Royal Canadian Mounted Police Gendarmerie royale du Canada

Protected "B"

PRIVACY IMPACT ASSESSMENT

AUTOMATIC LICENSE PLATE RECOGNITION (ALPR)

Prepared By:
Robert J. Howe, (Sgt. Retired)
HRH Howe-L'Africain Consulting

Royal Canadian Mounted Police
Gendarmerie royale du Canada

Document Change Control Table

Version Number	Date of Issue	Author(s)	Brief Description of Change(s)
0.1	December 20th, 2007	R.J. Howe	Initial Draft
0.3	January 15th, 2008	R.J. Howe	Draft
0.4	January 25th, 2008	R.J. Howe	Draft
0.5	February 22nd, 2008	R.J. Howe	Draft
1.0	February 25th, 2008	R.J Howe	Final
1.1	February 27th, 2008	R.J. Howe	Final Revision
1.2	August 24th, 2009	Supt Norm Gaumont	Final Revision
1.3	September 8, 2009	Supt Norm Gaumont	Final Revision
1.4	October 17, 2009	Supt Norm Gaumont	Final Revision

Royal Canadian Mounted Police Gendarmerie royale du Canada

[redacted]

CAVEAT

This document contains "designated information" and "designated assets" that are the property of the RCMP and must be afforded protection in accordance with the information protection standards as detailed in the Government of Canada Security Policy for information designated as Protected "B".

Executive Summary

The Automatic License Plate Recognition (ALPR) program was initiated by the RCMP in concert with the Government of British Columbia Ministry of Solicitor General Police Services Division. This project represents a multi-agency endeavor and includes Major Crime / Integrated Municipal Provincial Auto Crime Team (IMPACT) and RCMP "E" Division Traffic Services.

The ALPR goal is to reduce auto theft and motor vehicle violations in particular those related to prohibited, suspended, unlicensed and uninsured drivers. The ALPR program also assists in the recovery of stolen vehicles, property and related vehicle criminality. Major Crime/IMPACT determined that the majority of auto thefts in the Province of British Columbia are related to the commission of other criminal offences. The data collected on the ALPR pilot project revealed the ALPR system is even more beneficial in identifying individuals driving while prohibited, suspended, unlicensed or uninsured under the Provincial Motor vehicle Act or the Criminal code. The prohibited, suspended and unlicensed drivers are major road safety issues since the drivers lost their licenses because of poor driving behaviors which caused collisions.

The ALPR System is a license plate recognition program that allows vehicles observed by cameras to have their license plate read and recorded using pattern recognition software. ALPR uses colour, infrared cameras and recognition software to read license plates at a rate of up to 3000+ per hour. The cameras are mounted on marked and "unmarked" police vehicles and take a picture of parked and moving vehicles.

The photographed license plates are run against the ALPR data base loaded daily into each ALPR on board computer unit. "Hits" appear on an ALPR screen in un-marked vehicles and on the MWS in marked vehicles. While the "hit" can be made to appear on the MWS screen, there is not direct interface to the MWS and the plates are not run against the CPIC or ICBC Driver's data bank. A manual interface (member) is required to key the license plate into the MWS for CPIC and ICBC Driver's database access. The ALPR System does not collect personal information but does use personal information when a "hit" is registered and results in a vehicle stopped by police and an investigation is commenced.

There is an increasing recognition that individuals involved in auto thefts, unlicensed, prohibited suspended and uninsured drivers are all high risk drivers that are over represented in serious collisions. It is hoped by using the ALPR this will increase the perception of apprehension and lower the high violation rates associated to unlicensed, prohibited, suspended and uninsured drivers that have been observed in the initial ALPR pilot project. ALPR together with MWS access to CPIC, and ICBC Drivers database allows the police the full use of modern technology to detect, and challenge the criminal element of the use of vehicles and highways in their commission of criminal and provincial offences.

Royal Canadian Mounted Police   Gendarmerie royale du Canada

Table of Contents

Table of Figures

Acronyms Definition of Acronym Used

The following is a list of abbreviations and acronyms that may be used in this report:

1X	Airwave radio type signal data carrier for MWS Operations
ACU	PRIME-BC Audit and Compliance Unit
ACUPIES	Automated Canadian/USA Police Information Exchange System
AFIS	Automated Fingerprint Identification System
ALPR	Automatic License Plate Recognition
ATIP	Access to Information and Privacy
AVL	Automatic Vehicle Locator
CABS	Computer Aided Booking System
CAD	Computer Aided Dispatch
CCJS	Canadian Center for Justice Statistics
CDPD	Cellular Digital Packet Data (Mode of airwave carrier)
CFRS	Canadian Firearms Registration System
CIIDS	Computerized Integrated Information Dispatch System
CIO	Chief Information Officer
CJB	Criminal Justice Branch
COTS	Commercial-Off-The-Shelf
CPEG	Common Police Environment Group
CPIC	Canadian Police Information Center
CPSIN	Canadian Public Safety Information Network
CRD	Capital Regional District
Data	Information and personal information
D/COMMR OPS	Deputy Commissioner Operations
DMZ	De-Militarized Zone
DRE	Direct (Desktop) Report Entry
DSO	Division Security Officer
ERTT	Emergency Request to Talk
FIP	Firearms Interest To Police
FOIPPA	Freedom of Information and Protection of Privacy Act
FPS	Fingerprint Service Number
GIS	General Investigation Section
GO	General Occurrence (occurrence report in Prime-BC)
GOC	Government of Canada
GPS	Global Positioning Satellite
I & A	Identification and Authentication
ICBC	Insurance Corporation British Columbia
ICURS	Institute for Canadian Urban Research Studies
IDS	Integrated Data Service
IDS	Intrusion Detection System
IFAB	Visiphor InForce Arrest and Booking Application-formerly CABS
IJI	Integrated Justice Initiative
IM	Information Management
IMPACT	Integrated Municipal Provincial Auto Crime Team
IQT	Integrated Query Tool

JUSTIN	Integrated Justice for the Province of British Columbia
KO	Known Offender
LEIP	Law Enforcement Information Portal
MCM	Major Case Management
MDT	Mobile Data Terminal
MJ	Multi-jurisdictional
MNI	Master Name Index
MOU	Memorandum of Understanding
MRE	Mobile reporting Environment
MVI	Master Vehicle Index
MWS	Mobile Work Station(s)
NCDB	National Criminal Data Bank
NIII	National Integrated Interagency Information System
NPS	National Police Services
NPS Net	National Police Services Network
O/RMS	Occurrence/Records Management System
OCA-BC	Organized Crime Agency – British Columbia
OMS	Occurrence Management System
OPSSC	Operations Police Systems Services Center
OSR	Operational Statistical Reporting
PCO	Privacy Commissioner's Office
PEV	Production Environment Validation
PIA	Privacy Impact Assessment
PIP	Police Information Portal (See LEIP)
PIRS	Police Information Retrieval System
PKI	Public Key Infrastructure
PMO	Parallel Mode of Operation
POLICE CAD	Versaterm Computer Aided Dispatch System
PRIME-BC	Police Records Information Management Environment – BC
PROS	Police Reporting and Occurrence System
QA	Quality Assurance
QC	Quality Control
RBAC	Role based Access Control
RCC	Report to Crown Counsel
RCMP-GRC	Royal Canadian Mounted Police
RF	Radio Frequency
RMS	Records Management System
ROADS	Remote Office And Dispatch System (Mobile work station)
ROSS	RCMP Office Support System
RWRS	Restricted Weapon Registration System
SAMM	Status And Messaging Module (new ROADS application)
SCCJR	Sun Centre for Criminal Justice Research
SOS	Statement of Sensitivity
SPURS	Simplified Paperless Universal Reporting System
SUA	Special User Agreement
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment
TRC	Telephone Report Center
UCR	Uniform Crime Reporting
UHF	Ultra High Frequency
VA	Vulnerability Assessment

Royal Canadian Mounted Police Gendarmerie royale du Canada

VERSADEX RMS	Versaterm Records Management System (PRIME-BC)
ViCLAS	Violent Crime Linkage Analysis System

1. Project Definition

The "Automatic License Plate Recognition" (ALPR) technology is a program implemented for the RCMP "E" Division Traffic Services, Major Crime, Integrated Municipal Provincial Auto Crime Team (IMPACT) Operations, RCMP front-line uniform and plain clothes units. The ALPR enables the ability, at high speed, to quickly scan and check plates against the CPIC vehicle data base, and the ICBC (Insurance Corporation of British Columbia) driver's data base for: stolen vehicles, uninsured vehicles and drivers license suspensions, or prohibitions attached to a registered owner of a motor vehicle.

Policy Centre:

Primary	"E" Division Contracting Policing Services
Secondary	"E" Division Traffic Services

1.1. Background
1.2.

The Automatic License Plate Recognition System is implemented to provide the RCMP Traffic, Major Crime, Integrated Municipal Provincial Auto Crime Team (IMPACT) and policing in general the ability to electronically check license plates using effective, efficient, modern technology.

The ALPR system is a license plate recognition application whereby vehicles observed by infrared cameras have their license plates read, recorded and checked against a pre-loaded data base using pattern recognition software. The primary purpose of the ALPR system is to improve road safety by targeting drivers that have lost or fail to have a valid driver's license because of past bad driving behaviors.

1.1.1. Modes of Operation

The "Automatic License Plate Recognition" application is operated in two modes:

Overt Operational Mode

A marked police transport has four (4) cameras mounted on the light bar, two facing forward and one to each side. The ALPR computer is trunk mounted with a connection to the mobile work station (MWS) screen allowing any "Hits" to be monitored. There is no direct system interface between the MWS and the ALPR. The operator must manually key "Hit" information into the MWS to run the "Hit" against live / real time CPIC or ICBC data bases. The loading of the ALPR information is described on pages 19-21 and 25-30 of this report.

Covert Operational Mode

The unmarked police operational mode has six (6) cameras mounted in a roof top carrier / cargo box on a sport utility vehicle (SUV). The ALPR unit is mounted in the rear of the SUV but does not have a connection to the MWS for viewing purposes. There is an ALPR view screen (approximately 4" X 6") mounted in the front for the operator to view any hit information. The unmarked vehicles are used by IMPACT, Detachments and Traffic Services to target the high risk drivers that steal vehicles and driver that are uninsured, unlicensed, suspended or prohibited .

The scope of work encompassed in this deliverable is a Privacy Impact Assessment (PIA) for the ALPR application. This process that enables police the full use of modern technology to read, record and recognize a high volume of license plates while the police transport is either mobile or stationary.

1.1.2. Loading Information on ALPR Computer

Each morning, A RCMP ALPR designated employee downloads the stolen vehicle / CPIC "Hotlist" from CPIC, the updated Motor Vehicle Branch list of suspended drivers and the Insurance Corporation British Columbia (ICBC) list of uninsured motor vehicles.

A RCMP ALPR designated employee with appropriate role based access controls (RBAC) posts the information and down loads to a shared folder on a ROSS server where only appropriate ALPR users have access to. The purpose for this is to share the hotlists with ALPR users in the field without having the users download the hotlists directly from CPIC and ICBC themselves. Only one designated person has rights to download the hotlists from CPIC and ICBC.

1.1.3. Storage and Retention of ALPR Information

The electronic information (photos of the vehicle and license plates) are stored on the server in the following fashion:

"No Hit Information" two month / 60 day period and then purged from the system. (This information can only be accessed through a legitimate serious criminal investigation where there is already a suspect vehicle and the plate and associated personal information is already known. The request must be authorized by the OIC of "E" Division Traffic Services or his delegate after an operational file number is provided and justification for the search must be provided) On non hit the picture of the vehicle is not kept, only the picture of the plate, therefore there is no way to identify the driver.

"Hit Information" two year period, and an operational file opened for the investigator. The picture of the vehicle and plate is kept for court purposes.

If there is no court or other action, the file is purged after two years. The retention periods is in accordance with the Government of Canada records keeping and file management procedures, based on crime type / activity.

