not directly accessible from the Internet;
- (b) the management network is internally segmented, with each server's dedicated network interface on its own segmented network and that interfaces on the management network do not have visibility to each other; and
- (c) all access to the management network is strictly controlled and exclusively enforced through a secure access gateway, bastion host or equivalent.

Remote management and secure access gateway

51. The Contractor must perform any remote management of Systems or Devices in a secure manner, using encrypted communication channels and adequate access controls.

Database security

52. The Contractor must ensure that for any Systems:

- (a) database maintenance utilities that bypass controls are restricted and monitored;
- (b) there is a formal approval process in place for handling requests for disclosure of database contents or for database access, including steps to evaluate privacy impacts and security risks of such requests; and
- (c) methods to check and maintain the integrity of the data are implemented (for example, consistency checks and checksums).

53. For database security, the Contractor must implement logical isolation and encryption of Protected Information.

Device security and antivirus scanning

54. The Contractor must ensure all Devices:

- (a) have antivirus and malware protection as appropriate for the particular Device active at all times;
- (b) are configured to perform antivirus scans at least once per week;

- (c) have host based firewall configured, enabled and active at all times; and
- (d) have all patches and appropriate security updates installed for the operating system and all installed software.

VULNERABILITY PREVENTION, SCANNING AND MANAGEMENT

Proactive management

55. The Contractor must:
- (a) obtain information in a timely basis about technical vulnerabilities relating to Systems and Devices; and
 - (b) implement processes to stay current with security threats.

Patching

56. The Contractor must patch all Systems regularly in line with security best practices and ensure that current software, operating systems and application patching levels are maintained.
57. The Contractor must ensure that all Systems have all patches installed on a regular schedule, within the time frame recommended by the manufacturer unless the Province otherwise consents in writing.
58. The Contractor must ensure that vulnerabilities are remedied and patches installed on an accelerated basis for zero-day, critical and high vulnerabilities. For zero-day vulnerabilities, the Contractor must implement appropriate mitigation measures promptly on notification of the zero-day vulnerability. The Contractor must remediate zero-day, high and critical vulnerabilities through patching, decommission, or compensating controls.
59. The Contractor must patch high vulnerabilities within 30 days or less of discovery and patch medium vulnerabilities within 90 days or less of discovery.

Vulnerability Scanning

60. The Contractor must ensure that a vulnerability scan is completed on components of all Systems:
- (a) with any identified vulnerabilities remedied, before being placed into production; and
 - (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Web application vulnerability scanning

61. The Contractor must ensure that a vulnerability scan is completed on any web applications used for Tenancy or in any other Systems:
- (a) and on any major changes to such web applications, with any identified vulnerabilities remedied, before being placed into production; and
 - (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Antivirus and malware scanning

62. The Contractor must ensure that all Systems servers:

- (a) have antivirus and malware protection configured, active and enabled at all times;
- (b) have antivirus and malware definitions updated at least once a day; and
- (c) are configured to undergo a full anti-virus scan for latent infections (to detect infections missed by the real-time agent) at least once a week.

DISPOSALS

Asset disposal

- 63. The Contractor must ensure that all disposals of assets used in providing or relating to the Services are done in a secure manner that ensures that Protected Information cannot be recovered.

Asset management

- 64. The Contractor must have asset management and disposal Policies that are followed, and reviewed and updated regularly in line with security best practices, and that address hardware, software and other critical business assets.
- 65. The Contractor must keep an asset management inventory that includes the name of the System, location, purpose, owner, and criticality, with assets added to inventory on commission and removed on decommission.

Information destruction and disposal

- 66. Unless this Agreement otherwise specifies, the Contractor must retain all records containing Protected Information in the Contractor's possession until instructed by the Province in writing to dispose or deliver them as instructed.
- 67. The Contractor must securely erase:
 - (a) records that contain Protected Information and Tenancy Security Event Logs when instructed in writing by the Province; and
 - (b) any backup, transitory and extra copies of records that contain Protected Information or Tenancy Security Event Logs when no longer needed in relation to this Agreement.
- 68. The Contractor must ensure that Protected Information and Tenancy Security Event Logs on magnetic media are securely wiped by overwriting using procedures and adequate media wiping solutions, degaussing, or other method in line with security best practices for disposal of media.

NOTICES, INCIDENTS AND INVESTIGATIONS

Notice of demands for disclosure

- 69. In addition to any obligation the Contractor may have to notify or assist the Province under applicable law or this Agreement, including the Privacy Protection Schedule if attached, if the Contractor is required (including under an enactment or a subpoena, warrant, order, demand or other request from a court, government agency or other legal authority) to produce, provide access to or otherwise disclose any Protected Information, the Contractor must, unless prohibited by applicable law, immediately notify and provide reasonable assistance to the Province so the Province may seek a protective order or other remedy to prevent or limit the disclosure.

E-discovery and legal holds

- 70. The Contractor must fully co-operate with the Province to enable the Province to comply with e-discovery and legal hold obligations.

Incidents

71. In addition to any obligation the Contractor may have under applicable law, including the *Freedom of Information and Protection of Privacy Act*, or this Agreement, if, during or after the Term, the Contractor discovers a suspected or actual unwanted or unexpected event or series of events that threaten the privacy or security of Protected Information (including its unauthorized access, collection, use, disclosure, alteration, storage or disposal) or Tenancy, whether accidental or deliberate, the Contractor must:
- (a) immediately report the particulars of such incident to, and follow the instructions of, the Province, confirming any oral report with a notice in writing to the Province as soon as reasonably practicable (if unable to contact the Province's contract manager or other designated contact for this Agreement, the Contractor must follow the procedure for reporting and managing information incidents on the Province's website at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents>; and
 - (b) make every reasonable effort to recover the records containing Protected Information and contain and remediate such incident, following such reasonable instructions as the Province may give.

Investigations support and security investigations

72. The Contractor must:
- (a) conduct security investigations in the case of incidents (including any security breach or compromise) affecting Devices, Facilities, Systems, Tenancy or Protected Information, collecting evidence, undertaking forensic activities and taking such other actions as needed;
 - (b) provide the Province with any related investigation reports, which the Contractor may sanitize first;
 - (c) upon the Province's request, provide the Province with any logs relating to such investigation reports as validation/confirmation of such investigation, which the Contractor may sanitize first; and
 - (d) maintain a chain of custody in all such security investigations it undertakes.
73. Upon the Province's request, the Contractor must:
- (a) provide investigative support to the Province to enable the Province to conduct its own security investigations into incidents (including security breaches or compromises) affecting the Tenancy or Protected Information;
 - (b) provide the Province with timely access via an on-line, real-time GUI (Graphic User Interface) facility to any Tenancy Security Event Logs and to other Security Event Logs for Systems (the latter of which the Contractor may sanitize first to mask or remove, for example, data pertaining to the Contractor's customers) to assist the Province in conducting the Province's security investigations, or in case of technical limitations, other method acceptable to the Province (for example, on-site visits to enable direct access to those Security Event Logs).
74. The Contractor must work with and support the Province if the Province needs assistance in legal proceedings in relation to security investigations related to Protected Information or Tenancy.

Province Security Threat and Risk Assessment ("STRA") support

75. The Contractor must, via its technical and security resources, support the Province in completing a STRA for the Services and to otherwise assess the risks associated with the Services, including by providing all information and documentation (for example, architecture diagrams, service architecture, controls architecture and technical information), which the Contractor may sanitize first and that the Province may reasonably require for such purpose.

Notification of changes

76. The Contractor must notify the Province of any changes to its security Policies, management practices and security controls described in this Agreement that may potentially negatively impact the security of Tenancy, Protected Information, or those Systems providing the Services.

Compliance verification

77. Upon the Province's request, the Contractor must provide, at no additional cost, the following security reports to the Province at least every six months during the Term:
- (a) vulnerability scan reports of those Systems providing the Services; and
 - (b) patch status reports for those Systems providing the Services.
78. In addition to any other rights of inspection the Province may have under this Agreement or under statute, the Province has the rights, at any reasonable time and on reasonable notice to the Contractor, to:
- (a) request the Contractor to verify compliance with this Schedule and to keep security controls documentation or records to support compliance; and
 - (b) enter on the Contractor premises and Facilities to inspect and to validate the Contractor's compliance with the security obligations under this Agreement
79. The Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province's rights under this section. If any non-compliance or deficiency is found, the Province may (in addition to any other rights it may have) require the Contractor, at the Contractor's expense, to develop and implement a corrective action plan within a reasonable time.

Notice of non-compliance

80. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

MISCELLANEOUS

Interpretation

81. In this Schedule, unless otherwise specified, references to sections by number are to sections of this Schedule.
82. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under this Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
83. Any reference to a specified Policy refers to it as may be revised or replaced from time to time.
84. If a provision of this Schedule conflicts with a documented process required by this Schedule to be created or maintained by the Contractor, the provision of the Schedule will prevail to the extent of the conflict.

Referenced documents

85. Policies and other documents of the Province referenced in this Schedule may be updated or replaced by the Province from time to time without notice, and if not found at the hyperlink or URL provided or via the Province's main website at <http://www.gov.bc.ca>, be obtained from the Province's contact for this Agreement.

Survival

86. Sections 63, 66, 67, 68, 69, 70, and 71 and other obligations of the Contractor in this Schedule which, by their terms or nature, are intended to survive the completion of the Services or the termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

CPU/CRRU Amalgamation Proposal

POLICY, FINANCE AND OPERATIONS STEERING COMMITTEE

JESS GUNNARSON

1.1 BACKGROUND:

Prior to 2019, Security Programs Division (SPD) of the Ministry of Public Safety & Solicitor General (PSSG) contracted directly with retired police officers with legacy database permissions and security clearance enabling access to law enforcement databases to collect information from the Canadian Police Information Centre (CPIC) and the Police Records Information Management Environment-BC (PRIME-BC). Though contracted by the Province, the CRRU was identified as an RCMP unit in the 2009 Letter of Agreement (LOA) between the RCMP and PSSG. The purpose of these direct contracts was to search CPIC and PRIME-BC information to help inform SPD's decision makers with respect to SPD's eight regulatory and non-regulatory programs involving approximately 280,000 checks annually. The program areas are as follows:

- *Criminal Records Review Act* (CRRRA) provides the Deputy Registrar the authority to conduct criminal record checks for employees/ volunteers involved in unsupervised employment/ volunteer activities with children and/ or vulnerable adults to determine if an individual was the subject of an outstanding charge or conviction related to a "relevant offence or specified offence";
- *Security Services Act* (2007) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of security worker/ business licensing;¹
- *Body Armour Control Act* (2009) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of registration of body armour;
- *Armoured Vehicle and After-Market Compartment Control Act* (2010) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of registering armoured vehicles;
- *Pill Press Related Equipment Control Act* (2018) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of registering pill presses;
- *Cannabis Control and Licensing Act- CCLA* (2018) provides the Security Manager the authority to carry out the following checks: criminal record check or fingerprint based criminal record verification by searching CPIC, police information check (PRIME/PROS), law enforcement intelligence databases, the justice information system, and correction service information check for purpose of clearance to work in or operate a business in the non-medical legal cannabis industry;
- Personnel Security Screening for BC public service employees which involves a search for charges/ convictions and, in designated instances, Enhanced Security Screening (ESS) for BC public service employees whose roles require more stringent security screening. For ESS, each client organization enters a separate agreement which may involve CPIC, PRIME/ PROS, and other queries/ checks of law enforcement databases;
- 'Outside the Act' checks, including criminal record checks for the Ministry of Children and Family Development in accordance with the *Child, Family and Community Services Act* (1996) which provides the Director of the CFCSA with the authority to have access to any information that is

¹ Although the Act allows for a police information check (PRIME/PROS) to be conducted in every instance, SPD determines when the CRRU will go beyond a CPIC check and look at these additional law enforcement databases for adjudication purposes.

in the custody or control of a public body that is necessary to enable them to exercise their powers to perform their duties under the Act.

In December 2018, the Provincial Government, on behalf of SPD entered a business case and funded the Criminal Record Review Unit (CRRU) under the RCMP/CFSEU-BC (OCABC positions) to conduct criminal record checks for the above regulatory and non-regulatory programs, with the exception of the CCLA. Access to information on police databases is highly regulated and restricted to law enforcement agencies and, while the contractors had the requisite security clearance and access, the access was not under the direct supervision of the RCMP. An amendment was entered to the business case and signed in April/ May 2019. The CRRU was created as an entity of CFSEU-BC with OCABC positions. This transition enabled direct oversight of the CRRU by the RCMP and also ensured the unit was following proper policy as a "Category 1" policing agency to access the various law enforcement databases. The April/ May 2019 business case amendment allocated annual funding of \$887,187 at 100% to fund the CRRU with the Province's contribution (70%) at \$621,031.

s.15; s.16

For context, the Police Information Check (PIC) Guidelines were developed in collaboration between the RCMP, municipal police forces, PSSG, and PRIME-BC in 2010 and implemented in the spring of 2012. The guidelines were amended in 2014 subsequent to recommendations by BC's privacy commissioner and again in 2016. The guidelines are intended to create consistency in practice between police agencies province-wide who are conducting criminal record checks, including vulnerable sector checks, at the request of individuals for employment/ volunteer purposes. BC PIC guidelines prescribe two types of checks: 1) PIC check which includes a search of CPIC and PRIME for charge/ conviction information, and 2) PIC-VS check for individuals working with the vulnerable sector which includes a search of CPIC and PRIME and can include disclosure of any non-conviction information where the applicant was in a culpable role code within the disclosure period. While other jurisdictions in Canada have placed significant constraint upon the disclosure of non-conviction information in criminal record checks given the potentially prejudicial nature of the information (see Ontario's *Police Criminal Record Check Reform Act* enacted in 2018 and the Alberta Police Information Check Disclosure procedures endorsed in 2019),

BC's PIC guidelines continue to enable disclosure of non-conviction information in multiple circumstances.

s.15; s.16

In April/ May 2019, the Province, on behalf of SPD, entered a separate business case and funded the Cannabis Organized Crime Counter Proliferation Unit (CPU) which was functional commencing in October 2018 to support the Security Manager at SPD with security screening for cannabis businesses, associates, and workers in accordance with the *Cannabis Control & Licensing Act* (CCLA). The April/ May 2019 CPU business case allocated annual funding of \$1,150,268 at 100% to fund CPU with the Province's contribution (70%) at \$805,187. The total sum of annual funding allocated to CRRU and CPU was \$2,037,455 with the Province's contribution (70%) at \$1,426,218.

Concurrent to the above discussions involving the CRRU, non-medical cannabis was legalized in October 2018. CPU supported SPD with searches of law enforcement databases and investigations through 2019 and 2020. In September 2020, the Cannabis Licensing Regulation was amended to remove the Security Manager's (SM) independent statutory decision-making authority and, while the SM maintains a role with information provided by CPU, the General Manager is now the sole statutory decision-maker. With more than two years since legalization, and with few 'not fit and proper' findings, the Province has learned a significant amount regarding the risks in the non-medical legal cannabis market and this business case makes changes to the CPU structure in response to learnings.

2.1 PURPOSE

The purpose of the present business case is twofold:

1. Obtain approval for the amalgamation of CPU and CRRU into a single unit termed the Criminal Record Review Unit. This merger enables greater flexibility and operational efficiencies in maximizing the new CRRU's impact across the key mandates and priorities detailed in the business case below. The financial forecast is attached as Appendix A and reflects the combination of the separate CRRU and CPU funding allocations with no additional funding. In other words, the funding requirements of the new CRRU will not exceed the current combined funding (at 100%) of the CRRU and CPU with a combined annual budget of \$2,037,455;
2. Obtain approval for the realignment of resources within the new combined CRRU to enable the CRRU to conduct the additional effort required to be consistent with the PIC guidelines, including PIC-VS equivalent checks for the CRRU. This involves the maintenance and transition of 3.5 positions from the CPU to the CRRU for support of Cannabis Organized Crime background checks

and monitoring of the legal cannabis industry, including two (2) Junior Intelligence Analysts² and one (1) Information Coordinator, as well as the ½ NCO i/c Sergeant position. Five of CPU's positions will be absorbed by CFSEU-BC/ OCABC as Surplus to Establishment (STE) with two positions deleted as they are vacant (for a net total of 3 STEs). With the financial capacity created by moving the five CPU positions to STE, this proposal requests an increase in CRRU capacity by seven (7) Organized Crime Agency of BC (OCABC) positions, including one (1) Team Coordinator and six (6) Information Officers (please refer to Appendix B for the revised organizational chart).

3.1 CRRU Composition

Prior to the 2009 letter of agreement, the CRRU consisted of seven (7) retired RCMP members and one clerical staff member who were direct-awarded contracts administered by SPD and renewed on an annual basis. Between 2009 and 2019, the unit has expanded to include a total of ten (10) established positions, including one (1) operational position and nine (9) civilian positions.

On February 25, 2019, E Division RCMP received a funding letter from PSSG and the business case was signed between the Province and RCMP E Division, as described above, which transferred supervision and oversight of the CRRU under the umbrella of CFSEU-BC/ RCMP on April 1, 2019. This reform of the CRRU ensured that the unit continued to operate as a centralized service delivery model to support the obligations and requirements of the Registrar under SPD's eight regulatory and non-regulatory programs as authorized by legislation, policy, and consent. At this time, all retired police member contractors were transitioned into full-time civilian employees with OCABC and one OCABC Sergeant was assigned as the operational and administrative oversight of the CRRU.