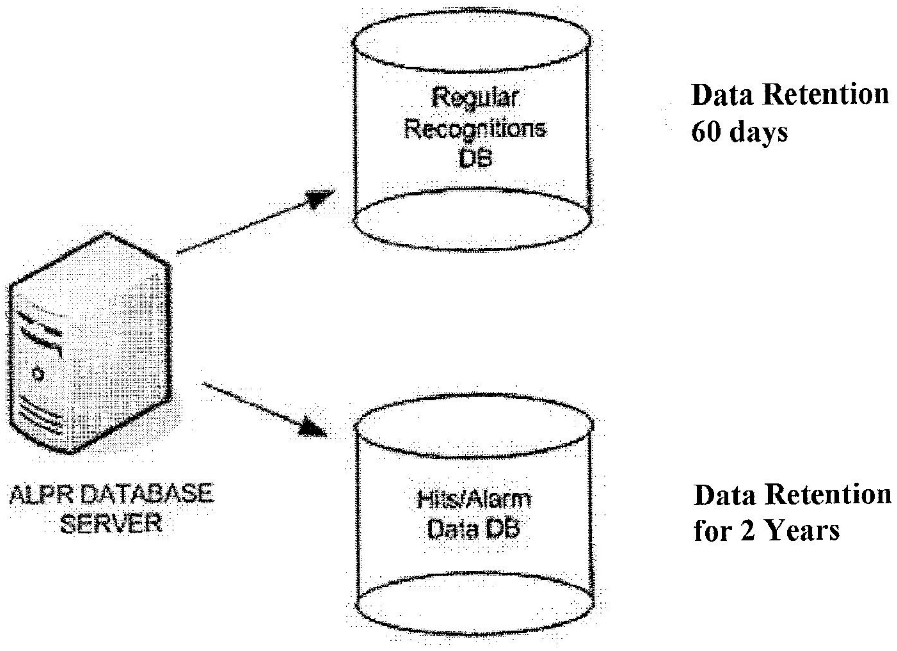


FIGURE 1. ALPR DATA STORAGE

1.2 Scope of the Privacy Impact Assessment (PIA)

The scope of the PIA is to analyze the business processes and data flow for the information being managed and protected, ensuring any privacy considerations or issues relative to the collection, use and disclosure of personal information will be addressed by the RCMP as the lead agency responsible for the implementation and management of the ALPR. This includes the Network infrastructure to and from the ALPR Server to the RCMP ALPR designated employee's work station at "E" Division Traffic Service, and into the USB memory key / thumb drive. The data flow transactions to and from the ALPR computer utilizing the USB External Storage Device (USB Thumb Drive)will also be examined.

The CPIC information data is housed within the CPIC data base which is managed by the RCMP. The central hub to the RCMP National Police Services Network (NPSN) is located at the RCMP National Headquarters, Canadian Police Information Center (CPIC) building, 1200 Vanier Parkway, Ottawa, Ontario, K1A OR2. The NPSN is used from "E" Division Headquarters at 5255 Heather Street., Vancouver, B.C. to "E" Division Traffic Services located at #306C-20338 65th Avenue, Langley, BC V2Y 2X3.

The information contained in the Province of British Columbia, ICBC Driver's data base, which is managed by the Province of British Columbia, is considered outside the scope of this PIA.

This PIA will identify the safeguards and vulnerabilities to confidentiality, integrity, and availability of the network infrastructure as well as the data repositories (databases). It will also supply recommendations, if required, to further secure and protect the integrity of the system.

This PIA has been completed as outlined in the directives by Treasury Board and the RCMP Administration Manual.

1.3 Assumptions

The ALPR will be implemented in the Province of British Columbia, throughout the RCMP "E" Division predominately within Municipal and Provincial Traffic Services and interagency law enforcement units responsible for policing stolen vehicles such as IMPACT and Detachments.

The ALPR will potentially be implemented nationally across the RCMP and to other external police agencies.

1.4 Key Personnel

Technical, operations and security related information was provided by CIO representatives, RCMP Network Services Ottawa, RCMP Departmental Security and specific personnel:

R.J. Howe	HRH Howe Consulting Services
Andre Plante	RCMP Departmental Security
Doug Edward	RCMP Computer Services Pacific Region
Lori Eng	RCMP Computer Services "E" Division
Norm Gaumont	OIC RCMP "E" Division Traffic Services
Warren Nelson	RCMP "E" Division Traffic Services
Bunny Edward	RCMP Pacific Region Departmental Security
Peter Rowe	RCMP "E" Division Informatics Branch/OSB
Steve Hambrook	RCMP "E" Division Network Services
Wayne Holland	IMPACT

1.4.1. Project Team

R.J. Howe	HRH Howe Consulting Services

2. Description of Assets

2.1. Hardware Assets ALPR

Description	Name/Model	Value (per unit)	Total
Database Server(s) X (1)		50,000	50,000
ALPR Unit X 9		30,000	270,000
Capital - Software	To be determined		
Traffic Work Station	Desk Tops already in place		
Memory Keys 4Gb		75	3,000
RF interface- Modem	To be determined		
Security Tokens -	Not required		
Mobile Work Stations	Tree Mounted MWS or Portable already in place		
Network/ADSL Access	In place		
TOTAL COST initial phase			**$350,000**

2.2. Software Assets

ALPR Software is a product originating from ANPR (Automatic Number Plate Recognition) Technologies. The Canadian vendor is Blue Max Lighting & Emergency Equipment, 18446 - 53rd Ave., Surrey, BC V3S 7A4, (604 574-4062) E-mail: bluemaxcanada.com

3. SYSTEM DESCRIPTION

3.1 System Rationale

The use of modern efficient and effective technology has allowed policing agencies to quickly access information with respect to persons whose rights to operate a motor vehicle have been suspended either by the justice system or through the Motor Vehicle Branch. Studies have shown that impaired, drunk or suspended drivers have similar offending profile(s) to mainstream criminal offenders. Nearly 80% of suspended drivers had a criminal record prior to any suspension taking effect. The study was conducted by the Home Office in Great Britain. An important point in the study indicated that persons repeatedly committing serious traffic offences are likely to commit serious criminal offences as well. The ALPR operation has already helped to identify and lead to the arrest of a homicide suspect in the Lower Mainland Area.

One of the key challenges facing the RCMP and other police agencies is the competition for limited budget resources from the public purse. The RCMP and other police agencies must take advantage of modern computer based technology to efficiently support law enforcement activities in public safety and enforcement. The ALPR represents a viable tool to support public safety and brings focus to future policing requirements and options for service delivery.

The ALPR Program will assist the RCMP in meeting its vision, values and goals with additional tools for crime prevention, traffic enforcement and ensuring safer homes and communities. To enable operational readiness, it is essential that the RCMP continue being proactive in its use of contemporary technologies.

Over the following few years the RCMP "E" Division Traffic Services projects the expansion of the ALPR Program to the major centers throughout the Province of British Columbia. The current ALPR Program has capacity to support up to twenty-five ALPR units. If the number of vehicles exceeds twenty-five, additional ALPR systems will have to be acquired.

The intent of implementing the ALPR system into the RCMP and integrated policing programs is to provide a more efficient and effective method of checking vehicular traffic for:

<u>ICBC DRIVER"S DATABASE</u>
a) Prohibited Drivers (Provincial) linked by License Plate Number
b) Unlicensed Drivers linked by License Plate Number
c) Suspended Drivers (Provincial) linked by License Plate Number
d) Uninsured motor vehicles by license plate

<u>CPIC Databases</u>
a) Stolen Vehicles
b) Wanted Persons linked by License Plate Number
c) Missing Persons linked by License Plate Number
d) Prohibited Persons linked by License Plate Number
e) Accused Person linked by License Plate Number
f) Court Action linked by License Plate Number
g) Person on Parole linked by License Plate Number
h) Special Interest Police linked by License Plate Number
i) Person Refused Firearms linked by License Plate Number

Vehicle license plates that are not entered or flagged on CPIC or the Insurance Corporation of British Columbia (ICBC) Driver's database are recognized and ignored by the ALPR System. Should a flagged license plate be checked, 6 different audible signal can be sounded for the attention of the operator.

1) Possible prohibited Driver
2) Possible unlicensed Driver (includes suspended drivers)
3) Possible uninsured vehicle
4) Possible stolen vehicle
5) Possible outstanding warrant
6) Information only, no authority to intercept (this includes all other CPIC categories related to a vehicle)

On warnings 1 through 5 the operator validates the ALPR at this point by the manually entering the license plate into the mobile work station (MWS), which checks CPIC, or ICBC systems. Once confirmation is received any necessary enforcement action can be taken and an operational police file is generated. The ALPR system recording time is accurate to within .01 seconds.

On warning number 6 no action can be taken since this is simply for information only. This allows the Police officer to review the information through CPIC to make sure the individual does not have Parole or Probation restriction that they may be in violation, such as being out past a curfew. The information is available if the police officer observes a violation and need to interact with the driver.

At the end of shift, the ALPR operator cleans out the system buffer in the police vehicle. The USB External Storage Device (USB Thumb Drive) is returned to the designated RCMP "E" Division Traffic Services employee and the data is downloaded to the ALPR Server located in "E" Division Headquarters. When a "hit" is registered, the ALPR System generates:

a) Picture of the license plate.
b) Picture of the Vehicle. ("Hits" only)
c) Text box with the date and time of the check.
d) The GPS coordinate where the picture was taken.
e) Data base that originated the hit, i.e. CPIC or ICBC.

An off-line or data base search may be conducted. The parameters established for this search is consistent with legitimate policing enquiries and for official use only. Any off-line search requests must be in writing and approved by the OIC or designate of "E" Division Traffic Services for legitimate investigational purposes. The investigating agency must have a suspect plate with the associated personal information as part of an ongoing criminal investigation. On "Non Hits" there is no ability to get the picture of the vehicle only the plate. Therefore the ALPR database will only provide the investigator with a plate at a given location with the time and date.

3.2. Access/Operation

The ALPR Program is available to all bona fide police agencies in the Province of British Columbia. The Policy Center for the ALPR, for all RCMP and non-RCMP police agencies, is RCMP "E" Division Traffic Services situated at #306C-20338 65th Avenue, Langley, BC.

The ALPR system is presently available to Provincial and Municipal Traffic units for road safety purposes and for the auto theft interagency units such as IMPACT. Detachment can also request for covert ALPR vehicles after they submit an operational plan outlining how the vehicles is to be used. A request is made to the policy centre ("E" Division Traffic Services) for the ALPR deployment to deal with road safety issues and stolen vehicles only. The ALPR system is not to be used as an intelligence gathering tool. Upon approval, the appropriate vehicle will be readied and the necessary information loaded onto the ALPR computer. Only designated trained employees will have direct access to the download information from the server through the Ross system, and input this information via a USB External Storage Device (USB Thumb Drive) into the vehicle supporting the ALPR computer. The information contained therein consists of CPIC and ICBC driver's data in plain text and is a listing of license plate information (numbers – alpha numeric) with no connecting personal information. The CPIC and ICBC Driver's data is uploaded each morning or at the beginning of their shift.

At the end of shift, or the following day, the USB External Storage Device (USB Thumb Drive) is downloaded through the Ross system to the secure severs. The USB External Storage Device (USB Thumb Drive) is erased, and the blank USB External Storage Device (USB Thumb Drive) is recycled for use. After the ALPR police vehicle is readied for operation, the vehicle can be deployed in stationary or mobile mode. The ALPR cameras take photos of each vehicle, which includes the license number. Should the license number register a "hit", the unit operator will receive an audible signal and the vehicle is "flagged". At this point, the operator will manually enter the license plate into the mobile work station (MWS) component and run it against CPIC, MVBS and the ICBC data base. A police investigation is initiated on the incident and a records management file is created.

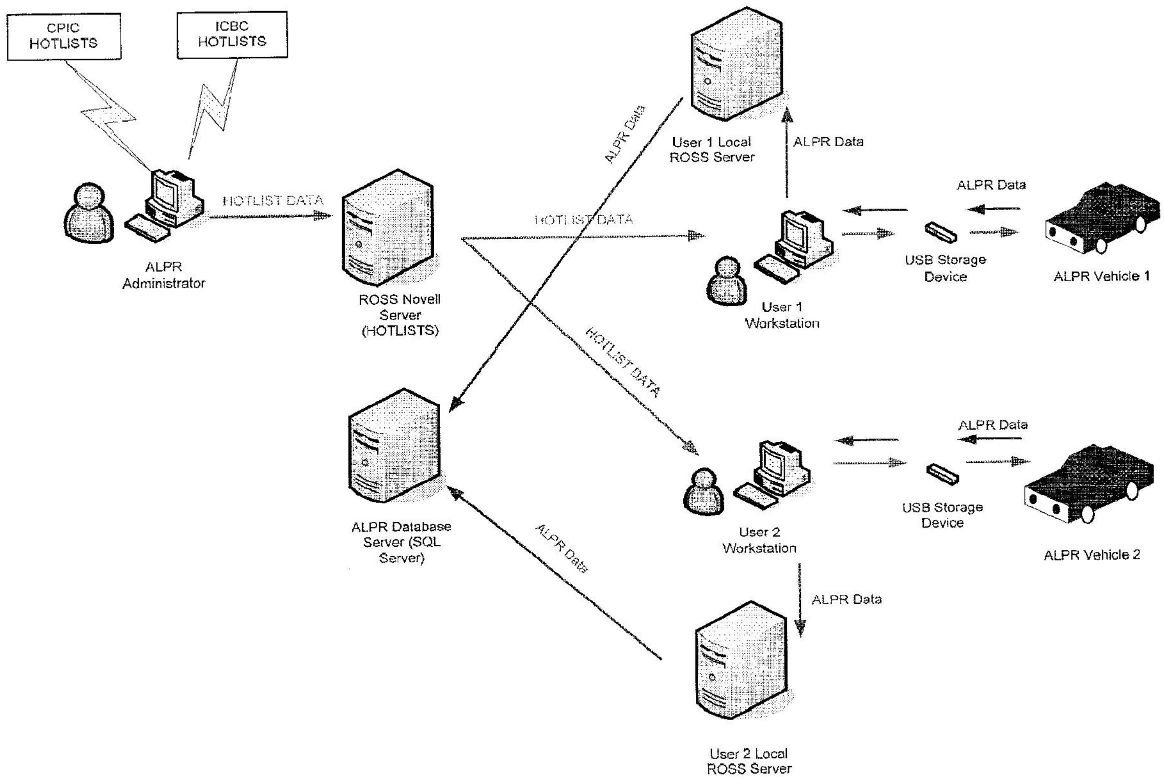
Vehicle / license plates identified as "hits" are stored on the ALPR server for a period of two years with the retention period corresponding to the applicable retention period for the investigational type in accordance with Government of Canada standards for Records Management and Uniform Crime Reporting. Otherwise the hit is "purged" after two years.