The following table represents the positions current to January 2021 within the CRRU:

CRRU	Title/Rank	Classification	Position Number	Funding Collator	Location Collator
1	NCO i/c Sergeant	OCA ½ time	OCA-115	E1469	E1469
2	Team Coordinator	Pay Grade 7	OCA-120	E1469	E1469
3	Information Officer	Pay Grade 6	OCA-121	E1469	E1469
4	Information Officer	Pay Grade 6	OCA-122	E1469	E1469
5	Information Officer	Pay Grade 6	OCA-123	E1469	E1469
6	Information Officer	Pay Grade 6	OCA-124	E1469	E1469
7	Information Officer	Pay Grade 6	OCA-125	E1469	E1469
8	Information Officer	Pay Grade 6	OCA-126	E1469	E1469
9	Information Officer	Pay Grade 6	OCA-127	E1469	E1469
10	Information Officer	Pay Grade 6	OCA-128	E1469	E1469

3.2 Internal Review of CRRU:

s.13; s.15; s.16

² One of which must be converted from an Analyst Assistant position to Junior Criminal Intelligence Analyst

3.3 Proposed CRRU Model and Required Resources:

In discussions between PSSG, the RCMP and, legal counsel with the Department of Justice, the RCMP communicated that the CRRU falls under the administrative and operational umbrella of the RCMP which is governed by federal legislation. Although legislation exists at the provincial level, the RCMP views its authority for background checks as stemming from signed consent forms in accordance with the *Privacy Act*. Despite confines placed by the provincial CRRA, the RCMP has identified that authority by way of consent prevails and the access/ disclosure of non-conviction information will best insulate the RCMP from the perspective of perceived financial and reputational liability and mitigate risks the RCMP have stated surrounding public safety.

In order to ensure consistency with police departments/detachments and conduct vulnerable sector background checks that comply with the PIC guidelines, the RCMP has required that the CRRU expand criminal record checks under the CRRA through the utilization of additional law enforcement databases (PRIME/PROS), thus aligning with the existing PIC guidelines. All applicants who are identified as having been in a culpable role for a non-conviction matter associated to a CRRA Schedule I or III offence will be assessed by CRRU. A Service Level Agreement will be instituted to identify the extent of CRRU analysis and the degree and circumstances under which non-conviction information is disclosed to SPD.

In order for the CRRU to conduct BC PIC-VS on all CRRA-related applications, additional Information Officers are required. In 2019, the CRRU conducted 248,311 CRRA related background checks, which averages to a total of 985 checks conducted per/day. The CRRU's internal assessment indicates that each Information Officer is capable of conducting approximately 120 BC-PIC background checks per/shift. Applying this rate to the 985 background checks conducted per day and recognizing that CRRU is currently conducting PRIME checks in some circumstances, the CRRU will be allocated a net addition of six (6) Information Officers and one (1) team lead. It must also be remembered that in addition to the CRRA checks, the CRRU also supports SPD with numerous other regulatory and non-regulatory background checks and the RCMP's requirement to conform to the PIC Guidelines is likely to create additional workload for CRRU.

3.4 Cannabis Organized Crime Counter Proliferation Unit (CPU)

On October 17, 2018 the *Cannabis Act* was enacted. Under this federal legislation, adults are allowed access and possession of regulated, quality controlled, legal non-medical cannabis. Under this Act, the provinces and territories are responsible for overseeing and licensing the distribution and sale of cannabis products, subject to federal conditions.

A key priority in the legalization of cannabis is ensuring public safety and preventing an organized crime presence in the legalized cannabis market. The CPU was created in 2018 to support SPD and the Security Manager under the *Cannabis Control and Licensing Act* (CCLA) with conducting background checks of all retail applicants and workers in BC's non-medical cannabis industry with a goal of identifying applicants and associates with a nexus to organized crime. The CPU is a fenced unit within CFSEU-BC, independent and separate from other enforcement teams with business rules established to ensure alignment with provincial priorities and privacy laws.

At full strength, the unit is funded for a total of 8.5 positions (OCABC and RCMP). The CPU consists of 0.5 OCABC Sergeant (shared with CRRU), 1 RCMP Corporal and 1 RCMP Criminal Intelligence Analyst (Vacant), and 6 OCABC civilian employees including the following: 2 Open Source Analysts, 1 Junior Criminal Intelligence Analyst (Vacant), 1 Analyst Assistant, 1 Information Coordinator and 1 Investigative Assistant.

A tremendous amount has been learned from the inception of the CPU in 2018 and the unit has transitioned in accordance with the provincial requests over the past two years. In August 2020, the CPU commenced working with PSB to revise the screening process related to cannabis to garner greater effectiveness and efficiencies. This has resulted in a proposal to combine the resources from the CPU with the CRRU and to streamline the overall background check process as it relates to Cannabis. These enhancements and efficiencies will be implemented as aspect of this amalgamation.

s.15

After numerous discussions, the CPU resources transitioning into CRRU are all OCABC civilian employees including 1 Information Coordinator, 2 Junior Criminal Intelligence Analyst and the ½ NCO i/c Sergeant position. It should be noted that approval is required from the Province to change the existing Analyst Assistant to a Junior Criminal Intelligence Analyst for this merger.

The following table represents the established positions within the CPU as of January 2021:

CPU	Title/Rank	Classification	Position Number	Funding Collator	Location Collator	Amalgamated? Yes/No
1	NCO i/c Sergeant	OCA ½ time	OCA-115	E1463	E1463	Yes
2	2 i/c Corporal	RCMP (RM)	55376	E1463	E1463	No
3	Jr Crim Intel Analyst	Pay Grade 7	OCA-116	E1463	E1463	Yes
4	Analyst Assistant ¹	Pay Grade 3	OCA-117	E1463	E1463	Yes
5	Information Coordinator	Pay Grade 4	OCA-119	E1463	E1463	Yes
6	Sr Crim Intel Analyst ²	RCMP (CM)	55380	E1463	E1463	No
7	Investigative Assistant ²	Pay Grade 2	OCA-118	E1463	E1463	No
8	Open Source Analyst	Pay Grade 6	OCA-92	E1463	E1463	No
9	Open Source Analyst	Pay Grade 6	OCA-93	E1463	E1463	No

¹ The OCA-117 position is currently an Analyst Assistant, Pay Grade 3, and requires reclassification to a Junior Criminal Intelligence analyst, Pay Grade 7, in order to conduct the necessary duties and have access to sensitive law enforcement databases.

² Positions currently vacant

As per the above, CFSEU-BC/OCABC will have to absorb three (3) positions Surplus to Establishment (STE). The total estimated financial impact of this absorption is \$389,436, as detailed in the table below and Appendix C:

Title/Rank	Salary & Benefits	Other Divisional and O&M Costs	Total Cost
RCMP Corporal	\$150,067	\$18,972	\$169,039
OCABC Open Source Analyst	\$102,299	\$7,900	\$110,199
OCABC Open Source Analyst	\$102,299	\$7,900	\$110,199
TOTAL	\$389,436		

With the overall size of CFSEU-BC there is a fair amount of internal movement with resources either transferring, retiring or finding alternate employment outside of the agency. The table below details the timeline for the three STEs to be absorbed into CFSEU-BC/OCABC. The 2 vacant positions will be deleted once this business case is approved; and the 3 STE positions will be deleted upon each incumbent's transfer into an equivalent position, as outlined below and as soon as is practicable and in accordance with the RCMP's internal processes.

CPU	Title/Rank	CPU Position Number	Current Collator	Pending Position Number	New Collator	Timeline
1	RCMP Corporal	55376	E1463	48719	E1150	April 1, 2021 to acting Sgt. position on PVGO (PTEP)
2	OCA Open Source Analyst – Pay Grade 6	OCA-92	E1463	OCA-143	GGVAF	Current OS Analyst on the Firearms Team will be departing CFSEU in the next 12 months and

						will be replaced by the CPU OS Analyst
3	OCA Open Source Analyst – Pay Grade 6	OCA-93	E1463	TBD	E1478	Business Case for OS Analyst on the Witness Security Program and once approved (12 months) this CPU OS Analyst will occupy the position.
4	Sr Crim Intel Analyst	55380	E1463	To be deleted		
5	Investigative Assistant	OCA-118	E1463	To be deleted		

A STE position would be created for the RM, which would not affect Annex A and would not be attached to a collator. For the Open Source Analysts, the STE boxes would be attached to the Open Source collator which would be added financial pressure to the Open Source collator. As the corporal position would be vacant starting April 1, 2021, there would be no additional financial pressure resulting from the RM position.

4.1. AMALGAMATION OF THE CRRU AND CPU:

In consultation with senior leaders from PSSG, combining some of the resources from CPU with the larger CRRU will garner greater efficiencies. The attached organizational chart (Appendix B) outlines the new positions and the structure of the combined unit once approved.

The proposal increases the CRRU by 7 OCABC positions which includes 1 additional Team Coordinator and 6 Information Officers. In addition, 2 Junior Intelligence Analysts and 1 Information Coordinator positions would transition from the CPU (including the ½ NCO i/c/ Sergeant position) to the CRRU for additional support of the Cannabis OC background checks and monitoring of the legal non-medical cannabis market. It is critical to note that the aforementioned CPU positions will continue to focus on cannabis-related background checks but will be situated within the larger CRRU team to enhance efficiencies and create greater flexibility in task assignment. Funding for the CPU was provided by Treasury Board for the purpose of protecting the cannabis industry against illegal activity and organized crime involvement. The functions and duties of the existing CPU positions within the broader CRRU will continue to be fulfilled in accordance with the mandate and responsibilities outlined in CPU's business case and delegation letters from the Province.

This includes:

- To address the risk of organized crime infiltration in non-medicinal cannabis distribution, specifically to support screening strategies during the retail licensing process and for employees working with non-medical cannabis in the market;
- To provide the necessary background and information checks to ascertain ties, association, or a nexus to organized crime for cannabis retail applicants/associates, and workers as required;
- Checks include:
 - a criminal record check or fingerprint-based criminal record verification through CPIC;
 - a police information check;
 - a check of intelligence databases maintained by law enforcement agencies;

- a check of records in the justice information system of the Ministry of the Attorney General;
- a check of records in the corrections information system of PSSG.
- To develop and maintain an information system for the legal and illegal cannabis market, including a file management system for CPU checks and processes in alignment with required reporting and evaluation metrics;
- Submit any files that require additional investigation regarding a potential nexus to organized crime to SPD, in order for SPD's investigators to conduct a follow-up investigation into the matter;
- To provide timely and evidence-based reports for license applicants and workers to SPD;
- Establish a system of evidence management and evidence presentation commensurate for required judicial proceedings as required and prepare/provide all required materials for any judicial matters that arise from the licensing or employee application screening process.

s.15; s.16

The following table depicts the future state of the amalgamated unit:

CRRU AMALGAMATED	Position Number	Classification	Funding Collator	Location Collator
1	OCA-115	OCA	E1469	E1469
2	OCA-120	Pay Grade 7	E1469	E1469
3	OCA-TBD *	Pay Grade 7	E1469	E1469
4	OCA-121	Pay Grade 6	E1469	E1469
5	OCA-122	Pay Grade 6	E1469	E1469
6	OCA-123	Pay Grade 6	E1469	E1469
7	OCA-124	Pay Grade 6	E1469	E1469
8	OCA-125	Pay Grade 6	E1469	E1469
9	OCA-126	Pay Grade 6	E1469	E1469
10	OCA-127	Pay Grade 6	E1469	E1469
11	OCA-128	Pay Grade 6	E1469	E1469
12	OCA-TBD *	Pay Grade 6	E1469	E1469
13	OCA-TBD *	Pay Grade 6	E1469	E1469
14	OCA-TBD *	Pay Grade 6	E1469	E1469
15	OCA-TBD *	Pay Grade 6	E1469	E1469
16	OCA-TBD *	Pay Grade 6	E1469	E1469
17	OCA-TBD *	Pay Grade 6	E1469	E1469
18	OCA-116	Pay Grade 7	E1469	E1469
19	OCA-117	Pay Grade 7	E1469	E1469
20	OCA-119	Pay Grade 4	E1469	E1469

** It is anticipated that these additional OCABC positions will be added to the newly enhanced CRRU.*

The unit will remain fenced and an independent unit within the CFSEU-BC's Support Services and all operational and administrative aspects of this unit will be managed within the structure of CFSEU-BC.

4.2 Funding

It is understood the funding for this proposal must come from within the CFSEU-BC and with combining the two units there will be sufficient funding for this proposal.

The annual cost estimate (Appendix A) for the amalgamated CRRU including salaries, benefits and O&M totals \$2,037,455. This reflects the existing total allocation for the CRRU and CPU independently, without addition of any further funding allocation.

There are several key risks that must be considered with respect to the proposed business case:

1. The absorption of the three (3) STEs poses both short- and long-term financial risks for CFSEU-BC. It will be critical that CFSEU-BC appropriately forecasts and manages these financial impacts to ensure a balanced budget.
2. The current proposal is dependent on the continued availability of funding for the CPU by Treasury Board. If funding is reduced or ended in future years, the continuity of the proposed changes to the CRRU will be impacted.
3. While the conduct of checks in accordance with the PIC guidelines and, specifically, PIC-VS checks for all CRRA checks addresses the liability and public safety concerns of the RCMP, it is not in line with the terms outlined in the CRRA which raises risks of substantial complaint, civil recourse, and financial/ reputational liability for the Province. SPD will work to manage the risk, including through development of a Service Level Agreement/ Information Sharing Agreement with the RCMP, and ensure there is a process that limits the disclosure of non-conviction information.
4. The implementation of the PIC Guidelines for SPD's regulatory and non-regulatory programs creates a risk of unidentified resourcing pressures for SPD which, unless managed through provisions in the Service Level Agreement, will impede the success of this business case.

4.3 Space Allocation

The enhanced CRRU for the most part will continue to work remotely on a permanent basis and there will be no requirement for additional office space at the Island District Headquarters in Victoria. The two Junior Criminal Intelligence Analysts and one Information Coordinator will work from the CFSEU-BC office at RCMP Headquarters in Surrey.

5.1 IMPLEMENTATION:

It is expected that the amalgamated CRRU will become operational in 2021/22, upon endorsement of the Service Level Agreement, and that the HR process will begin immediately upon approval of this business case, in order to mitigate impact and backlog. Ideally, the new employees would be hired by the first quarter of FY2021/2022.

5.2 Performance Evaluation Framework

As with all public safety initiatives, it is critical that the amalgamated CRRU is guided by a comprehensive performance evaluation framework. It is critical that this framework not only captures the activities and service demands over time, but also the downstream impacts of the unit's work on the organized crime landscape and communities at large. In support of this key priority, SPD is working in consultation with Ministry partners to develop a comprehensive list of performance metrics, which link to the key

priorities and objectives of the unit.

To evaluate and measure the success of each initiative, several levels of analysis are employed. Descriptive analyses of all metrics are conducted to provide an overview of the activities, outputs, and outcomes of each initiative. Additional context is provided to situate these metrics within the broader context of the unit's operational environment. Comparative analyses of the unit's outputs and outcomes across reporting periods are completed to show changes to unit performance over time, as well as the cumulative impact of the initiative to-date.

All findings and analyses will be included in a performance metrics report that will be completed on a biannual basis. The report will be shared with Executive at PSSG and CFSEU-BC, including the CFSEU-BC/OCABC Board of Governance. Briefings will be held both internally and externally to ensure that all stakeholders have a chance to voice their opinions on the report findings and discuss potential implications for next performance cycle. This iterative process ensures that both PSSG and CFSEU-BC have a mutual understanding of the success of each initiative and ensure that initiatives continue to meet key mandates and priorities.

5.3 Service Level Agreement

s.15; s.16

GENERAL SERVICE AGREEMENT



<i>For Administrative Purposes Only</i>	
<p>Ministry Contract No.: SGPSB22CS12</p> <p>Requisition No.: _____</p> <p>Solicitation No.(if applicable): _____</p> <p>Commodity Code: _____</p> <p>Contractor Information</p> <p>Supplier Name: Equifax Canada Co.</p> <p>Supplier No.: 16877</p> <p>Telephone No.: 778-877-8067</p> <p>E-mail Address: john.maiorino@equifax.com</p> <p>Website: _____</p>	<p>Financial Information</p> <p>Client: 010</p> <p>Responsibility Centre: 15407</p> <p>Service Line: 11710</p> <p>STOB: 6309</p> <p>Project: 1500000</p> <p>Template version: February 20, 2020</p>

TABLE OF CONTENTS

No.	Heading	Page
1.	Definitions	1
1.1	General	1
1.2	Meaning of "record"	2
2.	Services	2
2.1	Provision of services	2
2.2	Term	2
2.3	Supply of various items	2
2.4	Standard of care	2
2.5	Standards in relation to persons performing Services	2
2.6	Instructions by Province	2
2.7	Confirmation of non-written instructions	2
2.8	Effectiveness of non-written instructions	2
2.9	Applicable laws	2
3.	Payment	3
3.1	Fees and expenses	3
3.2	Statements of accounts	3
3.3	Withholding of amounts	3
3.4	Appropriation	3
3.5	Currency	3
3.6	Non-resident income tax	3
3.7	Prohibition against committing money	3
3.8	Refunds of taxes	4
4.	Representations and Warranties	4
5.	Privacy, Security and Confidentiality	4
5.1	Privacy	4
5.2	Security	4
5.3	Confidentiality	4
5.4	Public announcements	5
5.5	Restrictions on promotion	5
6.	Material and Intellectual Property	5
6.1	Access to Material	5
6.2	Ownership and delivery of Material	5
6.3	Matters respecting intellectual property	5
6.4	Rights relating to Incorporated Material	5

7.	Records and Reports	6
7.1	Work reporting	6
7.2	Time and expense records	6
8.	Audit	6
9.	Indemnity and Insurance	6
9.1	Indemnity	6
9.2	Insurance	6
9.3	Workers compensation	6
9.4	Personal optional protection	6
9.5	Evidence of coverage	7
10.	Force Majeure	7
10.1	Definitions relating to force majeure	7
10.2	Consequence of Event of Force Majeure	7
10.3	Duties of Affected Party	7
11.	Default and Termination	7
11.1	Definitions relating to default and termination	7
11.2	Province's options on default	8
11.3	Delay not a waiver	8
11.4	Province's right to terminate other than for default	8
11.5	Payment consequences of termination	8
11.6	Discharge of liability	8
11.7	Notice in relation to Events of Default	9
12.	Dispute Resolution	9
12.1	Dispute resolution process	9
12.2	Location of arbitration or mediation	9
12.3	Costs of mediation or arbitration	9
13.	Miscellaneous	9
13.1	Delivery of notices	9
13.2	Change of address or fax number	10
13.3	Assignment	10
13.4	Subcontracting	10
13.5	Waiver	10
13.6	Modifications	10
13.7	Entire agreement	10
13.8	Survival of certain provisions	10
13.9	Schedules	10
13.10	Independent contractor	11
13.11	Personnel not to be employees of Province	11

13.12	Key Personnel	11
13.13	Pertinent Information	11
13.14	Conflict of interest	11
13.15	Time	11
13.16	Conflicts among provisions	11
13.17	Agreement not permit nor fetter	11
13.18	Remainder not affected by invalidity	12
13.19	Further assurances	12
13.20	Additional terms	12
13.21	Tax Verification	12
13.22	Governing law	12
14.	Interpretation	12
15.	Execution and Delivery of Agreement	12

SCHEDULE A – SERVICES

- Part 1 - Term
- Part 2 - Services
- Part 3 - Related Documentation
- Part 4 - Key Personnel

SCHEDULE B – FEES AND EXPENSES

- Part 1 - Maximum Amount Payable
- Part 2 - Fees
- Part 3 - Expenses
- Part 4 - Statements of Account
- Part 5 - Payments Due

SCHEDULE C – APPROVED SUBCONTRACTOR(S)

SCHEDULE D – INSURANCE

SCHEDULE E – PRIVACY PROTECTION SCHEDULE

SCHEDULE F – ADDITIONAL TERMS

SCHEDULE G – SECURITY SCHEDULE

SCHEDULE H – TAX VERIFICATION

APPENDIX 1 – SERVICE LEVELS AND PERFORMANCE STANDARDS

THIS AGREEMENT is dated for reference the 1st day of July, 2021.

BETWEEN:

Equifax Canada Co. (the "Contractor") with the following specified address and fax number:
5700 Yonge Street, Suite 1501
Toronto, Ontario
M2M 4K2
TEL: (416) 277-5253 FAX: (416) 227-5340

AND:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, as represented by the Minister of public Safety and Solicitor General (the "Province") with the following specified address and fax number:
Policing and Security Branch, Security Programs Division
PO Box 9285 Stn Prov Gov't
3350 Douglas Street
Victoria, B.C.
V8Z 3L1
FAX: (250) 356-5987

The Province wishes to retain the Contractor to provide the services specified in Schedule A and, in consideration for the remuneration set out in Schedule B, the Contractor has agreed to provide those services, on the terms and conditions set out in this Agreement.

As a result, the Province and the Contractor agree as follows:

1 DEFINITIONS

General

1.1 In this Agreement, unless the context otherwise requires:

- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
- (b) "Incorporated Material" means any material in existence prior to the start of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
- (c) "Material" means the Produced Material and the Received Material;
- (d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced or provided by the Contractor or a Subcontractor and includes the Incorporated Material;
- (e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Province or any other person;
- (f) "Services" means the services described in Part 2 of Schedule A;
- (g) "Subcontractor" means a person described in paragraph (a) or (b) of section 13.4; and

- (h) "Term" means the term of the Agreement described in Part 1 of Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

- 1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by Province

- 2.6 The Province may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are carried out.

Confirmation of non-written instructions

- 2.7 If the Province provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Province in writing, which request the Province must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

- 2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

3 PAYMENT

Fees and expenses

- 3.1 If the Contractor complies with this Agreement, then the Province must pay to the Contractor at the times and on the conditions set out in Schedule B:
- (a) the fees described in that Schedule;
 - (b) the expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Province's opinion, are necessarily incurred by the Contractor in providing the Services; and
 - (c) any applicable taxes payable by the Province under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Province is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Province a written statement of account in a form satisfactory to the Province upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

- 3.3 Without limiting section 9.1, the Province may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Province and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Province to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Province.

Appropriation

- 3.4 The Province's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Province during which payment becomes due.

Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are to Canadian dollars.

Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Province may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

- 3.7 Without limiting section 13.10(a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Province to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

- 3.8 The Contractor must:
- (a) apply for, and use reasonable efforts to obtain, any available refund, credit, rebate or remission of federal, provincial or other tax or duty imposed on the Contractor as a result of this Agreement that the Province has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement; and
 - (b) immediately on receiving, or being credited with, any amount applied for under paragraph (a), remit that amount to the Province.

4 REPRESENTATIONS AND WARRANTIES

- 4.1 As at the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Province as follows:
- (a) except to the extent the Contractor has previously disclosed otherwise in writing to the Province,
 - (i) all information, statements, documents and reports furnished or submitted by the Contractor to the Province in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,

- (ii) the Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractual or other agreements in place and available to enable the Contractor to fully perform the Services and to grant any licenses under this Agreement, and
 - (iii) the Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and
- (b) if the Contractor is not an individual,
 - (i) the Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and
 - (ii) this Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:

- (a) make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, alteration or disposal; and
- (b) comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Province's prior written consent except:

- (a) as required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
- (b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or
- (c) if it is information in any Incorporated Material.

Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Province and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

- 5.5 The Contractor must not, without the prior written approval of the Province, refer for promotional purposes to the Province being a customer of the Contractor or the Province having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Province, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Province.

Ownership and delivery of Material

- 6.2 The Province exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Province immediately upon the Province's request.

Matters respecting intellectual property

- 6.3 The Province exclusively owns all intellectual property rights, including copyright, in:
- (a) Received Material that the Contractor receives from the Province; and
 - (b) Produced Material, other than any Incorporated Material.

Upon the Province's request, the Contractor must deliver to the Province documents satisfactory to the Province that irrevocably waive in the Province's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Province of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Province:
- (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to exercise, in respect of that Incorporated Material, the rights set out in the *Copyright Act* (Canada), including the right to use, reproduce, modify, publish and distribute that Incorporated Material; and
 - (b) the right to sublicense or assign to third-parties any or all of the rights granted to the Province under section 6.4(a).

7 RECORDS AND REPORTS

Work reporting

- 7.1 Upon the Province's request, the Contractor must fully inform the Province of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Province. Unless otherwise specified in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement ends.

8 AUDIT

- 8.1 In addition to any other rights of inspection the Province may have under statute or otherwise, the Province may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Province's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

- 9.1 The Contractor must indemnify and save harmless the Province and the Province's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Province or any of the Province's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "Loss") to the extent the Loss is directly or indirectly caused or contributed to by:
- (a) any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or
 - (b) any representation or warranty of the Contractor being or becoming untrue or incorrect.

Insurance

- 9.2 The Contractor must comply with the Insurance Schedule attached as Schedule D.

Workers compensation

- 9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

- 9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- (a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
 - (b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

- 9.5 Within 10 Business Days of being requested to do so by the Province, the Contractor must provide the Province with evidence of the Contractor's compliance with sections 9.3 and 9.4.

10 FORCE MAJEURE

Definitions relating to force majeure

- 10.1 In this section and sections 10.2 and 10.3:

- (a) "Event of Force Majeure" means one of the following events:
 - (i) a natural disaster, fire, flood, storm, epidemic or power failure,
 - (ii) a war (declared and undeclared), insurrection or act of terrorism or piracy,
 - (iii) a strike (including illegal work stoppage or slowdown) or lockout, or
 - (iv) a freight embargoif the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
- (b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

- 10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

- 10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

- (a) "Event of Default" means any of the following:
 - (i) an Insolvency Event,
 - (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
 - (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and
- (b) "Insolvency Event" means any of the following:
 - (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
 - (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency,
 - (iii) a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
 - (iv) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
 - (v) a receiver or receiver-manager is appointed for any of the Contractor's property, or
 - (vi) the Contractor ceases, in the Province's reasonable opinion, to carry on business as a going concern.

Province's options on default

- 11.2 On the happening of an Event of Default, or at any time thereafter, the Province may, at its option, elect to do any one or more of the following:
- (a) by written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
 - (b) pursue any remedy or take any other action available to it at law or in equity; or
 - (c) by written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

- 11.3 No failure or delay on the part of the Province to exercise its rights in relation to an Event of Default will constitute a waiver by the Province of such rights.

Province's right to terminate other than for default

- 11.4 In addition to the Province's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Province may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

- 11.5 Unless Schedule B otherwise provides, if the Province terminates this Agreement under section 11.4:
- (a) the Province must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Province's satisfaction before termination of this Agreement; and
 - (b) the Contractor must, within 30 days of such termination, repay to the Province any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Province has notified the Contractor in writing was not completed to the Province's satisfaction before termination of this Agreement.

Discharge of liability

- 11.6 The payment by the Province of the amount described in section 11.5(a) discharges the Province from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

- 11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Province of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

- 12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
- (a) the parties must initially attempt to resolve the dispute through collaborative negotiation;
 - (b) if the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the Mediate BC Society; and
 - (c) if the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Arbitration Act*.

Location of arbitration or mediation

- 12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

- 12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

- 13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
- (a) by fax to the addressee's fax number specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
 - (b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
 - (c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or fax number

- 13.2 Either party may from time to time give notice to the other party of a substitute address or fax number, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or fax number specified for the party giving the notice.

Assignment

- 13.3 The Contractor must not assign any of the Contractor's rights or obligations under this Agreement without the Province's prior written consent. Upon providing written notice to the Contractor, the Province may assign to any person any of the Province's rights under this Agreement and may assign to any "government corporation", as defined in the *Financial Administration Act*, any of the Province's obligations under this Agreement.

Subcontracting

- 13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Province's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
- (a) any person retained by the Contractor to perform obligations under this Agreement; and
 - (b) any person retained by a person described in paragraph (a) to perform those obligations fully complies with this Agreement in performing the subcontracted obligations.

Waiver

- 13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

- 13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

- 13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to performance of the Services.

Survival of certain provisions

- 13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedules

- 13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

- 13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:

- (a) an employee or partner of the Province; or
- (b) an agent of the Province except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Province

- 13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Province.

Key Personnel

- 13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in Part 4 of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Province otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

- 13.13 The Province must make available to the Contractor all information in the Province's possession which the Province considers pertinent to the performance of the Services.

Conflict of interest

- 13.14 The Contractor must not provide any services to any person in circumstances which, in the Province's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Province under this Agreement.

Time

- 13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

- 13.16 Conflicts among provisions of this Agreement will be resolved as follows:
- (a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
 - (b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

- 13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Province or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Province or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

- 13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

- 13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

- 13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Tax Verification

13.21 Any terms set out in the attached Schedule H apply to this Agreement.

Governing law

13.22 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION



14.1 In this Agreement:


- (a) “includes” and “including” are not intended to be limiting;
- (b) unless the context otherwise requires, references to sections by number are to sections of this Agreement;
- (c) the Contractor and the Province are referred to as “the parties” and each of them as a “party”;
- (d) “attached” means attached to this Agreement when used in relation to a schedule;
- (e) unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
- (f) the headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
- (g) “person” includes an individual, partnership, corporation or legal entity of any nature; and
- (h) unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

15 EXECUTION AND DELIVERY OF AGREEMENT

15.1 This Agreement may be entered into by a separate copy of this Agreement being executed by, or on behalf of, each party and that executed copy being delivered to the other party by a method provided for in section 13.1 or any other method agreed to by the parties.

The parties have executed this Agreement as follows:

<p>SIGNED on the ____ day of _____, 2021 by the Contractor (or, if not an individual, on its behalf by its authorized signatory or signatories):</p> <p> <small>John LaVecchia (Sep 19, 2021 15:24 EDT)</small></p> <p>_____ Signature(s)</p> <p><u>John LaVecchia</u> Print Name(s)</p> <p><u>Senior Vice President</u> Print Title(s)</p>	<p>SIGNED on the <u>7th</u> day of <u>OCTOBER</u>, 2021 on behalf of the Province by its duly authorized representative:</p> <p> _____ Signature</p> <p><u>Jess Gunnarson</u> Print Name</p> <p><u>Executive Director, Security programs</u> <u>Division, Policing and Security Branch</u> Print Title</p>
--	--


JG on behalf of TT
09/17/2021

Schedule A – Services

PART 1. TERM:

1. Subject to section 2 of this Part 1, the term of this Agreement commences on July 1, 2021 and ends on December 31, 2021.
2. This agreement includes the option to extend the term by an additional three months to March 31, 2022.

PART 2. SERVICES:

- 1.1. **Services Generally.** The Province engages Equifax to provide eIDverifier service. For clarity, references in this Agreement to the Services refer only to those services selected by the Province and agreed to by Equifax to be provided.
- 1.2. **License.** During the Term of this Agreement, Equifax grants to the Province a non-exclusive, non-transferable, revocable license to access and use the Software, which shall include receiving information from the Database, for the sole purpose of receiving the Services for the Province's internal business purposes only. The Province acknowledges and agrees that it shall not acquire or claim any title to any of Equifax's (or its relevant licensor's) Intellectual Property Rights in the Software, Database or Services by virtue of the rights granted to the Province under this Agreement. For clarity, all Intellectual Property Rights in the Software, Database or Services shall remain vested in Equifax (or its relevant licensors, if applicable) and the Province agrees that it will not, at any time, do, or omit to do, anything which is likely to prejudice Equifax's ownership (or its licensors' ownership) of such Intellectual Property Rights.
- 1.3. **Limitation to License.** Except as provided in this Agreement, the Province covenants and agrees that no action whatsoever will be taken to access, store, merge, aggregate, compile, decompile, manipulate, copy, reverse engineer, create derivative products, sublicense, sell, distribute, commercially exploit or otherwise make available for use the Software, Database or Services. Upon termination of the Agreement all license rights to access and use the Software, Database and Services shall immediately cease and the Province shall immediately stop accessing and using the Software and Services.
- 1.4. **Access.** In order to receive Services, the User must provide User Information and input it into HTML application, through which application Software and Database can be accessed and Services shall be delivered to the Province.
- 1.5. **Configuration.** Equifax acknowledges and agrees to deliver the Services in accordance with the Specifications. Without limiting the foregoing, the Province acknowledges and agrees that it is responsible to ensure that its front end systems comply with the Specifications.
- 1.6. **Acceptance.** Once the Services are approved, Equifax will not change the Services in any manner that degrades the functionality (e.g., text, layout, functional operation, new promotions or branding) without the Province's prior approval. At all times, the parties will timely and diligently cooperate with each other in a commercially reasonable manner to facilitate the performance of their respective obligations under the Agreement.
- 1.7. **Configuration Changes.** The Province may request configuration changes to the Services after Acceptance. Equifax may charge the Province for further configuration changes, including without limitation, customized modifications, on a time and material basis, which fees shall be agreed to by the parties in writing and invoiced upon completion and payable in accordance section 3. In any case, after Acceptance as set out in section 4.6, Equifax reserves the right to decline or refuse to complete further configuration changes, where, in Equifax's reasonable judgment, the requested changes cannot successfully be implemented.

- 1.8. ID Proofing.** Notwithstanding sections 2.6 and 2.7, the Province is solely responsible for establishing the ID proofing strategy pursuant to which a User is either authenticated or not authenticated. Equifax may act as a consultant in this respect per the Service Levels outlined in Appendix 1, but the final ID proofing criteria will be set by the Province.
- 1.9. New Releases.** From time to time, Equifax may release new versions of the eID Solution to update, fix, and/or enhance the Software and/or Services (hereinafter, collectively, "New Release"). If in Equifax's sole discretion, the New Release will have no material impact to the Province, Equifax reserves the right to move the Province to the New Release as a part of regular maintenance and at no additional cost to the Province. The New Release may include new or upgraded functionality (hereinafter, collectively, "Feature"), which the Province may implement subject to additional fees for the implementation and use of the Feature. Equifax reserves the right to require the Province to enter into a supplemental or new agreement for the Feature. If in Equifax's sole discretion, the New Release will have a material impact to the Province, Equifax agrees to provide the Province with at least twelve (12) months prior written notice of the changes to the Software and/or Services (the "Notice Period"). During the Notice Period, the Province may opt to implement the New Release or, at the end of the Notice Period, this Agreement shall end. In respect of New Releases having a material impact on the Province, Equifax reserves the right to charge additional fees and require the Province to enter into a supplemental or new agreement, which shall be mutually negotiated in writing.
- 1.10. Reports.** As part of the Services, in addition to the standard reporting available as a part of the Services, Equifax shall also provide to the Province the following reports regarding the activity of the Services:
- Transaction Date Date the User accessed the Authentication Services
 - Transaction Time Time the User accessed the Authentication Services
 - User Name The name of the User
 - Postal Code The postal code of the User
 - Province The province in which the postal code is located
- 1.11. Contractor Representation and Warranty.** Contractor represents and warrants that the services shall meet or exceed the functionality described in Appendix 1.
- 1.12. Specific Disclaimer.** The Province acknowledges and agrees that the Services, including without limitation, the results of the scoring derived pursuant to section 2.8, are dependent, in part, upon information entered by the User, which cannot be controlled. Equifax makes no representation, warranty or guarantee regarding the accuracy, completeness, or reliability of the Services, including without limitation, the results of the scoring derived pursuant to section 2.8, to the extent that such accuracy, completeness or reliability is related to or dependent upon the accuracy, completeness or reliability of the information entered by the User and/or the scoring threshold implemented pursuant to section 2.8. Equifax also makes no representation, warranty or guarantee of the scoring threshold implemented pursuant to section 2.8 to verify or validate the identity of the User. For clarity, the Services are intended to streamline and increase the security of the Province's authentication processes and in any case, should not solely be relied upon to approve or decline a User for receipt of products or services.
- 1.13. General Disclaimer.** Except as otherwise expressly stated herein and in addition to section 2.11, the Services and Software are provided "as is" and Equifax disclaims all other warranties and conditions, express or implied, including without limitation merchantability and fitness for a particular purpose. Except as outlined in Appendix 1. Equifax does not warrant that the Services or Software will operate uninterrupted or error-free.

1.14. Security Obligations and Equifax Audit Rights. The Province shall maintain an information security program that includes appropriate administrative, technical and physical safeguards. The Province will promptly notify Equifax upon the Province's detection of any breach of the Province's systems or any actual unauthorized access to such systems if the breach or access impacts the Equifax products, services or brand in any way and will take appropriate action designed to prevent further unauthorized access. The Province will provide any information that Equifax reasonably requests pertaining to the incident and will cooperate fully with Equifax to investigate any such unauthorized access. Should the services under this agreement change a mutual review of this clause will be initiated to ensure the appropriate safeguards and rights are in place.