"Non-hit" vehicle / license plates are retained on the ALPR server for two months / sixty (60) days after first being checked and purged from the system. On "Non-hits only the picture of the plate is retained, therefore there is no ability to identify the driver.

With respect to the ALPR system, only authorized RCMP and non-RCMP Police agencies may have access.

Figure 2: ALPR Information Flow provides a graphic depiction of the information flow.

Figure 2: ALPR Information Flow



** There will be instances when certified extract copies of the server information on a "hit" is required for court purposes. Part of the file process is to include the exhibit seizure and follow an established exhibit continuity and maintenance procedure. The following is a draft of the intended exhibit process established for this purpose. **

4. ALPR Operational Policy - Exhibits

4.1. General Exhibit Instructions

The exhibit custodian(s) will make themselves familiar with any Operational and Administrative Policy concerning the seizure, handling, storage and release of any property, documentation, tapes, data disks or information seized and held as an exhibit for investigative or legal purposes. When an ALPR partner or ALPR itself identifies a requirement to seize any of the above or any other property or item held or controlled by ALPR:

4.2. Exhibit Storage

a. Only the Exhibit Custodian(s) will access the secure exhibit storage facility or cabinet.

b. The secure exhibit facility or cabinet will always be locked or secured except when the Exhibit Custodian(s) has to gain access.

c. The secure exhibit facility or cabinet must be secured with a lock and key which would be approved to be able to withstand any questions as to continuity of the exhibit(s) for court or legal purposes.

d. Exhibit forms (1625) will be readily available in the exhibit storage area. The exhibit forms are three pages and used for:

e. Page one (1) details of seizure and lists seized items/property.

f. Page two (2) continuation report for additional exhibits.

g. Page three (3) for the movement and handling of exhibits and a sign off for when the exhibit or property is no longer required to be held.

h. Page four (4) for the receipt of the exhibit or property back into the custody of investigator including the provision for a sign off if the item is no longer required to be held as an exhibit.

i. The exhibit area will be secure and free from any electro-magnetic fields.

4.3. Exhibit Seizure and Retention

Custodian(s) will:

a. Upon seizing exhibits, properly mark/tag all items for exhibit retention and assign an exhibit number.

b. Maintain a file and ledger itemizing all exhibits on the appropriate Exhibit form

c. After marking or tagging the exhibits, complete the appropriate exhibit report form, itemizing all articles seized.

d. Open an operational file with the details and/or requirement for the seizure, in the "E" Division Traffic or appropriate operational filing system (PRIME-BC) and ensure the file number is entered on the exhibit form.

e. Enter the exhibit(s) in the exhibit ledger.

f. Place the exhibit(s) in a secure storage facility, lock and secure.

g. If the exhibit is a data disk, a logging tape (including reproduction) or a video tape, ensure that there is no de-magnetizing equipment within 10 feet of the exhibit or in the area free of any electro-magnetic fields.

h. Diary Date the exhibit file with a ninety day (90) review date to determine if there is still the requirement to hold/retain the item as an exhibit. If the requirement continues, further Diary Date the exhibit file for a period of ninety (90) days

4.4 Disposition / Release or Movement of Exhibits

Exhibit Custodian Will:

a. Attend to disposition of exhibits without delay.

b. Obtain a signature and appropriate identification, (plus print the name, department and phone number) on Page three (3) of the Exhibit forms for the receipt of any exhibit released and why the exhibit/property was released (i.e. court purposes/investigation).

c. If an exhibit/item or property is returned to the investigator, sign the item back into exhibits as per Page four (4) and if no longer required to be held as an exhibit, have the bottom portion of the form signed off.

d. If the exhibit item is no longer required for any investigative, legal or court purposes, if it is a audiotape, video tape, memory stick or data disk it may be placed back into circulation for use.

4.5. Retention Periods

Exhibit Custodian(s) should:

a. Ensure that in the case of criminal proceedings, the appeal period has lapsed prior to putting an audio tape, video tape, memory stick or data disk back into circulation for use or otherwise disposing of any exhibit items. The appeal period ninety (90) days should have expired prior to the item being returned by the investigator however in some instances the item may not have been entered into the court process (i.e. in the case of a guilty plea) and could be returned prematurely.

b. In the case of civil proceedings, there is a two year time period from the time of the event before Civil Proceeding(s) have to be initiated. If notice is served that an exhibit item is required for a civil matter, long term exhibit storage and or file management will be required. In the normal course of business if a video, audio or data tape or disk is re-used prior to being served notice of requirement for civil proceedings, there is no onus on ALPR data manager(s) or the exhibit custodian to save and secure these type items "just in case".

5. ALPR Process

5.1 Step 1 - Informatics

1. The Canadian Police Information Centre (CPIC) "HOTLIST" is downloaded from the CPIC website.

2. The ICBC "HOTLISTS" are received via email or downloaded from ICBC's secured server.

3. Hotlists are posted to a shared folder on a ROSS server where only appropriate ALPR users have access. The purpose for this is to share the hotlists with ALPR users in the field without having the users download the hotlists directly from CPIC and ICBC themselves. Only one designated person has rights to download the hotlists from CPIC and ICBC. This is controlled out of "E" Division Traffic Services.

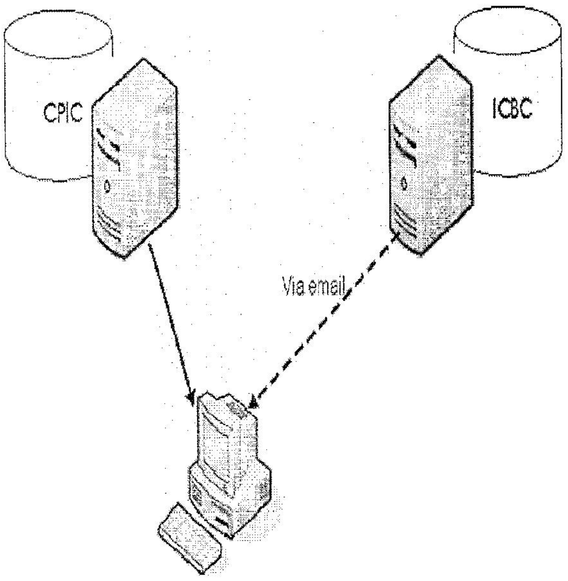


Figure 3: "HOTLIST" Download

5.2 Step 2 - Designated Traffic Employee

1. The designated trained employee will copy the CPIC and ICBC "HOTLISTS" to the folders on the USB External Storage Device (USB Thumb Drive)

2. The USB External Storage Device (USB Thumb Drive) is signed-out to the operational traffic / enforcement officer.

3. The USB External Storage Device (USB Thumb Drive) contains the CPIC and ICBC "HOTLISTS"

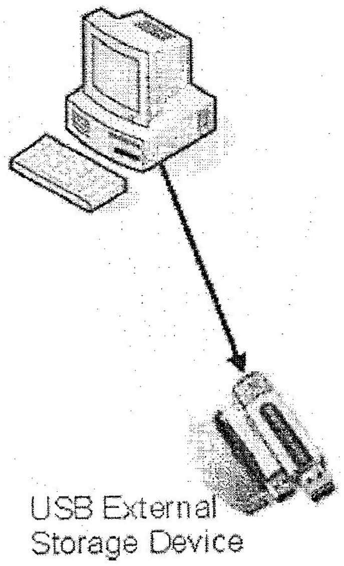


Figure 4: Data Transfer to Storage Device

5.3 Step 3 – Traffic / Enforcement Officer

1. The traffic / enforcement officer inserts the USB External Storage Device (USB Thumb Drive) into the vehicle's USB port and then powers up the in-vehicle computer.

2. Once the computer is on the system is ready to be deployed. All the data being collected is stored on the USB External Storage Device (USB Thumb Drive) rather than the in-vehicle computer's hard-drive. The storage devices are all password protected.

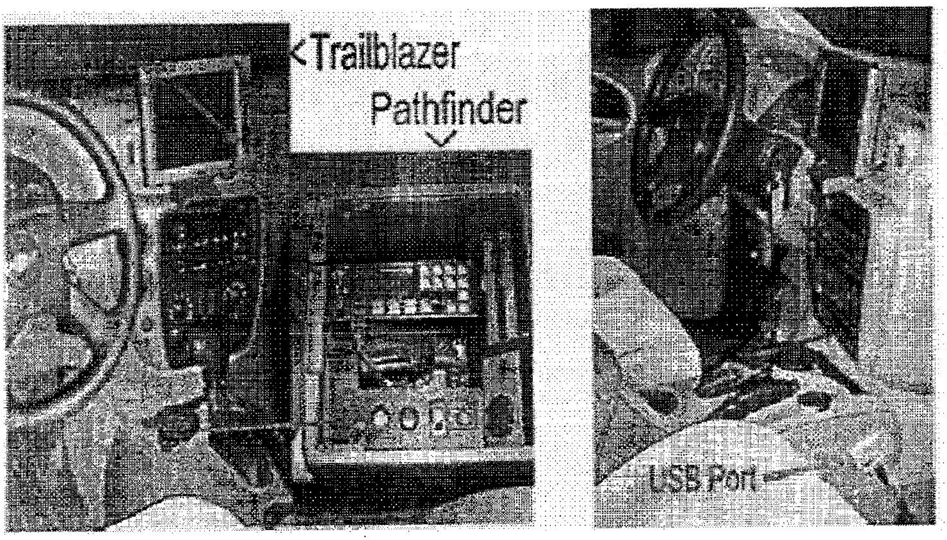
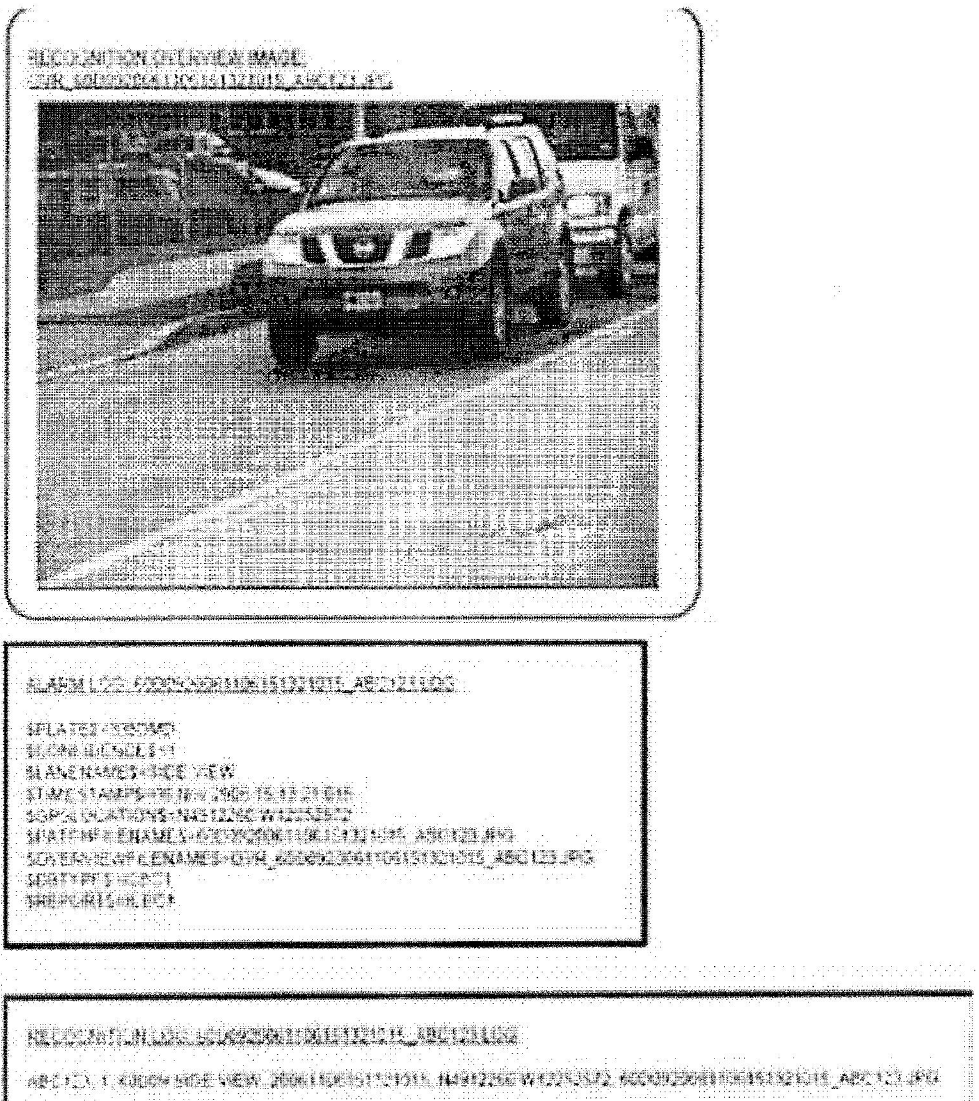


Figure 5: Interior USB Connection

3. Audible alarms represent an integral component to the ALPR. Each "hotlist" will have its own distinct audible sound (i.e. "Alert – Possible Stolen Vehicle"; "Alert – Possible Prohibited Driver"; etc.)