PART 3. RELATED DOCUMENTATION:

1. The Contractor must perform the Services in accordance with the obligations set out in this Schedule A including any engagement letter, Solicitation document excerpt, proposal excerpt or other documentation attached as an Appendix to, or specified as being incorporated by reference in, this Schedule.
2. The following are Appendices to this Schedule A:

Appendix 1 – Service Levels and Performance Standards

ATTACHED

PART 4. KEY PERSONNEL:

Not Applicable

Schedule B – Fees and Expenses

1. MAXIMUM AMOUNT PAYABLE:

Maximum Amount: Despite sections 2 and 3 of this Schedule, \$100,000 is the maximum amount which the Province is obliged to pay to the Contractor for fees and expenses under this Agreement (exclusive of any applicable taxes described in section 3.1(c) of this Agreement).

2. FEES:

Annual Transaction Volume – tiers	Price per transaction
0-50,000	\$1.80
50,001 – 100,000	\$1.35
100,001 – 200,000	\$1.30
200,001 – 350,000	\$1.15
350,000+	\$1.05

Setup Fee	- Waived
Incomplete Transactions	- \$0.73
Standard Reporting	- Included

Add-on Services:

Adaptive IQ:	
Setup Fee:	- \$1,500
Transaction fee:	- \$0.20 per transaction
Credit Card Verification	- \$0.15 per transaction
OFAC	- \$0.15 per transaction

Notes:

- Volume tiers will be reviewed and adjusted quarterly (September 30, 2021 and December 30, 2021 to ensure pricing is in correct annual volume tier. New tier pricing will take effect on the first day of the following each review day listed above.
- Initial volume tier will be determined by Equifax and the Province prior to July 1, 2021. Tier will be set according to expected volume in first three months.
- Volume tiers will be calculated on completed transactions only.

3. EXPENSES:

None.

4. STATEMENTS OF ACCOUNT:

Statements of Account: In order to obtain payment of any fees and expenses under this Agreement, for a period from and including the 1st day of a month to and including the last day of that month (each a "Billing Period"),

the Contractor must deliver to the Province on a date after the Billing Period (each a "Billing Date"), a written statement of account in a form satisfactory to the Province containing:

- (a) the Contractor's legal name and address;
- (b) the date of the statement, and the Billing Period to which the statement pertains;
- (c) the Contractor's calculation of all fees claimed for that Billing Period including a declaration that the Services of all units/deliverables provided during that Billing Period;
- (d) for which the Contractor claims fees and a description of the applicable fee rates;
- (e) a chronological listing, in reasonable detail, of any expenses claimed by the Contractor for the Billing Period with receipts attached, if applicable, and, if the Contractor is claiming reimbursement of any GST or other applicable taxes paid or payable by the Contractor in relation to those expenses, a description of any credits, rebates, refunds or remissions the Contractor is entitled to from the relevant taxation authorities in relation to those taxes;
- (f) the Contractor's calculation of all applicable taxes payable by the Province in relation to the Services for the Billing Period;
- (g) a description of this Agreement to which the statement relates;
- (h) a statement number for identification; and
- (i) any other billing information reasonably requested by the Province.

5. PAYMENTS DUE:

Payments Due: Within 30 days of the Province's receipt of the Contractor's written statement of account delivered in accordance with this Schedule, the Province must pay the Contractor the fees and expenses (plus all applicable taxes)

claimed in the statement if they are in accordance with this Schedule. Statements of account or contract invoices offering an early payment discount may be paid by the Province as required to obtain the discount.

Schedule C – Approved Subcontractor(s)

Schedule D – Insurance

1. The Contractor must, without limiting the Contractor's obligation or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Province:
 - (a) Commercial General Liability in an amount not less than \$2,000,000 inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must:
 - (i) include the Province as an additional insured,
 - (ii) be endorsed to provide the Province with 30 days advance written notice of cancellation or material change, and
 - (iii) include a cross liability clause; and
 - (b) Professional Errors and Omissions Liability insuring the Contractor's liability resulting from errors or omissions in the performance of the Services in an amount per occurrence, and in the aggregate, calculated as follows:
 - (i) not less than \$1,000,000, if the "Maximum Amount" set out in Schedule B is less than \$500,000; and
 - (ii) not less than \$2,000,000, if the "Maximum Amount" set out in Schedule B is \$500,000 or greater.
2. All insurance described in section 1 of this Schedule must:
 - (a) be primary; and
 - (b) not require the sharing of any loss by any insurer of the Province.
3. The Contractor must provide the Province with evidence of all required insurance as follows:
 - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Province evidence of all required insurance in the form of a completed Province of British Columbia Certificate of Insurance;
 - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide, within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
 - (c) despite paragraph (a) or (b) above, if requested by the Province at any time, the Contractor must provide to the Province certified copies of the required insurance policies.
4. Despite section 1(b) of this Schedule, if in the Province's sole discretion, the Province has approved in writing either a fronted self-insurance program or a duly licensed captive insurer as an alternative to the Professional Liability Insurance requirement set out in section 1(b), then the Contractor must maintain throughout the Term that alternative in accordance with the terms of the approval.

Schedule E – Privacy Protection Schedule

Definitions

1. In this Schedule,
 - (a) “**access**” means disclosure by the provision of access;
 - (b) “**Act**” means the *Freedom of Information and Protection of Privacy Act*;
 - (c) “**contact information**” means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
 - (d) “**personal information**” means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Province and the Contractor dealing with the same subject matter as the Agreement but excluding any such information that, if this Schedule did not apply to it, would not be under the “control of a public body” within the meaning of the Act; and
 - (e) “**privacy course**” means the Province’s online privacy and information sharing training course or other privacy training as approved by the Province.

Purpose

2. The purpose of this Schedule is to:
 - (a) enable the Province to comply with the Province’s statutory obligations under the Act with respect to personal information; and
 - (b) ensure that, as a service provider, the Contractor is aware of and complies with the Contractor’s statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor’s obligations, or the exercise of the Contractor’s rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
 - (a) the purpose for collecting it;
 - (b) the legal authority for collecting it; and
 - (c) the title, business address and business telephone number of the person designated by the Province to answer questions about the Contractor’s collection of personal information.

Privacy Training

6. The Contractor must ensure that each person who will provide services under the Agreement that involve

the collection or creation of personal information will complete, at the Contractor's expense, the privacy course prior to that person providing those services.

7. The requirement in section 6 will only apply to persons who have not previously completed the privacy course.

Accuracy of personal information

8. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Province to make a decision that directly affects the individual the information is about.

Requests for access to personal information

9. If the Contractor receives a request for access to personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province unless the Agreement expressly requires the Contractor to provide such access and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

10. Within 5 Business Days of receiving a written direction from the Province to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
11. When issuing a written direction under section 10, the Province must advise the Contractor of the date the correction request to which the direction relates was received by the Province in order that the Contractor may comply with section 12.
12. Within 5 Business Days of correcting or annotating any personal information under section 10, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Province, the Contractor disclosed the information being corrected or annotated.
13. If the Contractor receives a request for correction of personal information from a person other than the Province, the Contractor must promptly advise the person to make the request to the Province and, if the Province has advised the Contractor of the name or title and contact information of an official of the Province to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

14. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

15. Unless the Province otherwise directs in writing, the Contractor must not store personal information

outside Canada or permit access to personal information from outside Canada.

Retention of personal information

16. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

17. Unless the Province otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of personal information

18. Unless the Province otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Province if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
19. Unless the Agreement otherwise specifies or the Province otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

20. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.2 of the Act, if in relation to personal information in the custody or under the control of the Contractor, the Contractor:
 - (a) receives a foreign demand for disclosure;
 - (b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or
 - (c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure

the Contractor must immediately notify the Province and, in so doing, provide the information described in section 30.2(3) of the Act. In this section, the phrases "foreign demand for disclosure" and "unauthorized disclosure of personal information" will bear the same meanings as in section 30.2 of the Act.

Notice of unauthorized disclosure

21. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information in the custody or under the control of the Contractor, the Contractor must immediately notify the Province. In this section, the phrase "unauthorized disclosure of personal information" will bear the same meaning as in section 30.5 of the Act.

Inspection of personal information

22. In addition to any other rights of inspection the Province may have under the Agreement or under statute, the Province may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the

Contractor's information management policies or practices relevant to the Contractor's management of personal information or the Contractor's compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

23. The Contractor must in relation to personal information comply with:
 - (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
 - (b) any direction given by the Province under this Schedule.
24. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

25. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

26. In addition to any other rights of termination which the Province may have under the Agreement or otherwise at law, the Province may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

27. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
28. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
29. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
30. If a provision of the Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
31. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 32, the law of any jurisdiction outside Canada.

32. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

Schedule F – Additional Terms

Not Applicable

Schedule G – Security Schedule

Definitions

1. In this Schedule:

- (a) **“Device”** means any device to manage, operate or provide the Services or to connect to any Systems or any Province system or network, or that is capable of storing any Protected Information, and includes any workstation or handheld device the Contractor authorizes Personnel to use in relation to this Agreement;
- (b) **“Facilities”** means the physical locations (excluding those of the Province) the Contractor uses to provide the Services, or to house Systems or records containing Protected Information;
- (c) **“Least Privilege”** means the principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks so as to limit the damage that can result from accident, error or unauthorized use;
- (d) **“Need-to-Know”** means the principle where access is restricted to authorized individuals whose duties require such access and not merely because of status, rank or office;
- (e) **“Personnel”** means all individuals hired or used by the Contractor and Subcontractors to perform the Contractor’s obligations under this Agreement, including unpaid volunteers and the Contractor or a Subcontractor if an individual;
- (f) **“Policies”** means the intentions and directions of an organization or part of it, as expressed in record form by its top management (including, for example, policies, directions, standards, practices, procedures and guidelines);
- (g) **“Protected Information”** means any and all:
 - (i) “personal information” as defined in the Privacy Protection Schedule if attached;
 - (ii) information and records of information the Contractor is required to treat as confidential under this Agreement; and
 - (iii) records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked or instructed by the Province to be so preserved or otherwise treated as “Protected Information” under this Agreement;
- (h) **“Security Event Logs”** means any confirmed logs (also known as audit records) of events, notifications or alerts that any component of any Device or other device (not limited to security device), or any Systems or other system or software is technically capable of producing in relation to its status, functions and activities that may be used for such purposes as security investigations, auditing, monitoring and determining security incidents (examples of components capable of producing such logs include firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, dynamic host configuration protocols, dynamic naming services, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application firewalls);
- (i) **“Systems”** means any systems, subsystems, equipment, infrastructure, networks, management

networks, servers, hardware and software the Contractor uses in relation to this Agreement, including for managing, operating or providing the Services, but excluding any the Province owns or makes available to the Contractor for the Contractor to use in relation to this Agreement;

Additional obligations

2. The Contractor must comply with Appendix G1 if attached.

PERSONNEL

Confidentiality agreements

3. The Contractor must not permit any person the Contractor hires or uses to access or obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under this Agreement.

Personnel security screening

4. The Contractor may only permit individual Personnel to have access to any Protected Information or other asset of the Province (including to any system, network or device the Province makes available to the Contractor) in relation to this Agreement, if, after:
 - (a) verifying their identity and relevant education, professional qualifications and employment history;
 - (b) completing a criminal record check taking into consideration the duties of the individual, the level of access the individual may have to the Contractor's Systems and the type and sensitivity of information to which the individual may be exposed;
 - (c) requiring Personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law;
 - (d) performing any additional screening this Agreement or applicable law may require; and
 - (e) performing any additional background checks the Contractor considers appropriate,the Contractor is satisfied that the individual does not constitute an unreasonable security risk.
5. If any criminal record check or proactive disclosure reveals a prior criminal offence or pending criminal matter, the Contractor must make a reasonable determination of whether the applicable person constitutes an unreasonable security risk, taking into consideration the duties of the individual and the type and sensitivity of information to which the individual may be exposed.

6. Intentionally deleted.

Personnel information security training

7. Unless otherwise specified in this Agreement, the Contractor must ensure all Personnel complete any relevant information security training, at the Contractor's expense, before they provide any Services, or receive or are given access to any Protected Information or any system, device or secure facility of the Province, and thereafter at least annually.

Security contact

8. If not set out elsewhere in this Agreement, the Contractor (but not a Subcontractor) must provide in writing to the Province the contact information for the individual who will coordinate compliance by the Contractor and all Subcontractors and act as a direct contact for the Province on matters relating to this Schedule. For the purposes of this Schedule, unless and until the Contractor notifies the Province in writing of a change, the Province's contact person is:

Julia Szadkowski, VP Legal and General Counsel
Equifax Canada Co.
5700 Yonge St, Suite 1501
Toronto, ON M2M 4K2

Supply chain

9. The Contractor must ensure that the security requirements of those in its upstream and downstream supply chain are documented, followed, reviewed, and updated on an ongoing basis as applicable to this Agreement.

GENERAL POLICIES AND PRACTICES

Information security policy

10. The Contractor must have an information security Policy that is:
 - (a) based on recognized industry standards; and
 - (b) reviewed and updated at least every three years.

Compliance and Standard for Security Controls

11. Unless this Agreement otherwise specifies, the Contractor must apply controls and security management practices to manage or operate Protected Information and Systems, Devices, and Facilities that are compliant with certification with ISO/IEC 27001 or other equivalent standards.

Contractor security risk assessments

12. The Contractor must undertake a security threat and risk assessment against an industry security standard before placing any new or materially changed Systems or services into production.

Change control and management

13. The Contractor must:
 - (a) implement and maintain change control processes for Facilities, Systems and Devices in line with applicable security best practices to reduce security-related risks with respect to implemented significant changes; and
 - (b) ensure that adequate testing of any change is completed before the change is put into production.

Backups and restores

14. The Contractor must ensure that:

- (a) it has a backup Policy that is followed and is reviewed, updated and tested at least annually;
- (b) backups are taken and tested in accordance with the Contractor's backup Policy, but in any event at least annually; and
- (c) frequency and completeness of backups is based on reasonable industry practice.

Business continuity plan and disaster recovery plan

- 15. The Contractor must ensure that it has a documented business continuity plan and a disaster recovery plan that is reviewed at least annually.
- 16. The Contractor must ensure that Facilities and Systems are protected from loss, damage or other occurrence, including fire and environmental hazards and power interruptions, that may result in any of those Facilities and Systems being unavailable when required to provide the Services.

Security Incident Response and Management

- 17. The Contractor must ensure that it has a security incident management Policy and response plan that is reviewed at least annually.

PROTECTED INFORMATION AND DATA SECURITY

Encryption

- 18. The Contractor must ensure that end-to-end encryption is implemented for all Protected Information in transit.

No storage on unencrypted portable media

- 19. The Contractor must ensure that no Protected Information is stored on portable media for transport outside of the Facilities or Systems without both the prior written approval of the Province and ensuring that the portable media and the Protected Information are encrypted.

Encryption standard

- 20. With respect to section 18 regarding data in transit, encryption must comply with the Province's "Cryptographic Standards for Information Protection" accessible at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>.

Isolation controls and logical isolation of data

- 21. The Contractor must implement and maintain the logical isolation of Protected Information, in effect, uninterrupted and active at all times using the following industry leading and appropriately managed system isolation and management technologies:
 - (a) web application firewall (WAF) technology;
 - (b) security information and event management (SIEM) technology;
 - (c) third party anti-malware software agents;
 - (d) virtual desktop and multi-factor access controls for Systems administrators;
 - (e) network firewall technology; and

- (f) centralized access management and change management technology.

ACCESS AND AUTHENTICATION

User Identifiers

- 22. The Contractor must assign and ensure that user identifiers are unique and personal for log in to Systems and Devices.

Access

- 23. The Contractor must implement, follow, and regularly review and update, access control Policies that address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts for Facilities, Systems and Devices within the Contractor's control.
- 24. The Contractor must ensure that all access to Protected Information and to Facilities, Systems and Devices is based Least Privilege and Need-to-Know" based on role and responsibilities. The Contractor must identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse.
- 25. The Contractor must verify an individual's identity before assigning the individual a unique identifier that would give them access to Facilities, Systems or Devices.
- 26. The Contractor must implement a formal user registration process for Personnel that includes:
 - (a) verification of access levels;
 - (b) creating and maintaining records of access privileges;
 - (c) audit processes; and
 - (d) actions to ensure access is not given before approval is granted by the Contractor.
- 27. The Contractor must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts.
- 28. The Contractor must implement a monitoring process to oversee, manage and review Personnel access rights and roles at regular intervals.
- 29. The Contractor must ensure that all Systems and Devices:
 - (a) are configured in alignment with industry standards;
 - (b) enforce a limit of consecutive invalid logon attempts by a user during a predetermined time period;
 - (c) automatically lock the applicable account and Systems after failed logon failures;
 - (d) limit the number of concurrent sessions;
 - (e) prevent further access to Systems by initiating a session lock; and

- (f) provide the capability of disconnecting or disabling remote access to the Systems.

Authentication

- 30. The Contractor must use or require complex passwords or personal identification numbers (PINs) that are not shared, default or blank and that are encrypted (not displayed) when entered, biometric accesses, keys, smart cards, other logical or access controls, or combinations of them, to control access to Protected Information and to Systems and Devices.
- 31. The Contractor must ensure that Systems for password-based authentication:
 - (a) enforce minimum password complexity, including requiring passwords to be case sensitive, contain a minimum of eight characters and a combination of upper-case letters, lower-case letters, numbers, and/or special characters;
 - (b) change authentication passwords regularly at predetermined intervals, but at a minimum semi-annually;
 - (c) store and transmit only encrypted representations of passwords;
 - (d) enforce password minimum and maximum lifetime restrictions;
 - (e) prohibit password reuse;
 - (f) prevent reuse of identifiers; and
 - (g) disable the identifier after ninety days of inactivity.

Highly sensitive Protected Information

- 32. If this Agreement or the Province under this Agreement indicates that any Protected Information is highly sensitive, the Contractor must also ensure that Systems enforce with respect to that Protected Information:
 - (a) two-factor authentication for access;
 - (b) enhanced logging that logs all accesses;
 - (c) request based access; and
 - (d) no standing access rights.

SECURITY EVENT LOGS

Log generation, log retention and monitoring

- 33. The Contractor must ensure that logging of Security Event Logs is enabled on all applicable Systems components
- 34. The Contractor must retain Security Event Logs for the Systems online for a minimum of 90 days and either online or off-line for an additional period of time adequate to enable the Contractor to conduct effective security investigations into suspected or actual security incidents.

35. The Contractor must review Security Event Logs regularly to detect potential security incidents, using automated tools or equivalent processes for the monitoring, review, correlating and alerting of Security Event Logs.

PROVINCE PROPERTY

Application development

36. If the Services include software development, the Contractor must ensure that the applications and programming interfaces are developed according to industry standards and Province Policies applicable to application development standards. The Contractor must use secure application development practices for the development of the software.

FACILITIES, SYSTEMS, DATABASE AND DEVICE SECURITY

Physical security

37. The Contractor must ensure that adequate physical controls and processes are implemented to ensure that only authorized persons have physical access to the Facilities and Systems.
38. The Contractor must develop, document, and disseminate a physical and environmental protection Policy that it reviews at least annually.
39. The Contractor must review physical access logs at least once monthly.
40. The Contractor must ensure that physical security of any Systems or Facilities being used or capable of being used to house Protected Information meets a standard as would be reasonably expected to provide adequate protection based on the value of the data being protected and the environment in which the Systems or Facilities are located. At a minimum, this should include:
- (a) hardening of the perimeter of the Facilities;
 - (b) physical separation of public and restricted spaces;
 - (c) Intrusion Alarm System (IAS) partitioned to ensure areas containing Protected Information are protected at all times;
 - (d) Access Control Systems (ACS) and/or Key Management processes; and
 - (e) visitor and identity management processes – including access logs and identification badges.

Separation of production from test environments

41. The Contractor must not use any production data in any development, test or training environments used for the Services without the Province's prior written consent. If the Province gives such consent, the production data must, at minimum, be obfuscated (for example, by using data masking functionality).
42. The Contractor must keep its development, test and training environments separate from its production environments used for the Services at all times, even in case of failure.

Systems (including servers) hardening

43. The Contractor must:

- (a) harden all Systems against attack and misuse, using appropriate security best practices for the hardening of the specific deployed platform, before placing those Systems into production;
- (b) ensure that all unsecured and unneeded ports, services, applications, protocols and network communicating applications are uninstalled or disabled on all Systems;
- (c) applying Least Privilege, ensure that the Contractor only configures and makes operational ports, services, applications, protocols and network communicating applications based on the functional requirements of the respective Systems;
- (d) ensure that default passwords and shared accounts are not used for any Systems; and
- (e) in relation to Systems, implement server hardening using configuration security best practices (for example, Center for Internet Security, Inc. (CIS) Benchmarks or equivalent) for any server operating systems, server virtualization, server middleware (for example, web servers and database servers) and application servers.

Perimeter controls (firewall and intrusion prevention system) and network security

44. The Contractor must:

- (a) implement stateful packet inspection firewalls to control traffic flow to and from Systems at all times, and configure the stateful packet inspection firewalls applying security best practices and Least Privilege;
- (b) implement an intrusion prevention System to control and filter traffic flow leaving and entering Systems at all times, and configure the intrusion prevention System applying security best practices; and
- (c) implement a secure network perimeter and network segmentation for Systems, with ingress and egress points that are known and controlled.

Application firewall

45. The Contractor must implement application layer firewalls on Systems:

- (a) at such level of protection as the Province may instruct ; and
- (b) to detect and mitigate application attacks (for example, brute force, OWASP Top 10, SQL injection, cross site scripting).

Management network

46. The Contractor must ensure that for any Systems:

- (a) the management network remains logically separated from any other zone and is not directly accessible from the Internet;
- (b) the management network is internally segmented, with each server's dedicated network interface

on its own segmented network and that interfaces on the management network do not have visibility to each other; and

- (c) all access to the management network is strictly controlled and exclusively enforced through a secure access gateway, bastion host or equivalent.

Remote management and secure access gateway

- 47. The Contractor must perform any remote management of Systems or Devices in a secure manner, using encrypted communication channels and adequate access controls.

Database security

- 48. The Contractor must ensure that for any Systems:
 - (a) database maintenance utilities that bypass controls are restricted and monitored;
 - (b) there is a formal approval process in place for handling requests for disclosure of database contents or for database access, including steps to evaluate privacy impacts and security risks of such requests; and
 - (c) methods to check and maintain the integrity of the data are implemented (for example, consistency checks and checksums).
- 49. For database security, the Contractor must implement logical isolation and encryption of Protected Information.

Device security and antivirus scanning

- 50. The Contractor must ensure all Devices:
 - (a) have antivirus and malware protection as appropriate for the particular Device active at all times;
 - (b) are configured to perform antivirus scans at least once per week;
 - (c) have host-based firewall configured, enabled and active at all times; and
 - (d) have all patches and appropriate security updates installed for the operating system and all installed software.

VULNERABILITY PREVENTION, SCANNING AND MANAGEMENT

Proactive management

- 51. The Contractor must:
 - (a) obtain information in a timely basis about technical vulnerabilities relating to Systems and Devices; and
 - (b) implement processes to stay current with security threats.

Patching

- 52. The Contractor must patch all Systems regularly in line with security best practices and ensure that current

software, operating systems and application patching levels are maintained.

53. The Contractor must ensure that all Systems have patches installed on a regular basis, within the time frame recommended by the manufacturer unless the applicability of the patch is deemed by the Contractor, acting reasonably and following industry best practice, as damaging to the Contractor's Systems. In such case, the Contractor shall take all required alternate measures and precautions to protect the integrity and security of its Systems.
54. The Contractor must ensure that vulnerabilities are remedied and patches installed on an accelerated basis for zero-day, critical and high vulnerabilities. For zero-day vulnerabilities, the Contractor must implement appropriate mitigation measures promptly on notification of the zero-day vulnerability. The Contractor must remediate zero-day, high and critical vulnerabilities through patching, decommission, or compensating controls.
55. The Contractor must patch high vulnerabilities within 30 days or less of discovery and patch medium vulnerabilities within 90 days or less of discovery.

Vulnerability Scanning

- (a) The Contractor must ensure that a vulnerability scan is completed on components of all Systems with any identified vulnerabilities remedied, before being placed into production; and
- (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Web application vulnerability scanning

56. The Contractor must ensure that a vulnerability scan is completed on any web applications used as part of or within the Systems:
 - (a) and on any major changes to such web applications, with any identified vulnerabilities remedied, before being placed into production; and
 - (b) on a regular schedule, set at a minimum of one scan per quarter, unless the Province otherwise consents in writing.

Antivirus and malware scanning

57. The Contractor must ensure that all Systems servers:
 - (a) have antivirus and malware protection configured, active and enabled at all times;
 - (b) have antivirus and malware definitions updated at least once a day; and
 - (c) are configured to undergo a full anti-virus scan for latent infections (to detect infections missed by the real-time agent) at least once a week.

DISPOSALS

Asset disposal

58. The Contractor must ensure that all disposals of assets used in providing or relating to the Services are done in a secure manner that ensures that Protected Information cannot be recovered.

Asset management

59. The Contractor must have asset management and disposal Policies that are followed and reviewed and updated regularly in line with security best practices, and that address hardware, software and other critical business assets.
60. The Contractor must keep an asset management inventory that includes the name of the System, location, purpose, owner, and criticality, with assets added to inventory on commission and removed on decommission.

Information destruction and disposal

61. Within 90 days of the termination or expiry of the Agreement or sooner if requested by the Province, the Contractor will provide the Province with all Province Information in standard machine-readable format or as otherwise reasonably requested by the Province.
62. The Contractor will erase:
 - (a) all records that contain Protected Information and all backups, transitory and extra copies of such records by a date that is the sooner of (i) 1 year of their creation; or (ii) when no longer required by the Province pursuant to this Agreement; and
 - (b) all Security Event Logs when no longer required to be maintained by the Contractor pursuant to this Agreement.

NOTICES, INCIDENTS AND INVESTIGATIONS

Notice of demands for disclosure

63. In addition to any obligation the Contractor may have to notify or assist the Province under applicable law or this Agreement, including the Privacy Protection Schedule if attached, if the Contractor is required (including under an enactment or a subpoena, warrant, order, demand or other request from a court, government agency or other legal authority) to produce, provide access to or otherwise disclose any Protected Information, the Contractor must, unless prohibited by applicable law, immediately notify and provide reasonable assistance to the Province so the Province may seek a protective order or other remedy to prevent or limit the disclosure.

E-discovery and legal holds

64. The Contractor must fully co-operate with the Province to enable the Province to comply with e-discovery and legal hold obligations.

Incidents

65. In addition to any obligation the Contractor may have under applicable law, including the *Freedom of Information and Protection of Privacy Act*, or this Agreement, if, during or after the Term, the Contractor discovers a or actual unwanted or unexpected event or series of events that threaten the privacy or security of Protected Information (including its unauthorized access, collection, use, disclosure, alteration, storage or disposal) whether accidental or deliberate, the Contractor must:
 - (a) immediately report the particulars of such incident to, and follow the instructions of, the Province, confirming any oral report with a notice in writing to the Province as soon as reasonably practicable

(if unable to contact the Province's contract manager or other designated contact for this Agreement, the Contractor must follow the procedure for reporting and managing information incidents on the Province's website at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents>; and

- (b) make every reasonable effort to recover the records containing Protected Information and contain and remediate such incident, following such reasonable instructions as the Province may give.

Investigations support and security investigations

66. The Contractor must:

- (a) conduct security investigations in the case of incidents (including any security breach or compromise) affecting Devices, Facilities, Systems or Protected Information, collecting evidence, undertaking forensic activities and taking such other actions as needed;
- (b) provide the Province with any related investigation reports, which the Contractor may sanitize first;
- (c) upon the Province's request, provide the Province with any logs relating to such investigation reports as validation/confirmation of such investigation, which the Contractor may sanitize first; and maintain a chain of custody in all such security investigations it undertakes.

67. Upon the Province's request, the Contractor must provide investigative support to the Province to enable the Province to conduct its own security investigations into incidents (including security breaches or compromises) affecting the Systems or Protected Information.

68. The Contractor must work with and support the Province if the Province needs assistance in legal proceedings in relation to security investigations related to Protected Information.

Province Security Threat and Risk Assessment ("STRA") support

69. The Contractor must, via its technical and security resources, support the Province in completing a STRA for the Services and to otherwise assess the risks associated with the Services, including by providing all information and documentation (for example, architecture diagrams, service architecture, controls architecture and technical information), which the Contractor may sanitize first and that the Province may reasonably require for such purpose.

Notification of changes

70. On an annual basis, and on the Province's request, the Contractor will provide the Province with a copy of a compliance certificate from an independent, industry recognized auditor specifying that the Contractor complies with the requirements of ISO 27001. In addition, the Contractor will send timely notification to the Province of any changes to the Contractor's security policies, procedures or agreements that may materially lower the security of the Province Information. Compliance verification

71. Upon the Province's request, the Contractor must provide, at no additional cost, the following security reports to the Province at least every six months during the Term:

- (a) vulnerability scan reports of those Systems providing the Services; and
- (b) patch status reports for those Systems providing the Services.

72. In addition to any other rights of inspection the Province may have under this Agreement or under statute, if the Province has reasonable grounds to believe that the Contractor may be in material breach of this Schedule and that the security of Province may be compromised, the Province will have the right, at any reasonable time and on reasonable notice to the Contractor, to:
- (a) request the Contractor to verify compliance with this Schedule and to keep security controls documentation or records to support compliance; and
 - (b) enter on the Contractor's premises and Facilities to inspect and to validate the Contractor's compliance with its obligations under this Schedule subject to the Province's material compliance with any reasonable policy of Contractor generally applicable to third party access to Contractor's premises and Facilities.
73. The Contractor must permit, and provide reasonable assistance to, the exercise by the Province of the Province's rights under this section. If any non-compliance or deficiency is found, the Province may (in addition to any other rights it may have) require the Contractor, at the Contractor's expense, to develop and implement a corrective action plan within a reasonable time.

Notice of non-compliance

74. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Province of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

MISCELLANEOUS

Interpretation

75. In this Schedule, unless otherwise specified, references to sections by number are to sections of this Schedule.
76. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under this Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
77. Any reference to a specified Policy refers to it as may be revised or replaced from time to time.
78. If a provision of this Schedule conflicts with a documented process required by this Schedule to be created or maintained by the Contractor, the provision of the Schedule will prevail to the extent of the conflict.

Referenced documents

Survival

79. Sections 61, 64, 65, 66, 67 and 68, and other obligations of the Contractor in this Schedule which, by their terms or nature, are intended to survive the completion of the Services or the termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedule G – Appendix G1 – Additional Security Obligations

The personnel security screening requirements set out in this Appendix G1 are for the purpose of assisting the Contractor determine whether or not a Services Worker constitutes an unreasonable security risk.

Verification of name, date of birth and address

1. The Contractor must verify the name, date of birth and current address of a Services Worker by viewing at least one piece of “primary identification” of the Services Worker and at least one piece of “secondary identification” of the Services Worker,* as described in the table following this section. The Contractor must obtain or create, as applicable, Records of all such verifications and retain a copy of those Records. For a Services Worker from another province or jurisdiction, reasonably equivalent identification documents are acceptable.

Primary Identification	Secondary Identification
<p>Issued by ICBC:</p> <ul style="list-style-type: none"> • B.C. driver’s licence or learner’s licence (must have photo) • B.C. Identification (BCID) card <p>Issued by provincial or territorial government:</p> <ul style="list-style-type: none"> • Canadian birth certificate <p>Issued by Government of Canada:</p> <ul style="list-style-type: none"> • Canadian Citizenship Card • Permanent Resident Card • Canadian Record of Landing/Canadian Immigration Identification Record 	<ul style="list-style-type: none"> • School ID card (student card) • Bank card (only if holder’s name is on card) • Credit card (only if holder’s name is on card) • Passport • Foreign birth certificate (a baptismal certificate is not acceptable) • Canadian or U.S. driver’s licence • Naturalization certificate • Canadian Forces identification • Police identification • Foreign Affairs Canada or consular identification • Vehicle registration (only if owner’s signature is shown) • Picture employee ID card • Firearms Acquisition Certificate • Social Insurance Card (only if has signature strip) • B.C. CareCard • Native Status Card • Parole Certificate ID • Correctional Service Conditional Release Card

*It is not necessary that each piece of identification viewed by the Contractor contains the name, date of birth and current address of the Services Worker. It is sufficient that, in combination, the identification viewed contains that information.

Verification of education and professional qualifications

2. The Contractor must verify, by reasonable means, any relevant education and professional qualifications of a Services Worker, obtain or create, as applicable, Records of all such verifications, and retain a copy of those Records.

Verification of employment history and reference checks

3. The Contractor must verify, by reasonable means, any relevant employment history of a Services Worker, which will generally consist of the Contractor requesting that a Services Worker provide employment references and the Contractor contacting those references. If a Services Worker has no relevant employment history, the Contractor must seek to verify the character or other relevant personal characteristics of the Services Worker by requesting the Services Worker to provide one or more personal references and contacting those references. The Contractor must obtain or create, as applicable, Records of all such verifications and retain a copy of those Records.

Security interview

4. The Contractor must allow the Province to conduct a security-focused interview with a Services Worker if the Province identifies a reasonable security concern and notifies the Contractor it wishes to do so.

Schedule H – Tax Verification Schedule

Not Applicable

Appendix 1 – Service Levels and Performance Standards

1. Service Levels and Performance Standards

A. **Availability.** The Services will be operational, a minimum of 95% of the time during any thirty (30) day period, exclusive of scheduled down times. A scheduled downtime is an Service or Equifax Canada Page downtime which occurs during the Scheduled Maintenance Window or is: (a) scheduled with at least three (3) days prior notice; (b) scheduled for off-peak hours; and (c) does not exceed 6 hours at any one time.

B. **Response Time.** The average response time will not exceed more than 30 seconds for the Services solution to respond after successfully accepting a request.

C. **Bandwidth.** The bandwidth representing the servers' connection to the Internet will be operating at peak capacity no more than 10 minutes in any 24 hour period and at greater than 70% of peak capacity no more than 60 consecutive minutes of any 24 hour period.

E. **Functionality.** Equifax will ensure that each transaction posts only a "soft" inquiry to a User's credit report such that only the consumer and not a creditor will see the inquiry and a consumer's credit will not be affected as a result of the Services. Equifax will ensure that information provided by the Province with respect to a particular User will not be used by Equifax to authenticate or verify information in any other Transaction.

F. **Error Resolution.** For all incidents, Equifax will make all commercially reasonable attempts to facilitate the Equifax resolution of the condition within a reasonable time frame of Equifax learning of the loss or degradation of the Services.

G. **Browser Compatibility.** The Services support the latest version of Internet Explorer and Netscape. The Province may request that additional versions of a browser or additional browsers be added to the list that Equifax supports. Equifax generally will support only widely used and industry compliant browsers with industry best practices. If Equifax support is deemed appropriate, in Equifax's sole discretion, Equifax will determine the level of effort to provide this support and provide the Province an estimate of the development time and expense. Equifax reserves the right to terminate technology that it deems to be commercially inappropriate and will provide ninety (90) days' prior notice of such termination.

H. **Customer Support.** Equifax will provide no direct support or technical support to the Users. the Province will provide level 1 support to the Users. Equifax will provide level 2 technical support solely to the Province approved contacts relative to unscheduled outages.