RECOGNITION OVERVIEW IMAGE
OVR_[illegible]_ABC123.JPG

```
ALARM LOG: [illegible]_ABC123.LOG

$PLATE$=[illegible]
$CONFIDENCE$=1
$LANENAME$=SIDE VIEW
$TIMESTAMP$=[illegible]
$GPSLOCATION$=N[illegible]W[illegible]
$PATCHFILENAME$=[illegible]_ABC123.JPG
$OVERVIEWFILENAME$=OVR_[illegible]_ABC123.JPG
$[illegible]
$REPORT$=[illegible]
```

```
RECOGNITION LOG: [illegible]_ABC123.LOG

ABC123, 1, [illegible] SIDE VIEW, [illegible], N[illegible]W[illegible], [illegible]_ABC123.JPG
```

Figure 6: Audible Alarm

4. Cameras used in the ALPR vehicles are fixed and their settings are pre-set. In normal operation all cameras have the ability to function simultaneously.

5. At the end of a tour of duty, the traffic / enforcement officer logs off the ALPR application and shuts down the vehicle on-board computer after clearing the buffer.

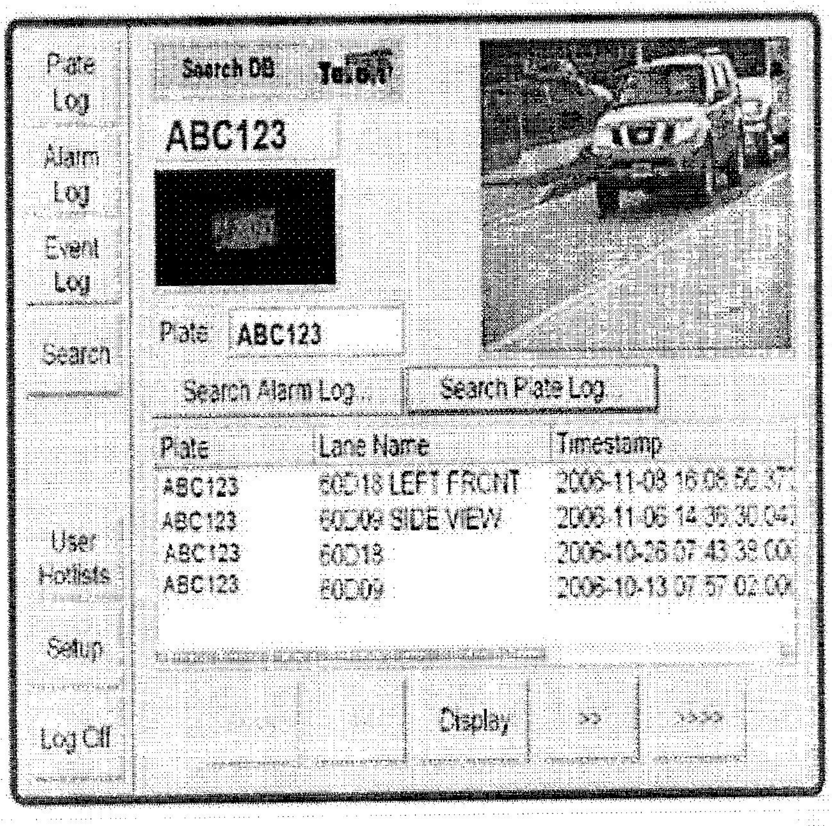


Plate: ABC123

Plate	Lane Name	Timestamp
ABC123	60D18 LEFT FRONT	2006-11-08 16:08:50.37
ABC123	60D09 SIDE VIEW	2006-11-05 14:36:30.04
ABC123	60D18	2006-10-26 07:43:39.00
ABC123	60D09	2006-10-13 07:57:02.00

Figure 7: Vehicle Log Display

6. The USB External Storage Device (USB Thumb Drive) is removed from the vehicle on-board computer and signed-in to the designated trained employee.

5.4 Step 4 - Designated Traffic Employee

1. The designated traffic employee will move the data from the USB External Storage Device to a directory on his/her local ROSS server. This directory is for temporary storage of the ALPR data until the data gets transferred to the server at the "E" Division Headquarters building. The folder used to store this data is used solely for temporary ALPR data storage with access permission given to only ALPR users. To prevent bandwidth issues during prime office hours, this transfer is not done until midnight.

2. A copy script set automatically to execute at midnight on the main ALPR database server located at the "E" Division Headquarters building. This script checks for data in the ALPR temporary storage folders on the ROSS servers of where ALPR officers post data. If data exists, it will be moved to the main ALPR database server where it will be imported into the database.

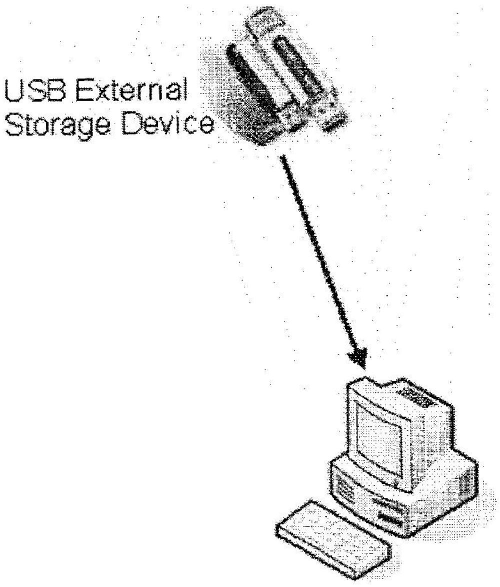


Figure 8: Data Transfer

5.5 Step 5 – Informatics (ALPR Back-Office)

There are programs running as services on the ALPR database server at all times. These programs watch for incoming ALPR data. Once ALPR data arrives in the processing folders on the server, the data is immediately ingested into the ALPR SQL Server database. Regular recognition data and alarm data are stored separately as they both have different retention purge policies.

5.6. Step 6 – Records Management (File Retention)

1. Vehicle / plates identified as "hits" are stored on the ALPR server for a period of two years with the retention period corresponding to the applicable retention period for the investigational file generated in accordance with Government of Canada standards for Records Management and Uniform Crime Reporting. Otherwise the hit is "purged" after two years.

2. "Non-hit" vehicle / license plates are retained on the ALPR server for two months / sixty (60) days after first being checked and purged from the system.

6. ALPR Objectives

The objectives of the ALPR process are:

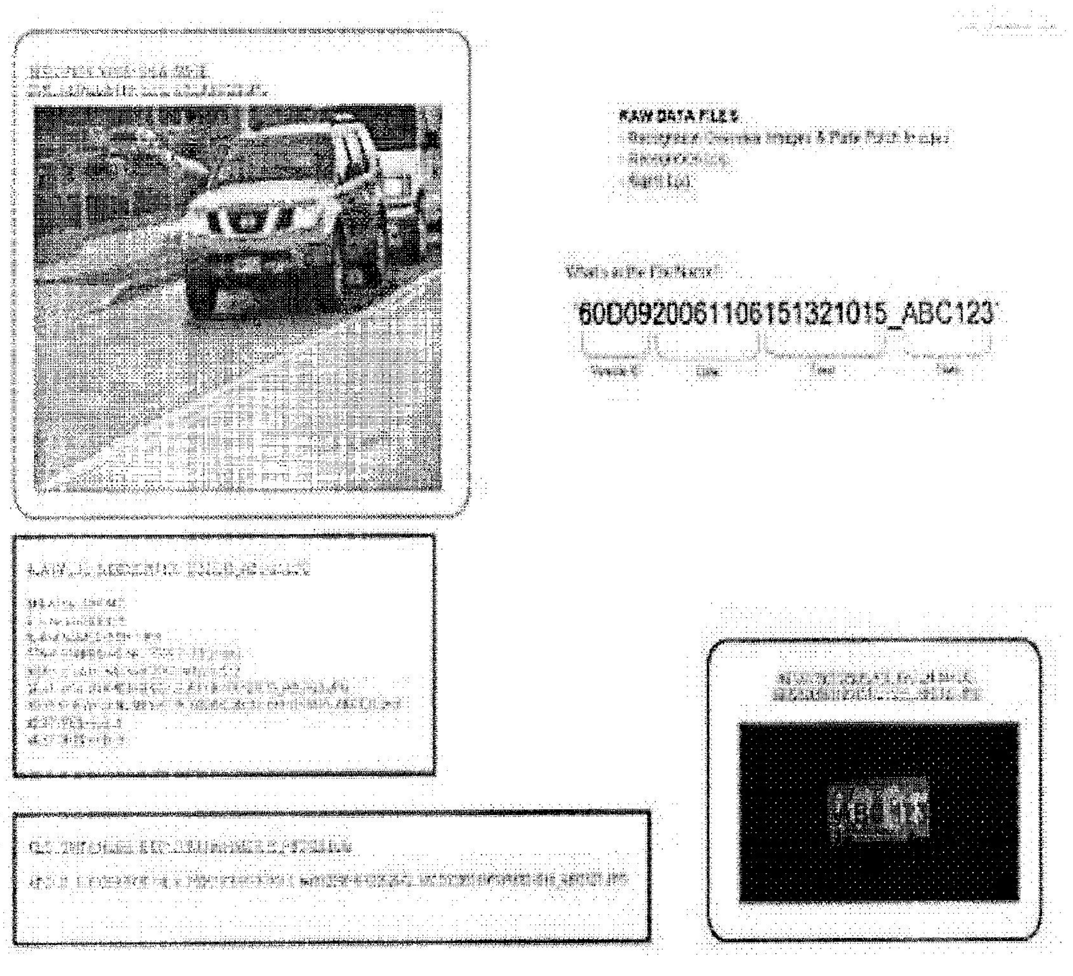
- is to improve road safety by concentrating and apprehending the worse drivers that have lost their Drivers licenses because of bad driving behaviors or are uninsured and to recover and charge individuals who make a career of stealing vehicles.

- to provide the RCMP and participating integrated policing agencies with modern tools enabling front-line traffic / enforcement officers to be more time efficient and effective than the current manually inputted individual checks with CPIC, and ICBC drivers database through the mobile workstation;

- to provide police investigators with instant feed-back on positive "Hits" so that the focus of the investigation is concentrated in the areas of high risk drivers.

- to decrease unnecessary police mobile radio or MWS air time and NPSN use during the performance of roadside or moving checks that may not be considered worthwhile or value added to duties;

- to provide photographic record of the vehicle license plate(s) including the vehicle ("Hits only), data and time the check was made on any positive "hits".



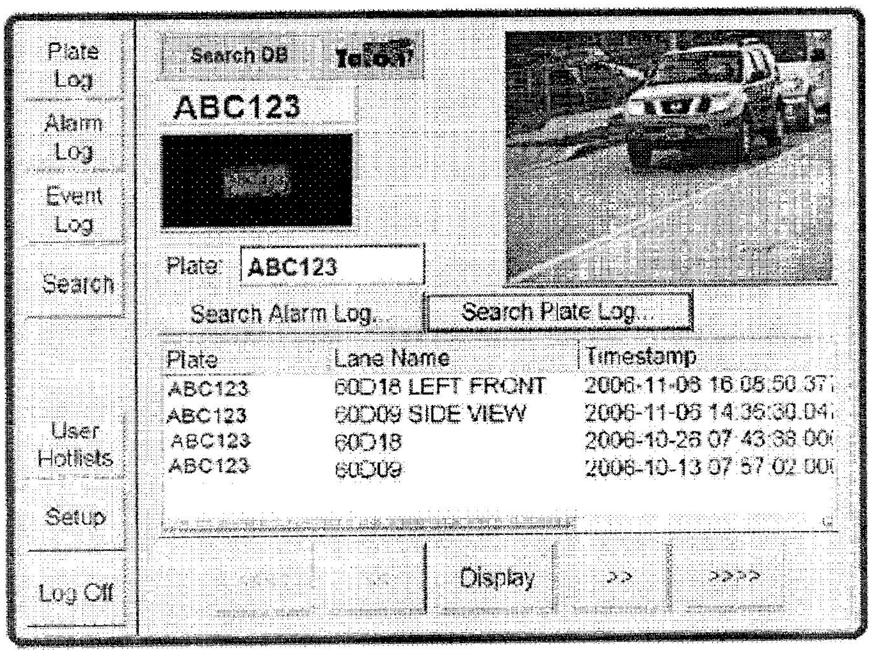


Plate: ABC123

Plate	Lane Name	Timestamp
ABC123	60D18 LEFT FRONT	2006-11-08 16:05:50.37
ABC123	60D09 SIDE VIEW	2006-11-06 14:35:30.04
ABC123	60D18	2006-10-26 07:43:38.00
ABC123	60D09	2006-10-13 07:57:02.00

Figure 9: ALPR Photo Image

6.1 Inefficiencies of the Current Process Environment

The current process for vehicle plate checks is completed in several different methods.

a. Investigator uses a mobile radio to call an OCC (Operational Communication Centre) and requests the dispatcher or info operator to run the vehicle plate on CPIC and against the ICBC and RMS data bases. If a "hit" is obtained, the investigator continues on with an investigation. The investigator is competing for both radio air time and the operator's time in this instance.

b. Investigator uses a land-line telephone to perform the same check, however is competing with other telephone traffic going into the OCC and again for the operator's time. Usually when this occurs, the instance of being able to stop and check a vehicle has past.

c. Investigator uses a mobile work station and may conduct stationary or rolling check of a plate. Any "hit" on the MWS for the check is received as a "hit" confirmation on the MWS and on the OCC Dispatcher's screen, providing the investigator has logged onto the dispatch system. This would not occur for covert operations. To date this has been the most efficient and effective use of technology for "checks" but is limited to those areas that can support the mobile work station technology.

6.2 Security of Information for the RCMP

The CPIC "HOTLIST" from the web site, and the ICBC "HOTLIST" information is downloaded to the Ross Server. "E" Division Traffic Services sends the information to all users every morning through ROSS. This information is transferred to a USB External Storage Device (USB Thumb Drive) and the designated employee physically takes the USB External Storage Device (USB Thumb Drive) and loads the information into each ALPR unit in the police vehicles. All checks are recorded on the USB External Storage Device (USB Thumb Drive). At the end of shift, the operator transfers the USB External Storage Device (USB Thumb Drive) onto the Ross network where it is automatically downloaded to the ALPR server. The entire process is controlled and any movement of information, computer to server is over the NPSN. Policies and Procedures are in place to govern the processes.

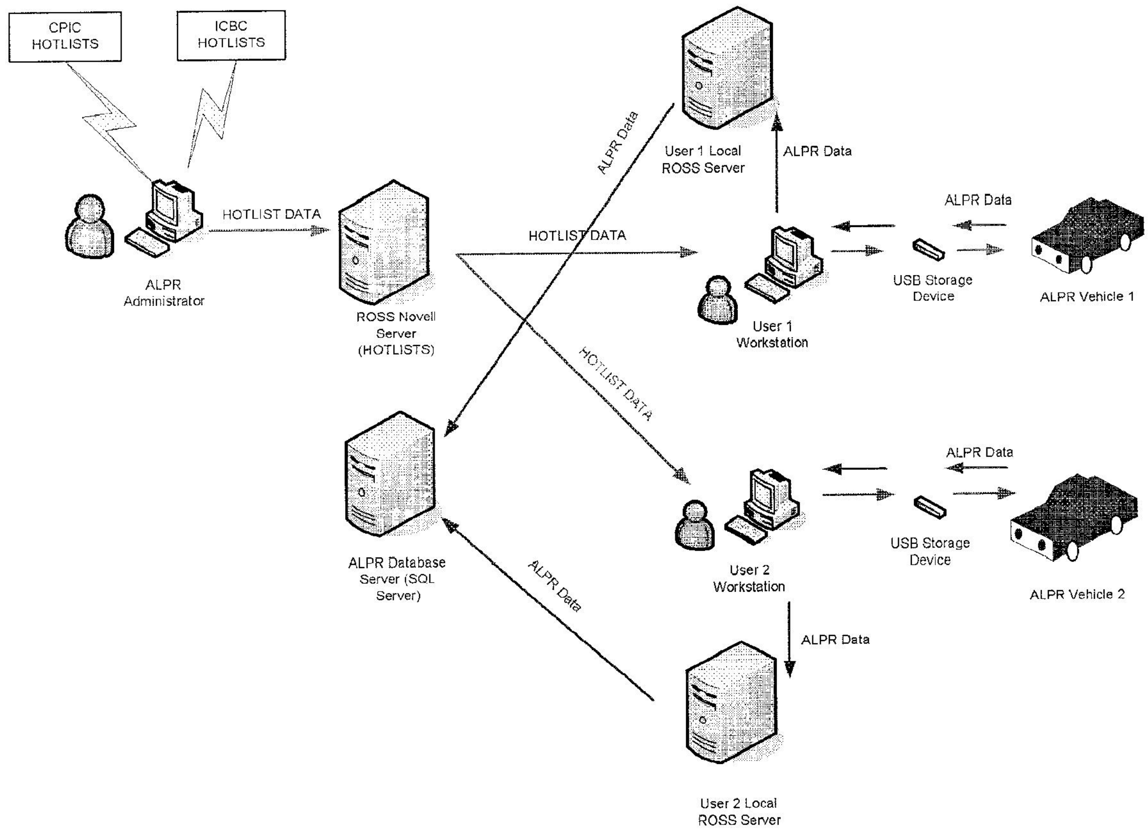


Figure 10: ALPR Information Flow

6.3 RCMP INFOWEB Overview

The RCMP Infoweb is the RCMP's internal intranet and the designated employee at "E" Division Traffic Services uses this feature to access the CPIC "HOTLIST" Web Site. A userid and password is required to access the RCMP Infoweb. A link on the Infoweb entitled "Change Password" allows an employee to change their password at any time. User accounts on the Infoweb are created without a password, which locks the employee out. A password is assigned on request to the RCMP's Central Help Desk, or to a specific email account set up to receive requests from new users. The passwords are provided to the employee via the RCMP's corporate email.

6.4 ALPR Privacy Notice

The information downloaded from CPIC and ICBC data is in plain text and is a listing of license plate information only. Policy prohibits the query of any plate numbers that links to personal information unless there is a hit or an active investigation where the plate is already a suspect and the personal information is already known. Therefore the ALPR database only provides a vehicle at a given location all other personal information must be obtained by other means such as an ongoing investigation.

When checks are made and a photograph taken by the ALPR unit, a picture of the vehicle is taken, including the license plate. If occupied, the occupant(s) of the vehicle may be visible in the photograph, although this is highly unlikely since the camera does not focus in on the driver but on the plate. A review of over 300 random photographs from the ALPR database has demonstrated that there is less then a 2% chance of an image showing enough facial characteristics to identify hair colour, ethnicity and sometimes gender. On Non hits the RCMP is deleting the picture of the vehicles and only retaining pictures of the plate number. Effectively drivers and occupants remain anonymous even after the USB External Storage Device (USB Thumb Drive) is downloaded to the server. On hits the pictures are retained since a violation has taken place and there is authority to pull the driver over.

6.5. Audits

Employees are not able to add, change or delete information on the ALPR data base server. This is an automated system and the only manual interaction is the downloading or transfer of information. "E" Division Traffic Services will utilize the RCMP Audit Guide and / or the PRIME-BC Audit Guide for quality assurance and audit purposes.

Note: Should a broadcast be received from the Operational Communications Centre (OCC) with respect to new stolen, amber alert, and crime vehicle(s), the ALPR user may key in the license plate(s) to the ALPR terminal. The data keyed is alpha-numeric license plate numbers only.

7. Business Data Flow Analysis

7.1. Data Flow Diagram

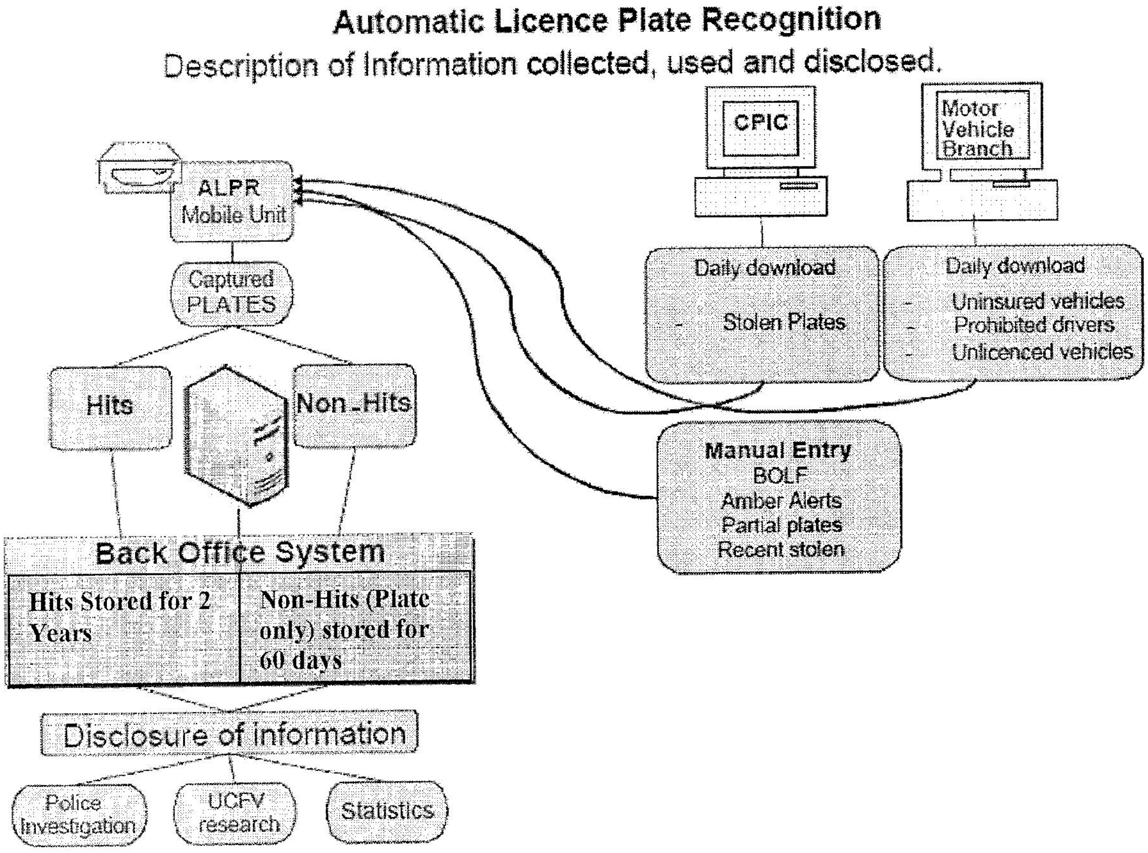


Figure 11: ALPR Information Flow

7.2 Information Storage and Retention

After the ALPR information is downloaded from the USB External Storage Device (USB Thumb Drive) via the "E" Division Traffic ALPR computer to the server, the information is separated into two storage areas.

1. Image Master Storage (IMAGESMASTER) – normal license plate recognition is held for sixty (60) days, and then purged from the system. Only license plates are retained for 60 days the picture of the vehicle is not kept.

2. Alarm Recognition Storage (HITSDB) – the "hit" data is retained two (2) years unless other retention periods apply due to further investigations.
   NOTE: In addition, an operational investigative file may be generated on the RMS which is also subject to the Government of Canada policy on records keeping.

8. Physical Environment

Users of the ALPR systems are either RCMP Members or accredited non-RCMP integrated policing unit members. ALPR equipped vehicles are locked in a secure covered parking area when not in use. The ALPR vehicles are issued out for operational purposes and the USB External Storage Device (USB Thumb Drive) to specific individuals who sign for release of the USB External Storage Device (USB Thumb Drive). The USB External Storage Device (USB Thumb Drive) is treated similar to exhibits and are password protected. They are issued / signed-out to individual users and returned directly to the appropriate designated employee or locked in an exhibit storage locker and signed-in when returned after hours.

The ALPR Server is situated inside the secure server room at RCMP "E" Division HQ. The "E" Division Traffic Services facilities have been subject to security inspections and approved by RCMP Department Security. The physical security requirements, locks, construction, cabling and conduit, walls and ceiling have been met and are considered satisfactory.

8.1. Harden ALPR Units

The on-board ALPR portable computer is secured in the locked trunk of the marked vehicles and the rear compartment of the unmarked vehicles. The computers in the unmarked vehicles are secured in an open locked rack.

Users can only access or change the input or output of the information downloaded to and from the ALPR unit via the USB External Storage Device (USB Thumb Drive) as there is personal intervention for the control of the download and custody of the USB External Storage Device (USB Thumb Drive).

Hardening procedures, maintenance and build documentation for servers and workstations include reviews to ensure that software has been tested and updated, relevant security patches applied, and configured to prohibit access to sensitive information. In particular, maintenance procedures should be modified to ensure that both outdated and unnecessary files created either during installation or maintenance are deleted and backed-up storage mediums such as CD's are made of the system logs to track all transactions and access to the system.

8.2. Policy and Procedures

Policy and Procedures and a Sign-Off process are documented for users requiring access rights to use this system in the ALPR Policy and Procedures, RCMP OM 25.100 (E Div) - ALPR Policy.

9. Security Requirements

9.1. Statement of Sensitivity

"A Statement of Sensitivity, file number 2004 E - 3100, was completed by R. J. Howe together with "E" Division Departmental Security, RCMP in 2007 and updated in September 2008."