2. Service Availability – Metrics Calculation and Component Definitions

Item	Definition
Emergency Maintenance	"Emergency Maintenance" means unscheduled maintenance periods during which emergency maintenance is performed or critical priority level problems relating to the Province's system deployment are resolved. By way of example, Emergency Maintenance includes deployment of a critical patch supplied by a third party vendor. Although Emergency Maintenance is not required to be scheduled, Equifax will attempt to notify the Province and coordinate Emergency Maintenance to minimize the impact.
Impacted Transaction	An "Impacted Transaction" is a transaction that was not processed because the Services or a component or components thereof was/were

Item	Definition
	unavailable.
Incident Response Time	<p>Incident response time shall begin at the Service Availability incident report problem start time recorded in the Equifax Canada incident tracking system. This time shall be the earlier of:</p> <ul style="list-style-type: none"> (a) The time that Equifax becomes aware of the Service Availability incident by receiving customer notification (b) The time that Equifax becomes aware of the Service Availability incident by Equifax defined monitoring processes. <p>Incident response time shall end when the Equifax responds to the incident reported by recording the Province incident and executing escalation and notification procedures for the incident as necessary. (please refer to Severity Levels under subsection 3 below).</p> <p>Please Note: The Province may need to remain engaged during problem resolution to provide details, assist in problem determination, and to validate the problem has been resolved.</p>
Minutes in Month	Minutes in Month is equal to the days in the calendar month times 1,440.

Permitted Exceptions	<p>A “<u>Permitted Exception</u>” is a service-impacting event caused by any of the following conditions or occurrences. Calculations of factors necessary to determine whether Equifax’s performance meets the above performance standards shall exclude Permitted Exceptions to the extent the inclusion of such items would result in Equifax not meeting a performance standard that Equifax otherwise would have met or exceeded. Notwithstanding anything to the contrary, Equifax shall have no obligation to resolve any condition consisting of or resulting from a Permitted Exception.</p> <ul style="list-style-type: none"> (a) User Information, hardware or software or any resources provided to Equifax by the Province or the Province’s contractors, including without limitation data, information, directions or specifications or adversely impact Equifax’s ability to meet the performance standard(s); (b) Force majeure events and other causes or events beyond Equifax’s reasonable control; (c) Scheduled or Province-approved maintenance events; (d) Downtime attributable to unavailability of data or data feeds, data communication failures or response times for transmissions sent through public networks including the Internet; (e) The Province’s failure to comply with Equifax’s minimum software requirements; (f) Any Province -approved exceptions;
----------------------	---

Item	Definition
	<p>(g) Use of eIDverifier or Services in a manner other than as specified in the Implementation Guide or as otherwise designed or intended; or</p> <p>(h) The use, operation, or combination of the Authentication system or Services with software, data, equipment, or materials not specified in the documentation.</p>
Root Cause Analysis	<p>The Equifax Canada Root Cause Analysis documentation will contain the following information:</p> <ol style="list-style-type: none"> 1. Incident Start and End Date and Time 2. Problem Description 3. Root Cause 4. Recovery 5. Permanent Resolution <p>The Root Cause Analysis will be made available upon request within two (2) business days of the Service Availability Incident resolution.</p>
Scheduled Downtime	<p>“Scheduled Downtime” means periods of unavailability of the Service due to regularly scheduled weekly maintenance windows, any maintenance scheduled in advance with Province or implementation of Province initiated changes. The periods during which Equifax systems are unavailable due to planned maintenance is defined in the Scheduled Maintenance Windows section for data source.</p> <p>A customer solution may utilize multiple products and services and the Scheduled Maintenance Window of each of these products and services may impact the performance of the customer solution during the Scheduled Maintenance Window of the individual products and services, for which Equifax is not responsible.</p>
Service Availability Uptime	<p>Uptime will be calculated and reported on a monthly basis.</p> <p>The Service Availability Uptime ratio will be calculated in accordance with the following formula:</p> $\frac{[\text{Minutes in Month} - (\text{Scheduled Downtime} + \text{Emergency Maintenance} + \text{Permitted Exceptions}) - \text{UIM}]}{[\text{Minutes in Month} - (\text{Scheduled Downtime} + \text{Emergency Maintenance} + \text{Permitted Exceptions})]}$

Transaction Response Time	The calculation of the average response time will be performed on a monthly basis. The calculation will not include any functional component consisting of a comparison or aggregation of multiple transactions, the response time of third-party data sources, or any other functionality implementation which is not an integral part of the e Services and is not executed by Equifax.
---------------------------	---

Item	Definition
	<u>Calculation:</u> The transaction response time is calculated by measuring the difference between the receipt of a processing request by the Authentication system at the Equifax data centre and the exit of the output response from the Authentication system. The response time calculations only include the Authentication processing time to the level of generation of questions only for eIDverifier transactions. The time taken to answer these questions and resubmits are dependent upon User interaction and is excluded from this calculation.
User Impacted Minutes	User Impacted Minutes or UIM is the ratio of Impacted Transactions to total transactions times the duration of the incident in minutes, calculated as follows: <i>Wall clock duration of outage x (Total Impacted Transactions During Outage / Total Transactions During Outage)</i>

3. Customer Support Centre

Equifax will provide the client with 24/7/365 contact access to a wide range of technical support, incident management and issue escalation protocol. The Advanced Delivery System contacts below outlines methods and contact protocols.

Severity Levels:

Severity Level	Description	Response
1 Severe Business Disruption	Multiple customers are impacted in production due to a system-wide outage or performance degradation where transactions cannot be completed and redundancy is not available as a bypass or workaround.	Best effort to ensure quick resolution. Equifax IT teams and partners will remain engage 24x7 until resolution. Regular updates to customers every 4 hours.
2 Major Business Disruption	A number of customers (1 or more) are impacted in production due to outage or performance degradation where transactions cannot be completed (due to error or timeout message) however a bypass or workaround is available	Best effort to ensure quick resolution. Equifax IT teams will remain engaged until resolution. Regular updates to customers daily.
3	A limited number of customers (1 or more) are	Best effort for problem root cause

Minor Business Impact	impacted in production. Most submitted transactions are completed as per expectation.	analysis and resolution plan definition. Updates provided upon request.
4 Minor/No Tangible Impact to Customer a	An incident with no tangible external customer Impact (Questions, Customization requests, etc).	TBD

Signature: J Guarascio
J Guarascio (Sep 17, 2021 18:21 EDT)

Email: james.guarascio@equifax.com



Modification Agreement 003

THIS MODIFICATION AGREEMENT dated for reference March 31, 2022

BETWEEN:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, represented by the Minister of Public Safety and Solicitor General

Policing and Security Branch
Security Programs Division
3350 Douglas Street – 4th Floor
Victoria, BC V8Z 7X9

(the "Province")

AND:

ITV Consulting Inc
577 Delora Drive
Victoria, BC V9C 3S2

(the "Contractor")

BACKGROUND

- A. The parties entered into an agreement numbered SGPSPB21CS09 dated for reference April 1, 2020 (the "Agreement").
- B. The parties have agreed to modify the Agreement effective April 1, 2022

AGREEMENT

The parties agree as follows:

- (1) The parties confirm their mutual consent and agreement to exercise the option to renew the Agreement SGPSPB21SC09 for the one-year renewal period. Accordingly, and for greater certainty, the Term of the Agreement shall end on March 31, 2023.

Schedule A, Part 1 – Term is replaced with: The initial term of this Agreement (the "**Initial Term**") commences on April 1, 2020, and ends on March 1, 2023, unless it is terminated earlier in accordance with the provisions of this Agreement.

- (1) Schedule B, Part 1 is replaced with the following:
 - a. Maximum Amount: Despite section 2 and 3 of this Schedule, \$660,000.00 is the maximum amount which the Province is obliged to pay to the Contract for fees and expenses under this Agreement (exclusive of any applicable taxes described in section 3.1(c) of this Agreement).
 - b. The maximum amount the Province is obliged to pay to the Contract for expenses under this agreement during the renewal term of April 1, 2022 to March 31, 2023 is \$220,000.

SGPSPB21SC09



Modification Agreement 003

(2) Schedule B, Part 3 is replaced with the following:

Expenses

- a) Travel, accommodation and meal expenses for travel greater than 32 kilometers away from Victoria, British Columbia on the same basis as the Province pays its Group II employees when they are on travel status; and
- b) The Contractor's actual long-distance telephone, fax, postage and other identifiable communication expenses.

Excluding good and services tax ("GST") or other applicable tax paid or payable by the Contractor on expenses described in (a) and (b) above to the extent that the Contractor is entitled to claim credits (including GST input tax credits), rebates, refunds or remission of the tax from the relevant taxation authorities.

The maximum amount the Province is obliged to pay to the Contract for expenses under this Agreement is \$70,000 for the renewal term April 1, 2022 to March 31, 2023.

(4) In all other respects, the Agreement is confirmed.

SIGNED AND DELIVERED on the _____ day of _____, 2022 on behalf of the Province by its duly authorized representative Signature: _____ Print name: _____ Title: _____	SIGNED AND DELIVERED on the _____ day of _____, 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation) Signature(s): _____ Print name(s): Don Wiebe Title: _____
---	---

Page 280 of 368 to/à Page 321 of 368

Withheld pursuant to/removed as

s.13 ; s.15 ; s.16

CPU/CRRU Amalgamation Proposal

POLICY, FINANCE AND OPERATIONS STEERING COMMITTEE

JESS GUNNARSON

1.1 BACKGROUND:

Prior to 2019, Security Programs Division (SPD) of the Ministry of Public Safety & Solicitor General (PSSG) contracted directly with retired police officers with legacy database permissions and security clearance enabling access to law enforcement databases to collect information from the Canadian Police Information Centre (CPIC) and the Police Records Information Management Environment-BC (PRIME-BC). Though contracted by the Province, the CRRU was identified as an RCMP unit in the 2009 Letter of Agreement (LOA) between the RCMP and PSSG. The purpose of these direct contracts was to search CPIC and PRIME-BC information to help inform SPD's decision makers with respect to SPD's eight regulatory and non-regulatory programs involving approximately 280,000 checks annually. The program areas are as follows:

- *Criminal Records Review Act* (CRRRA) provides the Deputy Registrar the authority to conduct criminal record checks for employees/ volunteers involved in unsupervised employment/ volunteer activities with children and/ or vulnerable adults to determine if an individual was the subject of an outstanding charge or conviction related to a "relevant offence or specified offence";
- *Security Services Act* (2007) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of security worker/ business licensing;¹
- *Body Armour Control Act* (2009) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of registration of body armour;
- *Armoured Vehicle and After-Market Compartment Control Act* (2010) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of registering armoured vehicles;
- *Pill Press Related Equipment Control Act* (2018) provides the Registrar the authority to carry out the following checks: criminal record check (CPIC), police information check (PRIME/PROS) and correction service information check for purpose of registering pill presses;
- *Cannabis Control and Licensing Act- CCLA* (2018) provides the Security Manager the authority to carry out the following checks: criminal record check or fingerprint based criminal record verification by searching CPIC, police information check (PRIME/PROS), law enforcement intelligence databases, the justice information system, and correction service information check for purpose of clearance to work in or operate a business in the non-medical legal cannabis industry;
- Personnel Security Screening for BC public service employees which involves a search for charges/ convictions and, in designated instances, Enhanced Security Screening (ESS) for BC public service employees whose roles require more stringent security screening. For ESS, each client organization enters a separate agreement which may involve CPIC, PRIME/ PROS, and other queries/ checks of law enforcement databases;
- 'Outside the Act' checks, including criminal record checks for the Ministry of Children and Family Development in accordance with the *Child, Family and Community Services Act* (1996) which provides the Director of the CFCSA with the authority to have access to any information that is

¹ Although the Act allows for a police information check (PRIME/PROS) to be conducted in every instance, SPD determines when the CRRU will go beyond a CPIC check and look at these additional law enforcement databases for adjudication purposes.

in the custody or control of a public body that is necessary to enable them to exercise their powers to perform their duties under the Act.

In December 2018, the Provincial Government, on behalf of SPD entered a business case and funded the Criminal Record Review Unit (CRRU) under the RCMP/CFSEU-BC (OCABC positions) to conduct criminal record checks for the above regulatory and non-regulatory programs, with the exception of the CCLA. Access to information on police databases is highly regulated and restricted to law enforcement agencies and, while the contractors had the requisite security clearance and access, the access was not under the direct supervision of the RCMP. An amendment was entered to the business case and signed in April/ May 2019. The CRRU was created as an entity of CFSEU-BC with OCABC positions. This transition enabled direct oversight of the CRRU by the RCMP and also ensured the unit was following proper policy as a "Category 1" policing agency to access the various law enforcement databases. The April/ May 2019 business case amendment allocated annual funding of \$887,187 at 100% to fund the CRRU with the Province's contribution (70%) at \$621,031.

s.15; s.16

For context, the Police Information Check (PIC) Guidelines were developed in collaboration between the RCMP, municipal police forces, PSSG, and PRIME-BC in 2010 and implemented in the spring of 2012. The guidelines were amended in 2014 subsequent to recommendations by BC's privacy commissioner and again in 2016. The guidelines are intended to create consistency in practice between police agencies province-wide who are conducting criminal record checks, including vulnerable sector checks, at the request of individuals for employment/ volunteer purposes. BC PIC guidelines prescribe two types of checks: 1) PIC check which includes a search of CPIC and PRIME for charge/ conviction information, and 2) PIC-VS check for individuals working with the vulnerable sector which includes a search of CPIC and PRIME and can include disclosure of any non-conviction information where the applicant was in a culpable role code within the disclosure period. While other jurisdictions in Canada have placed significant constraint upon the disclosure of non-conviction information in criminal record checks given the potentially prejudicial nature of the information (see Ontario's *Police Criminal Record Check Reform Act* enacted in 2018 and the Alberta Police Information Check Disclosure procedures endorsed in 2019),

BC's PIC guidelines continue to enable disclosure of non-conviction information in multiple circumstances.

s.15; s.16

In April/ May 2019, the Province, on behalf of SPD, entered a separate business case and funded the Cannabis Organized Crime Counter Proliferation Unit (CPU) which was functional commencing in October 2018 to support the Security Manager at SPD with security screening for cannabis businesses, associates, and workers in accordance with the *Cannabis Control & Licensing Act* (CCLA). The April/ May 2019 CPU business case allocated annual funding of \$1,150,268 at 100% to fund CPU with the Province's contribution (70%) at \$805,187. The total sum of annual funding allocated to CRRU and CPU was \$2,037,455 with the Province's contribution (70%) at \$1,426,218.

Concurrent to the above discussions involving the CRRU, non-medical cannabis was legalized in October 2018. CPU supported SPD with searches of law enforcement databases and investigations through 2019 and 2020. In September 2020, the Cannabis Licensing Regulation was amended to remove the Security Manager's (SM) independent statutory decision-making authority and, while the SM maintains a role with information provided by CPU, the General Manager is now the sole statutory decision-maker. With more than two years since legalization, and with few 'not fit and proper' findings, the Province has learned a significant amount regarding the risks in the non-medical legal cannabis market and this business case makes changes to the CPU structure in response to learnings.

2.1 PURPOSE

The purpose of the present business case is twofold:

1. Obtain approval for the amalgamation of CPU and CRRU into a single unit termed the Criminal Record Review Unit. This merger enables greater flexibility and operational efficiencies in maximizing the new CRRU's impact across the key mandates and priorities detailed in the business case below. The financial forecast is attached as Appendix A and reflects the combination of the separate CRRU and CPU funding allocations with no additional funding. In other words, the funding requirements of the new CRRU will not exceed the current combined funding (at 100%) of the CRRU and CPU with a combined annual budget of \$2,037,455;
2. Obtain approval for the realignment of resources within the new combined CRRU to enable the CRRU to conduct the additional effort required to be consistent with the PIC guidelines, including PIC-VS equivalent checks for the CRRU. This involves the maintenance and transition of 3.5 positions from the CPU to the CRRU for support of Cannabis Organized Crime background checks

and monitoring of the legal cannabis industry, including two (2) Junior Intelligence Analysts² and one (1) Information Coordinator, as well as the ½ NCO i/c Sergeant position. Five of CPU's positions will be absorbed by CFSEU-BC/ OCABC as Surplus to Establishment (STE) with two positions deleted as they are vacant (for a net total of 3 STEs). With the financial capacity created by moving the five CPU positions to STE, this proposal requests an increase in CRRU capacity by seven (7) Organized Crime Agency of BC (OCABC) positions, including one (1) Team Coordinator and six (6) Information Officers (please refer to Appendix B for the revised organizational chart).

3.1 CRRU Composition

Prior to the 2009 letter of agreement, the CRRU consisted of seven (7) retired RCMP members and one clerical staff member who were direct-awarded contracts administered by SPD and renewed on an annual basis. Between 2009 and 2019, the unit has expanded to include a total of ten (10) established positions, including one (1) operational position and nine (9) civilian positions.

On February 25, 2019, E Division RCMP received a funding letter from PSSG and the business case was signed between the Province and RCMP E Division, as described above, which transferred supervision and oversight of the CRRU under the umbrella of CFSEU-BC/ RCMP on April 1, 2019. This reform of the CRRU ensured that the unit continued to operate as a centralized service delivery model to support the obligations and requirements of the Registrar under SPD's eight regulatory and non-regulatory programs as authorized by legislation, policy, and consent. At this time, all retired police member contractors were transitioned into full-time civilian employees with OCABC and one OCABC Sergeant was assigned as the operational and administrative oversight of the CRRU.

The following table represents the positions current to January 2021 within the CRRU:

CRRU	Title/Rank	Classification	Position Number	Funding Collator	Location Collator
1	NCO i/c Sergeant	OCA ½ time	OCA-115	E1469	E1469
2	Team Coordinator	Pay Grade 7	OCA-120	E1469	E1469
3	Information Officer	Pay Grade 6	OCA-121	E1469	E1469
4	Information Officer	Pay Grade 6	OCA-122	E1469	E1469
5	Information Officer	Pay Grade 6	OCA-123	E1469	E1469
6	Information Officer	Pay Grade 6	OCA-124	E1469	E1469
7	Information Officer	Pay Grade 6	OCA-125	E1469	E1469
8	Information Officer	Pay Grade 6	OCA-126	E1469	E1469
9	Information Officer	Pay Grade 6	OCA-127	E1469	E1469
10	Information Officer	Pay Grade 6	OCA-128	E1469	E1469

3.2 Internal Review of CRRU:

s.13; s.15; s.16

² One of which must be converted from an Analyst Assistant position to Junior Criminal Intelligence Analyst

3.3 Proposed CRRU Model and Required Resources:

In discussions between PSSG, the RCMP and, legal counsel with the Department of Justice, the RCMP communicated that the CRRU falls under the administrative and operational umbrella of the RCMP which is governed by federal legislation. Although legislation exists at the provincial level, the RCMP views its authority for background checks as stemming from signed consent forms in accordance with the *Privacy Act*. Despite confines placed by the provincial CRRA, the RCMP has identified that authority by way of consent prevails and the access/ disclosure of non-conviction information will best insulate the RCMP from the perspective of perceived financial and reputational liability and mitigate risks the RCMP have stated surrounding public safety.