10. Security and Confidentiality Requirements

The ALPR software is designed to efficiently read process and run license plate numbers against a pre-loaded data base internal to the ALPR Unit. Any "hit" information is validated with the CPIC and/or ICBC/MVB data bases. The result is the RCMP and other police agencies are able to enter into immediate investigations, prevent furtherance of criminal offences, i.e. stolen autos, driving while prohibited or without insurance, solve crimes and acquire intelligence which would be shared amongst police departments. Currently the ALPR infrastructure only transmits information from the USB External Storage Device (USB Thumb Drive), to a RCMP desktop computer over the NPSN to the ALPR Server.

<u>NOTE:</u> It is foreseeable in the future, in order to maximize efficiencies, the Mobile Work Station application will be used as the carrier (1X) over cellular airwaves for the uploading and downloading of the ALPR information. In the event that this is implemented, an addendum to the PIA and TRA/SOS will be submitted.

The types of information presently being stored on and transmitted by the infrastructure are the download from the ICBC "HOTLISTS" email data and the CPIC "HOTLIST" website data. This information consists of a list of plain text license plate numbers associated with:

Stolen Vehicles

Description
For CPIC entry and record-keeping purposes, this primary category is used to record data on vehicles that are reported stolen.

Accused Person

Description
For CPIC entry and record-keeping purposes, this primary category is used to record data on a person (adult or young person):

1. against whom legal proceedings have commenced (that is, an information has been laid) in relation to:
    - a Criminal Code (CC) offence or an offence under a federal statute, who is awaiting final disposition, including any appeal, and for whom a warrant to arrest is not in force for that offence; or
    - an offence under a provincial statute or municipal by-law, who has been released by a court of law with specific conditions that can be monitored by the police. OR

2. to whom a peace officer has issued an appearance notice under Section 496*CC*; **OR**
3. who has been released from custody by an Officer in Charge under Section 498 or 499*CC*.

> ***Note***: Accused and Failure to Appear records are related. Upon issuance of a warrant for Failure to Appear, cross-reference the WANT record to the existing ACCD record. Officer in Charge is defined under Section 493CC.

4. who has been found Not Criminally Responsible on Account of Mental Disorder and is awaiting disposition from a Review Board (recognizance is to continue under Section 672.46 of the *Criminal Code).*

Court Action

Description

For CPIC entry and record keeping purposes, this primary category is used to record data on a person (adult or young person):

1. who has legal custody of a child as specified in an order of the court (criminal or civil); **OR**
2. against whom proceedings have commenced and who:
    1. has been given a Suspended Sentence, or Conditional Discharge under Section 736 (1) or Section 672.54 (b) *CC*; **or**
    2. has been released on probation (**NOTE**: For CPIC entry purposes, this includes a subject sentenced under the provision of para 42(2)(k) or 42(2)(I) YCJA); **or**
    3. has been placed on a peace bond (including issuance under Section 810.1 *CC*, where a person fears that the subject will commit a sexual offence against a child), recognizance or restraining order; **or**
    4. is a young person who is in "open custody"; or who has been sentenced under the provisions of paragraph 42(2) of the *Youth Criminal Justice Act* and who, upon the expiry of the custodial portion of the sentence, has been released into the community subject to conditions, under 42(2) (n) of the YCJA; or the subject is under conditional supervision under paragraph 42(2) (o), (q), or (r) YCJA; or for whom there is a deferred custody and supervision order under paragraph 42(2) (p) YCJA; **or**
    5. is a reluctant witness who has been arrested under the authority of Sec. 698(2), 704 or 705 *CC* and later released on a recognizance in form 32; **or**
    6. having been found Not Guilty by Reason of Insanity (prior to February 1992) or Not Criminally Responsible on Account of Mental Disorder (after February 1992), is subject to the conditions of a Review Board or Court disposition order (that includes orders issued pursuant to Section 672.54 C.C), which could be detention in hospital, subject to conditions, or a conditional discharge (formerly Lieutenant-Governor Warrant cases); **or**
    7. has been given a conditional sentence under Section 742.3 *CC*; **or**
    8. is an adult whose case has been dealt with by alternative measures under Section 717 *CC*; **or**
    9. is a young person whose case has been dealt with by alternative measures under the *Youth Criminal Justice Act.*

Missing Person

Description

This primary category is used to record data on a person:

1. reported missing, or
2. who has been admitted/committed to a mental institution or hospital psychiatric ward and has left without permission or formal discharge (designated as an ELOPEE), or
3. for whom a police agency has undertaken to assist in locating on compassionate grounds.

Parolee

Description

This primary category is used to record data on a person who has been convicted of a criminal offence and has been released on:

1. parole,
2. day parole,
3. life parole,
4. statutory release, or
5. temporary absence over 24 hours from a penal institution.
6. electronic monitoring (Canada or Province-wide).

Prohibited Person (including Previous Deportee)

Description

This primary category is used to record data on a person against whom an Order of Prohibition is in effect with regard to liquor, firearms, vehicle driving (and boat operation), hunting or any other court or statute-imposed prohibition, e.g. *Aeronautics Act*.

Refused Person

Description

This primary category has been incorporated into CPIC to meet the requirements of the firearms provisions of the *Criminal Code* and the *Firearms Act*. It is used to record data on a person who:

1. has been refused a Firearms Registration Certificate (FRC) that the Registrar was authorized to issue under Part III of the former *Criminal Code*, or has had such an FRC revoked under the former *Criminal Code* prior to 1998-12-01 or under the provisions of the *Firearms Act* on or since 1998-12-01;
2. has been refused one of the class of Firearms Licenses (e.g. Possession Only, Possession and Acquisition, Borrowing, Business, Commercial Carrier, Minors, Crossbow Acquisition, Temporary) authorized by the *Firearms Act*, which was issued on or since 1998-12-01 or has had such a license revoked since the day it was issued;
3. has been refused one of the class of Firearms Authorizations (e.g. Carry, Export, Import, Transport) authorized by the *Firearms Act,* which was issued on or since 1998-12-01 or has had such an authorization revoked since the day it was issued; 4. has been refused one of the class of Firearms Certificates (e.g. Registration, Shooting Club, Shooting Range) authorized by the *Firearms Act*, which was issued on or since 1998-12-01 or has had such a certificate revoked since the day it was issued.

Page(s) 000040 to\à 000040

Is(Are) exempted pursuant to section(s)
est(sont) exemptée(s) en vertu de(s)(l')article(s)

16(1)(b)

of the Access to Information Act
de la Loi sur l'accès à l'information

Wanted Person

Description

This primary category is used to record data on a person who is arrestable and / or for whom a warrant or apprehension order has been issued. The person must be known by name and be identifiable. Persons wanted on provincial, Canada-wide and extraditable warrants are recorded on this file. This primary category is also used to record data on a person who is the subject of a DNA Warrant (Form 5.02).

The following are taken from the ICBC Driver's database:

Unlicensed Drivers

Description

Those drivers that do not have a valid driver's license within the Province of British Columbia

Vehicles with no Insurance

Description

Vehicles that have not been insured by the Provincial Insurance Company for basic insurance coverage.

Prohibited Drivers (Provincial)

Description

Those drivers that are now prohibited from driving in British Columbia.

Suspended Drivers (Provincial)

Description

Those drivers that had their drivers license suspended because of unpaid fines.

The USB External Storage Device (USB Thumb Drive) information routed back to the ALPR server includes an image file / photo list of all vehicles scanned and read by the camera and ALPR Unit. Additionally, flagged vehicles, a photo of the vehicle, license plate, any occupants, time and date are also routed back to the ALPR server.

NOTE: This return information in future may be routed through the Mobile Work Station. A TRA, SOS and PIA have been previously submitted on the Mobile Work Station (MDT/MRE) application(s).

Because of the MWS application and the information transmitted has been previously determined to be assessed as Protected "B", the ALPR information which is currently assessed Protected "A" will be treated as Protected "B" material. Albeit there are no personal identifiers, the photographs of the occupant(s) of the vehicle may be used for intelligence purposes.

10.1. Security and Confidentiality

10.1.1. All information and documentation provided to, collected by, delivered to or compiled by "E" Division Traffic Services, Major Crime/IMPACT or any other police users of ALPR in the performance of their duties and responsibilities shall be dealt with subject to and in accordance with Federal and Provincial Statutes, particularly the *Privacy Act*, R.S.C. 1985, c.P-21, the *Access to Information Act*, R.S.C. 1985, c. A-1, and the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165.

10.1.2. For the purposes of the *Access to Information Act, Privacy Act* and the *Freedom of Information and Protection of Privacy Act*, all records, work product, and information created in relation to ALPR are under the custody and control of the RCMP or the policing agency or integrated police agency originating the work.

10.1.3. User_ID's and Passwords complete with Entrust Tokens are already in place for RCMP members and will be acquired by the integrated policing agencies as an additional security measure. RCMP agencies use the Entrust token to access the PRIME-BC will also use the Entrust token in the operation of the mobile work station (MWS). This will add a protected layer to the ALPR process of information movement. USB External Storage Device (USB Thumb Drives are password protected.

10.2. Acceptable User Policy

10.2.1. Each user should acknowledge the policy and procedures in place for ALPR by sign-off.

RCMP OM 25.100 (E Div) - ALPR Policy
RCMP OM 25 Supplement (E Div) - ALPR Policy

This policy is provided on the reference disk

10.3. Automatic Log-off for Idle Workstations

Once the USB External Storage Device (USB Thumb Drive) is removed from the ALPR Unit and the buffer cleaned, automatic log-off is not a requirement. Should the USB External Storage Device (USB Thumb Drive) step be eliminated log-on and log-off procedures would become mandatory.

10.4. Role Based Access Control (RBAC) Authorization

ALPR used by agencies other than "E" Division Traffic Services or IMPACT requires approvals from "E" Division Traffic Services. Physical control is maintained for the download of information to the ALPR units with access controls for the vehicles, ALPR computers and USB External Storage Device (USB Thumb Drive). ALPR training is required prior to using the system.

10.5 Hardware Disposal Plan

ALPR computer units and the USB External Storage Device (USB Thumb Drive) will be disposed of in accordance with Government of Canada & RCMP Policy guidelines for disposal of government assets.

10.6 IT Incident Response Plan

A comprehensive incident response plan for handling computer security breaches is necessary. Security breaches are to be reported to the ALPR Policy Center, the "E" Division Traffic Services Branch in accordance with the Government of Canada/RCMP Security Manual, and the ALPR Policy and Procedures. ALPR approved Policy and Procedures have been made available to ALPR Users.

10.7 Maintain ALPR System Administration Authorizations and Profiles

There is no System Administrator (SA) profile for ALPR at this time. The SA position entails the defining of job roles, the activities that the role is allowed to perform and the information it is allowed to access.

The "E " Division Traffic Services SA will obtain and issue the User-ID's and Passwords which are required for the records management system (RMS) PRIME-BC and the MWS applications and they will already be in place when the MWS is used as the carrier for ALPR. As stated previously, any process changes to the system would include an addendum to the TRA/SOS and PIA.

10.8 Monitoring User Activities

Monitoring User Activities (especially the users and vendor(s) for maintenance and upgrades) is a means to prevent potential insider threats from advertent misuse of an IT system. Monitoring activities may be conducted at source by the technical support group for the system. There is sufficient training, quality assurance and policy in place detailing the requirements for access and use to address this issue. The users in effect may only use the equipment but any work performed is subject to scrutiny and not changeable by the users.

10.9 Need-to-Know / Right-to-Know Principles

Any police person or agency user of the ALPR system meets the need-to-know and right-to-know criteria of the information input into ALPR for the checks. The output, or any flagged information routed back to the server may be restricted on a need-to-know/right-to-know basis by virtue of the fact that any material where a file is opened may be designated information and "privatized" depending on the operational requirement.

10.10 Role Based Access Controls

Role based access controls are determined with the User Group Profiles created in the records management system, PRIME-BC, and will be used in the ALPR application. A TRA, SOS and PIA have been previously submitted on the PRIME-BC records management system.

10.11 Separation of Duties

Critical security relevant IT functions should require more than one administrator to complete. The creation of a new user, for example, should require one person to input the data and a second person to verify it. ALPR has a DBA, but separate IT personnel and this will provide needed separation. Also the DBA administrator for the ALPR application is separate from the SA for PRIME-BC.

11. Availability Requirements

The ALPR System is not mission critical to OCC dispatched operational policing requirements or response units. It is however used 7x24 and in the event of technical problems, an individual is available day or night:

Karl Hunter	Work: (604) 574-4062 or	s.19(1)

The maximum acceptable downtime (MAD) limitation is not applicable as the unit if necessary is taken out of service and replaced.

11.1 Change Management

The process outlining how changes or software updates to the ALPR Server and/or its associated software applications and USB External Storage Device (USB Thumb Drive) is not crucial as per above. RCMP Computer Services has dedicated staff to co-ordinate changes and software updates with the ALPR Users.

11.2 Control of Outsourced IT System Management

The RCMP retains IT Staff who maintain and service their systems. Outsourcing of IT System Management is not an issue.

11.3 Dynamic Connectivity Points

The connectivity points at present are the ALPR Server connection over the NPSN to the dedicated desk top computer in "E" Division Traffic Services. The USB External Storage Device (USB Thumb Drive) is inserted into the USB port on the desk top, and the update information downloaded. The USB External Storage Device (USB Thumb Drive) is then inserted into the ALPR portable computer in the vehicle for operational use. The USB External Storage Device (USB Thumb Drive) represents the storage medium for all incoming data to the mobile unit. At the end of a tour of duty the USB External Storage Device (USB Thumb Drive) is removed from the portable computer and returned to the designated employee for furtherance.

ALPR is an operational police system with limitations but there are no concerns as to any effects or impacts to the operating system.

__Note:__ In future when the USB External Storage Device (USB Thumb Drive) is replaced by a download of information via the MWS, there will be an additional point of connection. The end-to-end connections however will be over a closed network. Appropriate updates to the TRA/SOS and PIA will be provided.

11.4 System Back-Up Strategy

System Backup strategy is not an issue as ALPR is a first-line response operational police system. There is server back-up for the collected information; however, the USB External Storage Device (USB Thumb Drive) while in operational mode is not backed up.

11.5 ALPR Training

Although, ALPR is an intuitive application, training is mandatory and required (4 hours) for all personnel that will be using this system.

11.6 Secure Off-Site Storage of IT System Back-Ups

IT system backups should be stored securely off-site from the system and a minimum distance of ten miles.

11.7 Scheduled Maintenance

ALPR is not a mission critical system. Maintenance should be scheduled during off-peak hours so as not to interfere with normal operations.

11.8 Service Level Agreement

As the ALPR is not a mission critical system, a Service Level Agreement is not mandatory however conditions are set out as part of the PILOT / Production Environment Validation (PEV) of the ALPR Program.

11.9 Update the Disaster Recovery and Business Resumption Plans

See "11.6 Secure off-site storage of IT Systems Back-up".

11.10 Use of a Separate Development System

A separate development system is not crucial. This is a COTS Product and any changes or upgrades to the system will be completed and tested by the vendor / supplier prior to implementation. A separate development system for the RCMP is not an imperative requirement as this system is not first-line response "police operational".

12. Integrity Requirements

This is a new application to the RCMP and Police Agencies in British Columbia but has been used widely in Great Britain with success. When the download process is expanded to cover uploads and downloads, the ALPR and MWS applications will have to go through some stages of development to ensure a workable interface is in place. All work will be done by the RCMP Computer Services in the RCMP VPN. There will be no integrity issues.

12.1 "Closed Network"

The ALPR System(s) will operate on an in-house network that has no access to and from the Internet. The ALPR Server access is controlled through secure routers and firewalls and this will be extended to include the interface to run the ALPR data through the MWS. It is considered a "closed" network, therefore less exposed to threats from opened networks. See "Integrity Requirements".

12.2 Certification and Accreditation

Certification and Accreditation is a requirement of the Government of Canada Security Policy. Completing this process will ensure that all required security components are in the ALPR system.

12.3 Complete Audit Program

Logs are available on the Servers providing usage information. A system and application audit event will be generated for all security relevant IT processes, such as failed and successful connection attempts, creation of accounts, changes in account privileges etc. A comprehensive audit program allows a chronological record of system activities to enable review in order to provide evidence of user transactions and to act on any potential breaches of security. Logs should be reviewed on a regular basis. A log reduction tool will facilitate log review. Audit logs should be safely archived. The Prime-BC Privacy & Security Officer, together with the PRIME-BC Audit and Compliance Team, working in conjunction with DSB will be responsible for conducting such reviews once the MWS interface is in place.

12.4 Data Verification

"E" Division Traffic Services is responsible for the quality or verifying the integrity of the ALPR Information. "E" Division has hired a full time informatics employee and a full time program manger to make sure the quality and integrity of the ALPR information is maintained at all times. The investigator is responsible to validate and confirm any flagged information surfaced by the ALPR unit, generate an operational file and enter into a police investigation. After a file has been opened on PRIME-BC it becomes a PRIME-BC Audit and Compliance responsibility.

12.5 Defense-in-Depth Strategy

Defense-in-depth is having multiple overlapping layers of protection, such that an attacker would have to compromise several successive security controls to reach a target. ALPR has a Defense-in-depth strategy for the network boundary protection that will include use of secured routers, firewall layers, Virtual LAN, and PKI encryption upon implementation of the MWS interface. Until then, there are no technical or electronic points of attack.

12.6 Encryption – Network Traffic

The use of encryption to protect data in transit between the client and server is desirable and recommended with a PKI token or swipe card at the workstation and this may be implemented with the MWS interface. At this time the USB External Storage Device (USB Thumb Drive) are password protected.

12.7 File Integrity Software

File integrity software is in place in the application.

12.8 Hard Disk Encryption

The use of strong encryption is recommended to protect the ALPR or other sensitive information residing on ALPR Server and the functional desk top computer in the "E" Division Traffic Services. This can be realized with the full implementation of PKI / "Entrust" for all law enforcement agencies accessing PRIME-BC via desk top or MWS.

12.9 Integrity and Quality of Database

Due to the high level of integrity requirement with the extract information to be loaded on the ALPR Server(s), the originator of the information is responsible to ensure integrity and quality of the data in the ALPR databases. Once an operational file is opened, quality assurance by RCMP supervisory and records personnel and the PRIME-BC Audit and Compliance Team will ensure the information provided to PRIME-BC from ALPR is of a suitable standard.

12.10 Intrusion Detection System

The use of a network and/or host-based intrusion detection system to detect unauthorized access to ALPR network(s) and particularly critical servers is in place on the NPSN.

12.11 IT Equipment Maintenance Policy

Only authorized and approved ALPR service providers will be permitted to maintain ALPR equipment. Equipment is to be checked to ensure that no sensitive corporate information is present on hardware being sent off-site for maintenance. This policy may also require the contracted provider of the service to sign a non-disclosure agreement regarding any ALPR information that they may become privy to in the course of their duties.

12.12 Mandatory Use and Update of Approved Anti- Virus Software

RCMP notebook / laptop and desktop computers and computers accessing the network are compliant. This will include the ALPR application once it is interfaced and operated through the MWS. The USB External Storage Device (USB Thumb Drive) may be virus scanned when connected to a computer.

12.13 Network Vulnerability Scans / Penetration Testing

The security of the ALPR Server will be tested periodically through the running of network vulnerability scans, both internal and external, by authorized and DSB approved specialists. Penetration testing is the portion of security testing where the evaluators attempt to circumvent the security features of a system. Penetration testing results will indicate where the system is vulnerable. Appropriate actions will then be taken to mitigate the risk of any detected vulnerabilities.

12.14 "Pilot" (PEV) Phase

The ALPR Program has been operating in "Pilot" / Production Environment Validation (PEV) phase by "E" Division Traffic Services and IMPACT in the Lower Mainland area of British Columbia. Indications are that the program is successful and worth expanding to the major centers throughout "E" Division. The program has already demonstrated its value in identifying and prosecuting individuals that steal vehicles and to hold accountable those individuals that have lost their licenses and still continue to drive. Prohibited, suspended, unlicensed and uninsured drivers are a risk on our roadways and but the whole integrity of the vehicle licensing program in jeopardy.

12.15 Security Audit of ALPR Assets

The ALPR application software and hardware is under the care and control of "E" Division Traffic Services and the RCMP Inventory Accountability process will apply. It should be audited periodically to ensure that security policy is being followed. This audit would look for such things as the proper hardening of servers, workstations, authorized installation of software application and tools, proper procedure and policies are followed as well as virus signature update. Also physical and personnel security are verified for policy compliance.

This will be a job function of a full time resource that has been put in place within "E" Division Traffic Services and a full time informatics employee.

12.16 Secure Network Segment

The back end database is implemented within a secure network environment at RCMP "E" Division Headquarters in the Computer Services server area.

12.17 Secure Remote Access for Network

RCMP protocols are followed with respect to the Server Management and the download and upload of information to and from "E" Division Traffic Services. This will be extended with the implementation of the MWS interface. It is recommended that only encrypted and trusted channels for remote network management be used. This includes not only strong non-plain text authentication and session encryption but device access lists to prohibit access to management services except from trusted management stations. Moreover, apply best practices to secure management workstations and limit the number of personnel authorized to manage devices.

12.18 Site Inspection

Site inspection may be performed as part of the duties and responsibilities of the Audit and Compliance Team, Privacy and Security Team together with Departmental Security to provide assurance from a physical and operational security standpoint.

12.19 Tamper Resistant Logs

ALPR Logs for their systems are tamper resistant which provides for their security and integrity. The logs are written to only by the system and/or trusted processes. They may be viewed only by specific roles, namely, system administrators and auditors.

12.20 Use of Public Key Infrastructure (PKI)

The use of Public Key Infrastructure provides for strong authentication, encryption, digital signature and non-repudiation. PKI has been integrated into RCMP records centres on the Provincial PRIME-BC Server. Any access to the PRIME-BC data warehouse will require use of PKI. The MWS application requires use of an "Entrust" Token and when the ALPR interface to the MWS is completed, this will already be in place.

13. Risk Management Approach

A Threat and Risk Assessment update will be performed on ALPR when and if there are any significant changes to the ALPR application. This best practice will detect if any changes made to the system have increased the risk or, in the case of a periodic review with no changes in the system, if the class of threat has increased over time and requires additional safeguards to mitigate the risk.

14. Confidentiality Safeguards

It was determined that the ALPR infrastructure has the following existing confidentiality safeguards:

1. The infrastructure is designed for use by RCMP Computer Services and RCMP "E" Division Traffic Services and IMPACT. The ALPR application has no external connections to outside networks. Any future consideration to interface connection through the MWS to the NPSN will be protected using a firewall and encryption.

2. User authentication, name, password and security tokens are required at login to the MWS and will be in place when the interface is completed.

NOTE: An addendum to the Privacy Impact Assessment will be submitted, in the event there are any future changes with respect to the collection, use and disclosure of personal information which could impact on the *Privacy Act*, R.S.C. 1985, c.P-21, the *Access to Information Act*, R.S.C. 1985, c. A-1, and the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165.

14.1. Define User Responsibilities

User responsibilities make the user accountable for information security, including the technology. This is the responsibility of everyone who can affect the system security. To maintain accountability, user specific duties and responsibilities are defined by the Project Manager(s), and in addition, role based access controls will be in effect.

14.2 Password Management

Password management would include such things as validity time frame, reuse policy, triviality, maximum number of consecutive incorrect login attempts before the user is permanently locked out, non-use time out, need to maintain the confidentiality of, and length and character requirement. The password used to authenticate to ALPR will follow the Government of Canada and RCMP Security Policy. The ALPR application is resident on RCMP systems and capitalizes on existing security protocols.

14.3 Quality Assurance and Functional Testing

Quality Assurance and Functional Testing are part of the development phase of any system or application. The ALPR is new to the policing world in "E" Division and a relatively new technology. Before the interface to the MWS goes into production, there will be some validation testing, including the testing of security features, Entrust tokens and strong I&A will be performed.

14.4 Security Awareness Program

All ALPR users and managers are operational police personnel, and are well aware of their security responsibilities. A Security Awareness Program does refresh users' awareness of their security responsibilities and correct practices. Elements of security awareness program include behavior, accountability, awareness, training, education and implementation.

14.5 Use of Two-Factor Authentication

Two-factor authentication consists of a password (strong I & A) in conjunction with either a smart card, token or biometrics in order to strongly authenticate the privileged user.

15. Integrity Safeguards

It was determined that the ALPR infrastructure has the following existing integrity safeguards:

1. All ALPR activities are logged on the USB External Storage Device (USB Thumb Drive) or downloaded to the server via the MWS. The USB Thumb Drive is password protected.

2. File backups are made on a regular basis with the "Hits" and "Non Hits" stored on separate data bases.

16. Availability Safeguards

It was determined that the ALPR infrastructure has the following existing availability safeguards:

1. There is cross training of support personnel to ensure redundancy of resources.

2. The ALPR system will be backed up weekly.

3. There are hardware and software contracts in place to ensure proper availability of system components.

4. Uninterruptible Power Sources (UPS) are used on the servers and all other crucial systems in "E" Division RCMP HQ.

17. PRIVACY EVALUATION

Description of Personal Information Cluster	Collected by	Type of format (e.g. Paper, electronic)	Used by	Purpose of Collection	Disclosed to	Storage or Retention Site

Description of Personal Information Cluster	Collected by	Type of format (e.g. Paper, electronic)	Used by	Purpose of Collection	Disclosed to	Storage or Retention Site
Picture of vehicles (Hits only) and vehicle Plate (Hits and Non hits)	Police Officers, Designated employees	Both electronic and paper	Police Officers Courts, probation, corrections *	Law Enforcement	Law Enforcement Agencies Courts, probation, corrections * Others **	(See note)
Vehicle Location (GPS)	Police Officers, Designated employees	Both electronic and paper	Police Officers Courts, probation, corrections *	Law Enforcement	Law Enforcement Agencies Courts, probation, corrections * Others **	(See note)
Actions taken when vehicle is intercepted (type of charges laid or reason for lack of action)	Police Officers, Designated employees	Both electronic and paper	Police Officers Courts, probation, corrections *	Law Enforcement	Law Enforcement Agencies Courts, probation, corrections * Others **	(See note)

Description of Personal Information Cluster	Collected by	Type of format (e.g. Paper, electronic)	Used by	Purpose of Collection	Disclosed to	Storage or Retention Site
Date, Time stamp when the Picture of the plate and vehicle ("Hits" only) was taken	Police Officers, Designated employees	Both electronic and paper	Police Officers Courts, probation, corrections *	Law Enforcement	Law Enforcement Agencies Courts, probation, corrections * Others **	(See note)
Origin of information that created the hit (CPIC or ICBC)	Police Officers, Designated employees	Both electronic and paper	Police Officers Courts, probation, corrections *	Law Enforcement	Law Enforcement Agencies Courts, probation, corrections * Others **	(See note)

Courts of Criminal Jurisdiction (at trial)

****National Archives of Canada***

It must be noted that solely the information deemed to be of national historical significance according to the *Library and Archives of Canada Act* is disclosed to National Archives of Canada consistent with 8(2) *Privacy Act*.