In order to ensure consistency with police departments/detachments and conduct vulnerable sector background checks that comply with the PIC guidelines, the RCMP has required that the CRRU expand criminal record checks under the CRRA through the utilization of additional law enforcement databases (PRIME/PROS), thus aligning with the existing PIC guidelines. All applicants who are identified as having been in a culpable role for a non-conviction matter associated to a CRRA Schedule I or III offence will be assessed by CRRU. A Service Level Agreement will be instituted to identify the extent of CRRU analysis and the degree and circumstances under which non-conviction information is disclosed to SPD.

In order for the CRRU to conduct BC PIC-VS on all CRRA-related applications, additional Information Officers are required. In 2019, the CRRU conducted 248,311 CRRA related background checks, which averages to a total of 985 checks conducted per/day. The CRRU's internal assessment indicates that each Information Officer is capable of conducting approximately 120 BC-PIC background checks per/shift. Applying this rate to the 985 background checks conducted per day and recognizing that CRRU is currently conducting PRIME checks in some circumstances, the CRRU will be allocated a net addition of six (6) Information Officers and one (1) team lead. It must also be remembered that in addition to the CRRA checks, the CRRU also supports SPD with numerous other regulatory and non-regulatory background checks and the RCMP's requirement to conform to the PIC Guidelines is likely to create additional workload for CRRU.

3.4 Cannabis Organized Crime Counter Proliferation Unit (CPU)

On October 17, 2018 the *Cannabis Act* was enacted. Under this federal legislation, adults are allowed access and possession of regulated, quality controlled, legal non-medical cannabis. Under this Act, the provinces and territories are responsible for overseeing and licensing the distribution and sale of cannabis products, subject to federal conditions.

A key priority in the legalization of cannabis is ensuring public safety and preventing an organized crime presence in the legalized cannabis market. The CPU was created in 2018 to support SPD and the Security Manager under the *Cannabis Control and Licensing Act* (CCLA) with conducting background checks of all retail applicants and workers in BC's non-medical cannabis industry with a goal of identifying applicants and associates with a nexus to organized crime. The CPU is a fenced unit within CFSEU-BC, independent and separate from other enforcement teams with business rules established to ensure alignment with provincial priorities and privacy laws.

At full strength, the unit is funded for a total of 8.5 positions (OCABC and RCMP). The CPU consists of 0.5 OCABC Sergeant (shared with CRRU), 1 RCMP Corporal and 1 RCMP Criminal Intelligence Analyst (Vacant), and 6 OCABC civilian employees including the following: 2 Open Source Analysts, 1 Junior Criminal Intelligence Analyst (Vacant), 1 Analyst Assistant, 1 Information Coordinator and 1 Investigative Assistant.

A tremendous amount has been learned from the inception of the CPU in 2018 and the unit has transitioned in accordance with the provincial requests over the past two years. In August 2020, the CPU commenced working with PSB to revise the screening process related to cannabis to garner greater effectiveness and efficiencies. This has resulted in a proposal to combine the resources from the CPU with the CRRU and to streamline the overall background check process as it relates to Cannabis. These enhancements and efficiencies will be implemented as aspect of this amalgamation.

s.15

After numerous discussions, the CPU resources transitioning into CRRU are all OCABC civilian employees including 1 Information Coordinator, 2 Junior Criminal Intelligence Analyst and the ½ NCO i/c Sergeant position. It should be noted that approval is required from the Province to change the existing Analyst Assistant to a Junior Criminal Intelligence Analyst for this merger.

The following table represents the established positions within the CPU as of January 2021:

CPU	Title/Rank	Classification	Position Number	Funding Collator	Location Collator	Amalgamated? Yes/No
1	NCO i/c Sergeant	OCA ½ time	OCA-115	E1463	E1463	Yes
2	2 i/c Corporal	RCMP (RM)	55376	E1463	E1463	No
3	Jr Crim Intel Analyst	Pay Grade 7	OCA-116	E1463	E1463	Yes
4	Analyst Assistant ¹	Pay Grade 3	OCA-117	E1463	E1463	Yes
5	Information Coordinator	Pay Grade 4	OCA-119	E1463	E1463	Yes
6	Sr Crim Intel Analyst ²	RCMP (CM)	55380	E1463	E1463	No
7	Investigative Assistant ²	Pay Grade 2	OCA-118	E1463	E1463	No
8	Open Source Analyst	Pay Grade 6	OCA-92	E1463	E1463	No
9	Open Source Analyst	Pay Grade 6	OCA-93	E1463	E1463	No

¹ The OCA-117 position is currently an Analyst Assistant, Pay Grade 3, and requires reclassification to a Junior Criminal Intelligence analyst, Pay Grade 7, in order to conduct the necessary duties and have access to sensitive law enforcement databases.

² Positions currently vacant

As per the above, CFSEU-BC/OCABC will have to absorb three (3) positions Surplus to Establishment (STE). The total estimated financial impact of this absorption is \$389,436, as detailed in the table below and Appendix C:

Title/Rank	Salary & Benefits	Other Divisional and O&M Costs	Total Cost
RCMP Corporal	\$150,067	\$18,972	\$169,039
OCABC Open Source Analyst	\$102,299	\$7,900	\$110,199
OCABC Open Source Analyst	\$102,299	\$7,900	\$110,199
TOTAL	\$389,436		

With the overall size of CFSEU-BC there is a fair amount of internal movement with resources either transferring, retiring or finding alternate employment outside of the agency. The table below details the timeline for the three STEs to be absorbed into CFSEU-BC/OCABC. The 2 vacant positions will be deleted once this business case is approved; and the 3 STE positions will be deleted upon each incumbent's transfer into an equivalent position, as outlined below and as soon as is practicable and in accordance with the RCMP's internal processes.

CPU	Title/Rank	CPU Position Number	Current Collator	Pending Position Number	New Collator	Timeline
1	RCMP Corporal	55376	E1463	48719	E1150	April 1, 2021 to acting Sgt. position on PVGO (PTEP)
2	OCA Open Source Analyst – Pay Grade 6	OCA-92	E1463	OCA-143	GGVAF	Current OS Analyst on the Firearms Team will be departing CFSEU in the next 12 months and

						will be replaced by the CPU OS Analyst
3	OCA Open Source Analyst – Pay Grade 6	OCA-93	E1463	TBD	E1478	Business Case for OS Analyst on the Witness Security Program and once approved (12 months) this CPU OS Analyst will occupy the position.
4	Sr Crim Intel Analyst	55380	E1463	To be deleted		
5	Investigative Assistant	OCA-118	E1463	To be deleted		

A STE position would be created for the RM, which would not affect Annex A and would not be attached to a collator. For the Open Source Analysts, the STE boxes would be attached to the Open Source collator which would be added financial pressure to the Open Source collator. As the corporal position would be vacant starting April 1, 2021, there would be no additional financial pressure resulting from the RM position.

4.1. AMALGAMATION OF THE CRRU AND CPU:

In consultation with senior leaders from PSSG, combining some of the resources from CPU with the larger CRRU will garner greater efficiencies. The attached organizational chart (Appendix B) outlines the new positions and the structure of the combined unit once approved.

The proposal increases the CRRU by 7 OCABC positions which includes 1 additional Team Coordinator and 6 Information Officers. In addition, 2 Junior Intelligence Analysts and 1 Information Coordinator positions would transition from the CPU (including the ½ NCO i/c/ Sergeant position) to the CRRU for additional support of the Cannabis OC background checks and monitoring of the legal non-medical cannabis market. It is critical to note that the aforementioned CPU positions will continue to focus on cannabis-related background checks but will be situated within the larger CRRU team to enhance efficiencies and create greater flexibility in task assignment. Funding for the CPU was provided by Treasury Board for the purpose of protecting the cannabis industry against illegal activity and organized crime involvement. The functions and duties of the existing CPU positions within the broader CRRU will continue to be fulfilled in accordance with the mandate and responsibilities outlined in CPU's business case and delegation letters from the Province.

This includes:

- To address the risk of organized crime infiltration in non-medicinal cannabis distribution, specifically to support screening strategies during the retail licensing process and for employees working with non-medical cannabis in the market;
- To provide the necessary background and information checks to ascertain ties, association, or a nexus to organized crime for cannabis retail applicants/associates, and workers as required;
- Checks include:
 - a criminal record check or fingerprint-based criminal record verification through CPIC;
 - a police information check;
 - a check of intelligence databases maintained by law enforcement agencies;

- a check of records in the justice information system of the Ministry of the Attorney General;
- a check of records in the corrections information system of PSSG.
- To develop and maintain an information system for the legal and illegal cannabis market, including a file management system for CPU checks and processes in alignment with required reporting and evaluation metrics;
- Submit any files that require additional investigation regarding a potential nexus to organized crime to SPD, in order for SPD's investigators to conduct a follow-up investigation into the matter;
- To provide timely and evidence-based reports for license applicants and workers to SPD;
- Establish a system of evidence management and evidence presentation commensurate for required judicial proceedings as required and prepare/provide all required materials for any judicial matters that arise from the licensing or employee application screening process.

s.15; s.16

The following table depicts the future state of the amalgamated unit:

CRRU AMALGAMATED	Position Number	Classification	Funding Collator	Location Collator
1	OCA-115	OCA	E1469	E1469
2	OCA-120	Pay Grade 7	E1469	E1469
3	OCA-TBD *	Pay Grade 7	E1469	E1469
4	OCA-121	Pay Grade 6	E1469	E1469
5	OCA-122	Pay Grade 6	E1469	E1469
6	OCA-123	Pay Grade 6	E1469	E1469
7	OCA-124	Pay Grade 6	E1469	E1469
8	OCA-125	Pay Grade 6	E1469	E1469
9	OCA-126	Pay Grade 6	E1469	E1469
10	OCA-127	Pay Grade 6	E1469	E1469
11	OCA-128	Pay Grade 6	E1469	E1469
12	OCA-TBD *	Pay Grade 6	E1469	E1469
13	OCA-TBD *	Pay Grade 6	E1469	E1469
14	OCA-TBD *	Pay Grade 6	E1469	E1469
15	OCA-TBD *	Pay Grade 6	E1469	E1469
16	OCA-TBD *	Pay Grade 6	E1469	E1469
17	OCA-TBD *	Pay Grade 6	E1469	E1469
18	OCA-116	Pay Grade 7	E1469	E1469
19	OCA-117	Pay Grade 7	E1469	E1469
20	OCA-119	Pay Grade 4	E1469	E1469

** It is anticipated that these additional OCABC positions will be added to the newly enhanced CRRU.*

The unit will remain fenced and an independent unit within the CFSEU-BC's Support Services and all operational and administrative aspects of this unit will be managed within the structure of CFSEU-BC.

4.2 Funding

It is understood the funding for this proposal must come from within the CFSEU-BC and with combining the two units there will be sufficient funding for this proposal.

The annual cost estimate (Appendix A) for the amalgamated CRRU including salaries, benefits and O&M totals \$2,037,455. This reflects the existing total allocation for the CRRU and CPU independently, without addition of any further funding allocation.

There are several key risks that must be considered with respect to the proposed business case:

1. The absorption of the three (3) STEs poses both short- and long-term financial risks for CFSEU-BC. It will be critical that CFSEU-BC appropriately forecasts and manages these financial impacts to ensure a balanced budget.
2. The current proposal is dependent on the continued availability of funding for the CPU by Treasury Board. If funding is reduced or ended in future years, the continuity of the proposed changes to the CRRU will be impacted.
3. While the conduct of checks in accordance with the PIC guidelines and, specifically, PIC-VS checks for all CRRA checks addresses the liability and public safety concerns of the RCMP, it is not in line with the terms outlined in the CRRA which raises risks of substantial complaint, civil recourse, and financial/ reputational liability for the Province. SPD will work to manage the risk, including through development of a Service Level Agreement/ Information Sharing Agreement with the RCMP, and ensure there is a process that limits the disclosure of non-conviction information.
4. The implementation of the PIC Guidelines for SPD's regulatory and non-regulatory programs creates a risk of unidentified resourcing pressures for SPD which, unless managed through provisions in the Service Level Agreement, will impede the success of this business case.

4.3 Space Allocation

The enhanced CRRU for the most part will continue to work remotely on a permanent basis and there will be no requirement for additional office space at the Island District Headquarters in Victoria. The two Junior Criminal Intelligence Analysts and one Information Coordinator will work from the CFSEU-BC office at RCMP Headquarters in Surrey.

5.1 IMPLEMENTATION:

It is expected that the amalgamated CRRU will become operational in 2021/22, upon endorsement of the Service Level Agreement, and that the HR process will begin immediately upon approval of this business case, in order to mitigate impact and backlog. Ideally, the new employees would be hired by the first quarter of FY2021/2022.

5.2 Performance Evaluation Framework

As with all public safety initiatives, it is critical that the amalgamated CRRU is guided by a comprehensive performance evaluation framework. It is critical that this framework not only captures the activities and service demands over time, but also the downstream impacts of the unit's work on the organized crime landscape and communities at large. In support of this key priority, SPD is working in consultation with Ministry partners to develop a comprehensive list of performance metrics, which link to the key

priorities and objectives of the unit.

To evaluate and measure the success of each initiative, several levels of analysis are employed. Descriptive analyses of all metrics are conducted to provide an overview of the activities, outputs, and outcomes of each initiative. Additional context is provided to situate these metrics within the broader context of the unit's operational environment. Comparative analyses of the unit's outputs and outcomes across reporting periods are completed to show changes to unit performance over time, as well as the cumulative impact of the initiative to-date.

All findings and analyses will be included in a performance metrics report that will be completed on a biannual basis. The report will be shared with Executive at PSSG and CFSEU-BC, including the CFSEU-BC/OCABC Board of Governance. Briefings will be held both internally and externally to ensure that all stakeholders have a chance to voice their opinions on the report findings and discuss potential implications for next performance cycle. This iterative process ensures that both PSSG and CFSEU-BC have a mutual understanding of the success of each initiative and ensure that initiatives continue to meet key mandates and priorities.

5.3 Service Level Agreement

s.15; s.16

Appendix 3: *British Columbia Guideline for Police Information Checks*

The *British Columbia Guideline for Police Information Checks* (PIC Guidelines) (2016) is 'intended to assist police agencies to understand and apply relevant legislation, policies, and directives to the processing of Police Information Checks' (2016, 1). The PIC Guidelines will guide the Criminal Records Review Unit (CRRU) in conducting checks of police information databases for Security Programs Division (SPD).

The PIC Guidelines can be found at the following URL:

https://www2.gov.bc.ca/assets/gov/law-crime-and-justice/criminal-justice/police/publications/police-information-checks/police_infochecks_guidelines_dec16.pdf

This URL is current as of June 2021.

Page 335 of 368 to/à Page 342 of 368

Withheld pursuant to/removed as

s.13

Information Incident Management Policy	
Office of the Chief Information Officer Ministry of Citizens' Services	Draft/Version #1.0 October 18, 2019

TABLE OF CONTENTS

INTRODUCTION	1
Overview	1
Purpose	2
Application	2
Authority	2
Legal	2
Advice on this Policy	2
POLICY REQUIREMENTS	3
1. General Requirements	3
2. Reporting.....	3
3. Preliminary Assessment	4
4. Containment and Recovery.....	4
5. Information Access Suspensions and Restrictions	4
6. Privacy Breach Harm Assessment and Notification	5
7. Investigations	6
8. Prevention	7
9. Documentation	7
10. Roles & Responsibilities	8
DEFINITIONS.....	10
REVISION HISTORY	10

INTRODUCTION

Overview

The Province of British Columbia is the steward of a significant amount of confidential information, including the personal information of British Columbians. Government must protect citizens' personal information in accordance with the requirements set out in the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and ensure that if an information incident occurs, it is managed in an appropriate manner. The Information Incident Management Policy is the Province's corporate policy for responding to and mitigating risks arising from actual or suspected information incidents, including privacy breaches.

The Information Management Investigations Unit (IMIU) within the Office of the Chief Information Officer's (OCIO) Corporate Information and Records Management Office provides ministries with expert advice, support and investigative services to assist them in navigating the information incident process. The IMIU partners with the OCIO's Security Investigations and Forensics Unit (SIFU) when suspected information incidents involve government information technology (IT) systems.

An **information incident** is a single or a series of events involving the collection, storage, access, use, disclosure, or disposal of government information that threaten privacy or information security and/or contravene law or policy.

A **privacy breach** is the theft or loss, or the access, collection, use or disclosure of personal information that is not authorized by Part 3 of FOIPPA. A privacy breach is a type of information incident.

Purpose

The purpose of this policy is to:

- Establish a comprehensive framework for managing information incidents.
- Provide clear direction and set out policy requirements.
- Clarify associated roles and responsibilities.

Application

This policy applies to all ministries, agencies, boards, and commissions subject to the Core Policy and Procedures Manual (referred to as ministries hereafter).

Authority

Core Policy and Procedures Manual Chapter 12

Legal

The Information Incident Management Policy does not replace or limit a ministry's legal obligations under the *Information Management Act* (IMA) or FOIPPA.

Advice on this Policy

For questions or comments regarding this policy, please contact:

Information Management Investigations Unit
Corporate Information and Records Management Office
Office of the Chief Information Officer
Ministry of Citizens' Services
Telephone: 250-356-0361

POLICY REQUIREMENTS

1. General Requirements

- 1.1 Supervisors must ensure that employees are made aware of their responsibilities under this policy:
 - a) At the commencement of their employment.
 - b) When a new or updated version of this policy is issued.
 - c) Annually for employees that have access to a significant amount of confidential information.
- 1.2 The IMIU must, in consultation with appropriate parties such as SIFU, review this policy regularly, update it as appropriate, and communicate any changes to ministries.
- 1.3 Ministries may establish ministry-specific policies and procedures, where necessary, to support this policy. All ministry-specific policies relating to information incident management must be submitted to the IMIU for review.
- 1.4 Ministries must assign a Ministry Incident Lead for each actual or suspected information incident. Please refer the Ministry Incident Lead Guideline¹ for information regarding the assignment of the Ministry Incident Lead.

2. Reporting

- 2.1 Employees must *immediately* report any actual or suspected information incidents to both
 - a) their supervisor; and
 - b) the IMIU by calling 250-387-7000 or toll-free 1-866-660-0811.

The requirement to report immediately includes actual or suspected information incidents discovered outside of normal working hours.

- 2.2 Employees must also report actual or suspected information incidents *within 24 hours* to the Risk Management Branch and Government Security Office by completing a General Incident or Loss Reporting Form,² in accordance with Procedure L³ of the Core Policy and Procedures Manual.
- 2.3 The IMIU must maintain and monitor a means for ministries to report information incidents 24 hours per day, 365 days per year.
- 2.4 Where the incident is ongoing and related to government IT resources, the OCIO Security Incident Response Process⁴ must be followed.

¹ Available at www.gov.bc.ca/privacy_breaches

² Available at gilr.gov.bc.ca

³ Refer to <https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/procedures/loss-reporting>

⁴ Available at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/cyber-security-incident-response-process>

- 2.5 Where the IMIU determines that an incident is outside of its mandate and/or jurisdiction, and where the IMIU determines that the incident is within the mandate and/or jurisdiction of another investigative unit, the IMIU must provide notice of the incident to that investigative unit.

3. Preliminary Assessment

- 3.1 The IMIU must conduct a preliminary assessment of reported information incidents that includes, but is not limited to, the following:
- a) Whether the incident falls within the IMIU's mandate.
 - b) Whether the incident is within the IMIU's jurisdiction.
 - c) The type of information involved, including whether personal information is involved.
 - d) The potential severity of the incident.
 - e) The likelihood that an actual information incident has occurred.
- 3.2 The IMIU may provide notice of information incidents to the Ministry Chief Information Officer of the responsible ministry.
- 3.3 The IMIU may provide notice, in accordance with the Joint Investigations Protocol⁵, of information incidents to other investigative units within government.

4. Containment and Recovery

- 4.1 In the event of an information incident, ministries must take appropriate steps to contain the incident and, wherever possible, recover any information that has been lost or otherwise exposed.

These steps will vary depending on the nature of the incident, but could include:

- a) Isolating or suspending the activity that led to the incident.
- b) Correcting weaknesses in physical or technical security.
- c) Recovering or seeking the disposal of any information or IT equipment that was lost, stolen, or otherwise exposed.
- d) Determining if any copies of confidential information were made or shared with third parties and attempting to recover them where possible.
- e) Requesting that individuals involved provide written attestations confirming that they have returned and/or destroyed any records they received without authorization, and whether they sent them to others and, if so, to whom.

5. Information Access Suspensions and Restrictions

- 5.1 Ministries may temporarily suspend or restrict access to information to contain an information incident at any time. Before suspending or restricting access to information, ministries must take the following into consideration:
- a) Whether there is reason to conclude that the actual or suspected information incident may potentially cause moderate or serious risk of harm to a member of the public, the ministry, an employee, a service provider, or any other person/entity.
 - b) Whether there is reason to believe that the person acted with malice or ill intent, intentionally and knowingly initiating or facilitating a privacy breach.

⁵ Available at https://www2.gov.bc.ca/assets/gov/careers/managers-supervisors/managing-employee-labour-relations/investigation_protocol.pdf

- c) Whether suspension of access will prevent further harm.
 - d) Whether there is reason to believe that not suspending or restricting the person's access will result in further breach activity and potential harm to individuals.
 - e) The impact of the suspension on the person whose access is being suspended and other parties.
 - f) Whether there is reliable, credible and relevant evidence available on which to base a decision regarding the suspension or restriction of access to information. Information access suspensions/restrictions should not be based purely on conjecture that an information incident has occurred.
 - g) The business context for which the information was being used and the information access arrangements for the person concerned.
 - h) Mitigation strategies that reduce the impact to the person whose access is being suspended including, restricting the person's access, creating a new account or provisional suspension until further evidence is identified.
- 5.2 The decision to suspend or restrict access to information must be documented in writing and be made by the Ministry Incident Lead, unless this responsibility has been otherwise assigned within a ministry.
- 5.3 The decision to temporarily suspend or restrict access should be periodically reviewed to ensure that the suspension is still justified. If it is found that the basis for the suspension is no longer valid, access to information must be reinstated immediately.
- 5.4 If information access is temporarily suspended or restricted, ministries must notify the individual subject to the suspension/restriction. Notification must include:
- a) The reason why access has been suspended or restricted.
 - b) The length of time that access is expected to be suspended or restricted.
 - c) Who to contact for further information.
- 5.5 At the conclusion of the investigation, the ministry must notify the person if the final decision is to suspend or restrict access to information permanently and provide an opportunity for the person to respond. The ministry must provide the person with:
- a) a written summary of the reasons and evidentiary basis for the decision; and
 - b) a reasonable opportunity to respond in writing or in-person.

6. Privacy Breach Harm Assessment and Notification

- 6.1 In consultation with the IMIU, ministries must ensure that a harm assessment is completed for all privacy breaches in order to determine the risk of harm to affected individuals as a result of the incident.

Harm assessments must consider informational and situational risk factors, in addition to the circumstances of the incident. This includes, but is not limited to:

- a) Which and how many individuals are impacted.
- b) The sensitivity, context, and volume of the personal information involved.
- c) The ability to quickly contain the incident and the potential likelihood of further dissemination of the information involved.

- d) The relationship between the party in receipt of personal information and the person the information is about.
 - e) Whether any affected individuals could face a risk of:
 - i. identity theft or identity fraud;
 - ii. physical harm;
 - iii. financial, business, or employment loss;
 - iv. hurt, humiliation or damage to reputation; and/or
 - v. loss of trust.
 - f) Whether legal or contractual obligations require notification.
- 6.2 In determining the risk of harm to an impacted individual, the weight applied to each factor should be determined according to the circumstances of the incident.
- 6.3 Notifications must be based on a balance of a harms assessment. Under this principle, the risk of harm to an impacted individual as a result of the breach must be weighed against the risk that notification would cause further harm to an individual. Ministries should notify the impacted individual(s) if the risk of harm, as a result of the breach, outweighs the risk of further harm to an individual, if notification occurs.
- 6.4 Notifications should occur without unreasonable delay, be direct wherever possible, and should include the following information:
- a) The date of the privacy breach.
 - b) A description of the privacy breach.
 - c) The personal information involved.
 - d) The risk to the individual and the steps taken to mitigate the potential for harm.
 - e) Steps the individual can take to further mitigate any potential harm they face.
 - f) Measures that have been, or will be, taken to prevent similar incidents from occurring in the future.
 - g) The contact information of an individual within the responsible ministry who can answer questions or provide further information.
 - h) The right of complaint to the Office of the Information and Privacy Commissioner (OIPC) or notice that the OIPC is aware of the breach and contact information for the OIPC.

7. Investigations

- 7.1 Ministries may initiate an investigation to determine the nature, extent, and/or cause of an information incident.
- 7.2 Ministries may request the support of the IMIU in conducting investigations into information incidents. If a ministry requests the IMIU's support, the IMIU takes on responsibility for 7.4 below.
- 7.3 Ministries must ensure that information incident investigations are conducted in accordance with principles of administrative fairness. This includes, but is not limited to:
- a) The terms of reference established in writing, including purpose and scope.
 - b) Objective, documented standards are used to measure the event or issue being investigated.
 - c) Investigations are conducted with an open mind and consider all reasonably available evidence.

- d) Individuals with allegations made against them are given an appropriate opportunity to respond to the allegations and provided with notice of the allegations in advance of any interview.
 - e) Individuals are treated with respect throughout the interview process.
 - f) Findings are based on a reasonable assessment of the available evidence.
- 7.4 Ministries must ensure that information incident investigators are sufficiently trained in:
- a) The subject-matter of information incident investigations.
 - b) How to gather, review, assess, document, and weigh evidence.
 - c) How to conduct an investigative interview.
 - d) Administrative fairness.
 - e) When and how to report potential crimes and/or share information with law enforcement agencies.

8. Prevention

- 8.1 Ministries must have appropriate measures in place to prevent information incidents from occurring. These measures will vary depending on the ministry and the type of information they hold, but may include the following:
- a) Regular training and awareness activities for employees.
 - b) Adequate policies, procedures, and/or guidelines for staff to follow.
 - c) Tools and resources to assist staff in performing their duties without risking an information incident.
 - d) Appropriate physical and technical security controls and processes to ensure confidential information is protected against such risks as unauthorized access, use, disclosure, or disposal.
- 8.2 In response to an information incident, ministries must, in consultation with appropriate parties such as the IMIU and SIFU, assess, implement and document preventative measures to mitigate the risk of a similar incident occurring.
- 8.3 The IMIU may request that ministries provide documentation of the preventative measures implemented to mitigate the risk of a similar incident happening.

9. Documentation

- 9.1. Evidence of the information incident must be preserved, and the circumstances of the information incident must be documented, including:
- a) The IMIU file number.
 - b) The OIPC file number (where applicable).
 - c) What happened and when.
 - d) How and when the incident was discovered.
 - e) Any personal information involved and the scope of any privacy breach.
 - f) Steps taken to contain the incident and their effectiveness.
 - g) The number and type of impacted individuals and the assessment of harm.
 - h) Any decision to notify the impacted individual(s) and the steps taken to notify (in the case of a privacy breach).

- i) The decision and the circumstances around any suspension/restriction of access to information.
- j) Prevention measures undertaken in response to the incident.
- k) Any IMIU recommendations (if applicable).

10. Roles & Responsibilities

Information Management Investigations Unit (IMIU)

The IMIU of the OCIO's Corporate Information and Records Management Office has the responsibility to:

- coordinate, investigate, and/or resolve actual or suspected information incidents, including privacy breaches;
- provide expert advice, recommendations and investigative services throughout incident response and investigative processes, including on the containment and recovery of information, the suspension of access to information, harm assessment and privacy breach notification, and preventative measures;
- act as government's liaison with the OIPC with regard to information incidents, including privacy breaches;
- maintain and monitor a means for ministries to report information incidents;
- provide notice of incidents to Ministry Chief Information Officers (MCIOs), the SIFU, program areas, and other stakeholders, as appropriate;
- ensure its investigation procedures and practices are administratively fair;
- provide sufficient training to its investigators;
- track and retain information about government's response to an information incident; and
- report on information incidents on behalf of government.

Deputy Ministers (or equivalent positions)

Deputy Ministers (or equivalent positions) have the responsibility to ensure that:

- ministry-specific policies to support this policy are developed as appropriate;
- information incident investigations are conducted in accordance with administrative fairness;
- information incident investigations are conducted by investigators with sufficient training and expertise;
- adequate resources are assigned to support information incident investigations;
- a process is in place to receive notifications of privacy breaches as per section 30.5 of FOIPPA;
- an appropriate Ministry Incident Lead has been identified; and
- preventative measures are developed, where appropriate, to prevent the recurrence of information incidents.

Ministry Chief Information Officers

Ministry Chief Information Officers have the responsibility to:

- lead the development of ministry-specific policies as appropriate;
- identify parties within the ministry who should be notified of information incidents;
- collect and retain summary information about information incidents for the ministry;

- act as a liaison and point of contact for issues within the ministry that may arise during an information incident investigation;
- liaise between investigative teams and other stakeholders within the ministry, as needed;
- ensure that information incidents are reported to ministry executives with responsibility for information management, including the head of the public body for the purposes of FOIPPA; and
- facilitate the implementation of preventative measures.

Ministry Incident Leads

Ministry Incident Leads have the responsibility to:

- act as the primary decision-maker for incident response and investigative processes, including approving preliminary assessments, Terms of Reference/Workplans, and decisions to conduct investigative interviews;
- where necessary, and in consultation with the IMIU wherever possible, direct employees and supervisors to take immediate action to contain an incident and recover any information exposed;
- consult and coordinate with the IMIU throughout the incident response and investigation processes, including assigning appropriate resources to facilitate an effective response and ensuring the IMIU is provided with sufficient information to formulate appropriate recommendations in a timely manner;
- approve notifications of privacy breaches to impacted individuals, including withholding notification on the basis of a balance of harms test;
- make decisions to suspend or restrict access to information, unless these decisions have been assigned to another party by the ministry;
- receive and accept the IMIU's investigative reporting materials; and
- ensure that the ministry's response to an information incident is adequately documented.

Employees

Employees have the responsibility to:

- be aware of their responsibilities under this policy;
- report any actual or suspected information incident in accordance with this policy; and
- take appropriate steps to contain an incident and recover any information as directed by the IMIU and/or the Ministry Incident Lead, as appropriate.

Service Providers

Service Providers have the responsibility to:

- report suspected information incidents in accordance with the terms of their contracts or service agreements; and
- be aware that, if their contracts or service agreements do not include privacy protection or security schedules that address information incidents, service providers are considered employees under this policy.

Supervisors

Supervisors have responsibility to:

- ensure employees are made aware of their responsibilities under this policy as per 1.1 of this policy;
- ensure that all actual or suspected information incidents reported to them are also reported to the IMIU in accordance with this policy; and
- take appropriate steps to contain an incident and recover any information exposed, as directed by the IMIU and/or the Ministry Incident Lead, as appropriate.

DEFINITIONS

Confidential information: a category of **Government Information** (as defined under the *Information Management Act*) with confidentiality requirements. Confidential information includes, but is not limited to:

- Cabinet confidences (for example, a briefing note to Cabinet).
- Government economic or financial information (for example, information about a proposed administrative plan that has not yet been implemented or made public).
- Information harmful to intergovernmental relations (for example, information received in confidence from another government).
- Third-party business information, where its disclosure could harm the third party.
- Personal Information.
- Legal advice or law enforcement information.

Employee: an individual working for, or on behalf of, a ministry, agency, board or commission subject to the Core Policy and Procedures Manual.

Personal Information: recorded information about an identifiable individual other than (business) contact information.

Service Provider: a person retained under a contract or service agreement to perform services for a ministry, agency, board or commission subject to the Core Policy and Procedures Manual.

Supervisor: a person to whom an **Employee** directly reports or a person who manages a **Service Provider** contract or service agreement.

REVISION HISTORY

Version	Date	Notes
1.0	October 18, 2019	CRO/GCIO-approved version posted online



Royal Canadian Mounted Police
Gendarmerie royale du Canada

Canada

[National Home](#) > [Technical Operations](#) > [Departmental Security](#) > Security incident reporting

Security incident reporting

Security incident reporting supports the delivery of services to Canadians and government operations by actively managing:

- management of threats
- vulnerabilities
- incidents

Effective management of security incidents is a fundamental component of security management to assess the:

- consequences of an incident
- risks posed by these incidents
- effectiveness of current practices

What is a security incident?

A security incident can be defined as any type of event/action, voluntary or not, caused by an individual(s) that could potentially harm:

- RCMP employees
- services
- information
- assets
- national interest

Below are the four types of security incidents, and how to report them:

Type of Security Incident	Description	How to Report
Security Breach	<ul style="list-style-type: none"> • Disclosure, theft or unauthorized access to classified/protected assets/information. • Loss of RCMP property (Radio, Blackberry, Smartcard, USB keys, 	<ul style="list-style-type: none"> • Complete Form 2159 • Email your regional security incident mailbox and copy National Coordination • If item has been recovered, email regional security incident

Type of Security Incident	Description	How to Report
	badges, I/D, keys, Building Access Card).	
Security Violation	Any act that contravenes: <ul style="list-style-type: none"> • security directives • unescorted visitors • failure to secure doors/windows or lock security containers • removal of classified/protected assets from a building • failure to safeguard assets 	<ul style="list-style-type: none"> • Complete Form 2159 • Email your regional security incident mailbox and copy National Coordination
Threat or Act of Violence	Threats or acts of violence against (letters, calls, receipt of potentially dangerous substances, stalking, assault,) RCMP employees or property (buildings, vehicles and radio towers).	<ul style="list-style-type: none"> • Complete Form 2159 • Email your regional security incident mailbox and copy National Coordination • Mark as URGENT
Malicious Code Attack	Computer program that performs illicit functions (viruses, Trojan horses, worms and system mis-configuration).	<ul style="list-style-type: none"> • Report to Central Help Desk (1-800-461-7797) • Complete Form 2159 • Email your regional security incident mailbox and copy National Coordination

What to expect once reported?

- You may be contacted by security personnel for additional information on the incident.
- This is not an emergency response process. For situations requiring urgent assistance please follow your local property security protocols.
- Please note that the [Security Incident Report \(2159\)](#) must not include personal information or protected/classified information.
- More information can also be found on the [RCMP Security Guide](#).

Contact Information

For additional information on security incidents, consult with your respective Security Incident unit.

National Coordination

SECURITY_INCIDENT@rcmp-grc.gc.ca

Divisions B, H, J, L

SECURITYINCIDENT_ATLANTIC@rcmp-grc.gc.ca

Divisions A, C, O

SECURITYINCIDENT_CENTRAL@rcmp-grc.gc.ca

Divisions D, F, G, K, V

SECURITYINCIDENT_NORTHWEST@rcmp-grc.gc.ca

Divisions E, M

SECURITYINCIDENT_PACIFIC@rcmp-grc.gc.ca

Date Modified: 2019-03-25

Page 356 of 368 to/à Page 357 of 368

Withheld pursuant to/removed as

s.13

Page 358 of 368 to/à Page 368 of 368

Withheld pursuant to/removed as

s.13 ; s.15