****Statistics Canada***

Disclosure is consistent with 8(2) *Privacy Act*. See details in Appendices B and D.

*****Medical data***

See details on medical data under the current system page 51 of the PIA.

2. Privacy Analysis

Questionnaire "B" has been completed for the ALPR application; the (B) Cross-Jurisdictional Program and Service Delivery.

2.1. Questionnaire B: Cross Jurisdictional Program and Service Delivery

Privacy Act Principle 1: Accountability

Questions For Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
1.1 Has responsibility for the PIA been assigned? Please indicate in the details column the name And the position of the person responsible.	Yes			Responsibility for completion of the PIA has been given to the OIC "E" Division traffic Services, Supt Norm GAUMONT. The PIA responsibility lies with the OIC "E" Division Traffic Services.
1.2 Is a separate PIA being undertaken for each Jurisdictions		No		The RCMP completed PIAs for ALPR in accordance with Federal requirements. The Provincial Privacy Commissioner has responsibility for determination of a PIA. However in the past the Provincial Privacy Commissioner has been provided information from the PIA submitted to the Federal Privacy Commissioner to satisfy their requirements.
1.3 Has custody and or/control of personal information been determined for the cross jurisdictional electronic service delivery proposal and:	Yes			The RCMP is responsible for ensuring that all personal information collected and used by the RCMP is so done in accordance with Canadian Law, including but not restricted to the *Access to Information Act* and the *Privacy Act*. Any information entered on the ALPR is the responsibility of the agency that inputs the information or retains it in their O/RMS.
➢ Has the accountability of the jurisdictions and individuals in jurisdictions been documented for all privacy requirements?	Yes			All multi-jurisdictional interagency use of the ALPR will be under the conditions set out in the ALPR Policy and Procedures. Any transactions are logged. The non-RCMP Municipal Police will observe the *FOIPPA* and the RCMP will observe the *Privacy Act*. "E" Division traffic Services has put in place a full time program manager position to make sure policies and procedures are maintained.

Questions For Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
➢ Are the performance requirements of the jurisdictions comprehensively specified in a measurable way, and subject to specific performance or compliance reviews?	Yes			Policing requirements are legislated and set down by the Attorney General, Policies of Procedures and subject to Quality Reviews by the Audit and Compliance Team. The RCMP submits an Annual Report to Parliament on its performance with respect to Privacy in accordance to section 72 of the *Privacy Act*. Information obtained by/for RCMP personnel and will continue to be subject to the *Privacy Act*. Each agency is responsible for the input of its information. The AC Team and the Privacy & Security Officer for PRIME-BC; and Officer i/c RCMP Departmental Security is responsible to ensure appropriate security is in place for the data once the file is opened on PRIME-BC. The retention and disposal period of the information has not changed from the previous application and the RCMP manages disposal consistent with the *Privacy Act* and *Library and Archives of Canada Act (2004, c. 11)*. The non-RCMP Municipal Police Agencies manage and dispose of their information consistent with the *FOIPPA*.
➢ Where a jurisdiction and/or the private sector and is not subject to a privacy law, will an agreement or contract establish equivalent privacy requirements? If yes, is the agreement in place?			N/A	All jurisdictions using the ALPR information will fall under the Provincial or Federal privacy laws.
➢ Will each jurisdiction be provided with the results of regularly scheduled audits and compliance checks on the privacy practices of the cross-jurisdiction service delivery application?	Yes			"E" Division Traffic Services has created a full time position to make sure all policies and procedures as it relates to the ALPT program are being followed. Each participating Agency is subject to the Policy and Procedures for Prime-BC that set out the Quality Assurance requirements including independent audits by the Audit and Compliance Team(s) plus the Privacy and Security Team for PRIME-BC. In addition the RCMP conducts internal audits when required. The A&CT will follow the same schedule as RCMP Audit Teams and perform an Audit every four to five years. Should there be any concerns with an agency; the A&CT may conduct an audit at any time. Audits and quality assurance are set out in the PRIME-BC Policy and Procedures. A written report will be provided to the agency being audited.

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
1.4 Have legal opinions or policy advise been sought regarding:				
➢ The identification of privacy and other statutory requirements of each jurisdiction relating to the collection, use, disclosure, retention and disposal of personal information for the electronic service delivery proposal?	Yes			PIA - The data downloaded from CPIC, and ICBC drivers database consists of license plate numbers (alpha -numeric) with no personal identifiers. When a "Hit" confirmation is received a file is opened on the records management system (PRIME-BC) and personal information is obtained at that time. Personal identifiers may be collected and retained in the RMS, at the time the vehicle is stopped and the driver checked or for pre-existing data banks such as CPIC, PROS/PIRS, PRIME-BC, or ICBC driver database. There is no change to the information type being collected and the information falls within consistent use. RCMP Admin Manual AM III.12.D.1 refers On "Non hits" the picture of the vehicle plate only is retained and kept for 60 days. All queries must be authorized by the OIC "E" Division Traffic Services or his delegate and policy states there must be an ongoing investigation where the plates and associated personal information are already known. Therefore the ALPR database can only be used on non hits to identify a vehicle plate at a given location, date and time.
➢ The identification of any statutory requirements among jurisdictions and how the conflicts will be resolved?		No		Documented in the LEIP MOU, which was signed, and applicable Policy and Procedures in PRIME-BC.
➢ If required, the authority to transfer jurisdictional program delivery responsibilities to the cross-jurisdictional electronic service delivery application, including a consideration of the authority for the electronic service to collect, use, disclose or retain personal information as necessary on behalf of jurisdictions?			N/A	The RCMP will continue to maintain control and responsibility for their operational records and ALPR data. "E" Division Traffic Services and informatics is responsible to make sure information is being collected, use, retained or disclosed as per policies and existing guidelines.
➢ If required, the authority to alter or limit in any material way the collection, use or disclosure of personal information as authorized by jurisdictional program statutes and privacy laws for the purpose of delivering service through the cross-jurisdictional application?			N/A	The collection of information is limited by legislation; any disclosure of personal information cannot be done in the ALPR unless there is an ongoing investigation. This ALPR "Hit" information is moved to the records management system, PRIME-BC, and is subject to Federal and Provincial Legislation, plus policies, procedures and MOU's. On non hits, vehicle plate numbers only will be retained within the ALPR, they can only be queried if there is an ongoing investigation and the plate and associated personal information is already known.
➢ The identification of any requirements for statutory or program delegation?			N/A	

Questions for Analysis	*Yes*	*No*	*N/D Or N/A*	*Provide Details*
1.5 Has each jurisdiction identified all privacy policy requirements related to personal information and have conflicting requirements been resolved?	Yes			The RCMP has put in place strict policies on how the ALPR data can be queried and used. A full time position within "E" Division Traffic Services has been created to make sure policies and procedures are followed. On vehicle plates that initiates a hit, the plate and vehicle pictures are retained for court purposes and linkages to personal information is allowed as part of an ongoing investigation within the PRIME RMS. On "Non hits" no vehicle picture are retained, only the picture of the plate. There is no ability to query the ALPR database for a plate unless the investigator already has the plate and associated personal information as part of an ongoing investigation. Therefore on non hits the only information provided by the ALPR database will be a vehicle at a given place, date and time. The respective Policies and Procedures for how CPIC, ICBC driver's database and PRIME-BC data is to be used is already well established and guidelines in place.
1.6 Are the views of the Privacy Commissioner on the proposed cross-jurisdictional electronic service delivery proposal known? If yes, please provide specifics in details column.	Yes			The ALPR, PRIME-BC, CPIC and ICBC Driver's database can only be used for ongoing investigational purposes. The privacy Act provides for the sharing of information, "consistent use".
1.7 Have arrangements been made for transparent documented information systems so that individuals can be informed about how their personal information is collected, used and disclosed?			N/A	Provincially under the Personal Information Directory as per the *Freedom of Information and Privacy Act*, Sec. 69.2

Questions for Analysis	Yes	No	N/D Or N/A	Provide Details
1.8 Have arrangements been made for independent audit, compliance and enforcement mechanisms for the cross-jurisdictional electronic delivery of services, including fulfillment of the commitments in the PIA process?	Yes			A full time position has been created within "E" Division traffic Services to make sure all policies and procedures as it relates to the ALPR program is being followed. RCMP has internal auditors who conduct audits as required. PRIME-BC, CPIC and ICBC drivers database Policy and Procedures set out the authority and responsibility of the Audit and Compliance Team.
1.9 Does the cross-jurisdictional electronic service delivery proposal entail a privacy risk because accountability for and/or compliance with existing privacy requirements will be diminished?		No		On non hits vehicle, vehicle plate picture are being retained only and there is no ability to query the ALPR database unless an investigator has an ongoing investigation with the vehicle plate and associated personal information already. All queries must be authorized by the OIC "E" Division Traffic Services or his delegate. On hits the plate and vehicle pictures are retained and linked to personal information only for investigation purposes and court. The PRIME RMS is used to link the plate with any personal information. No personal information is linked to the plate number within the ALPR database.
1.10 Have privacy law and other statutory and policy conflicts among jurisdictions been resolved?	Yes			The management of the ALPR is under "E" Division Traffic Services. Strict guidelines have been put in place as it relates to "Non hits". Plate numbers only are retained there is no ability to identify the drivers of these vehicles since vehicle pictures are not retained. Policy prohibits the query of non hits unless the investigator already has an ongoing investigation and a suspect plate and the associated personal information. The ALPR database will only provide a vehicle plate number , location, date and time where that plate was seen. On "Hit" information entered on PRIME-BC and PRIME-BC Policy and Procedures apply to both external RCMP Police Agencies and the RCMP and are consistent with the RCMP CCAPS Policy. The LEIP MOU can be used for conflict resolution together with the Policy and Procedures and submissions to the PRIME-BC Governing Council.
1.11 Where appropriate, have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the cross-jurisdictional electronic delivery of services proposal?	Yes			All key stakeholders are either represented or are members of the IMPACT, the Integrated Traffic Unit or, PRIME-BC. Views of the stakeholders are known, through their representation and participation in IMPACT and the Integrated Traffic Units and identified acceptance of the Policy and Procedures for ALPR and PRIME-BC. As such, privacy protection considerations represented one of the key areas in the system development.
1.12 Where appropriate, will public consultation take placed on the privacy risks and the plans for resolution?	Yes			"E Division traffic Services and the Province of British Columbia will be doing media events outlining how privacy concerns have been dealt with and providing general information on the program. Information on the ALPR program is being put on both the RCMP "E" Division Traffic Services and the Government web site.
1.13 Is there an Agreement that details each jurisdiction's responsibilities in relation to the cross-jurisdictional electronic delivery of services proposal and Privacy?	Yes			Only after a "Hit" confirmation causes a file to be opened on the records management system, PRIME-BC. Thus the Charter and Governance Model for PRIME-BC, and the Policy and Procedures for Prime-BC, together with the MOU for sharing of information address this issue. On non-hit data there must be an ongoing investigation where the plate and associated personal information is known. Therefore the only information available within the ALPR for non hits is the plate number, location,date and time where the plate was seen.

Privacy Act Principle 2: Identifying Purposes

Questions For Analysis	***Yes***	***No***	***N/D or N/A***	***Provide Details***
2.1 What are the specific authorities to collect personal information? If your authority is questionable then you need to consult your legal advice as to whether you have the authority to proceed with this proposal.				There are three distinct authorities: *Criminal Code of Canada, Identification of Criminals Act* and Common Law power of police officer to collect information and via the legislative and common law duties, the collection of information is necessarily incidental to meeting these obligations.
2.2 Has a clear relationship been established between the personal information to be collected and the cross-jurisdictional service delivery proposal's functional and operational requirements?	Yes			The use of the ALPR system is limited to photographing vehicles, either moving and/or stationary. No personal information is recorded during the ALPR operation. Sufficient information is obtained to further the investigation as required. Further clarification is found in the Policy & Procedures for ALPR. Information is collected as per CMP PPU 005.
2.3 Have the purposes for which the personal information is collected been documented among jurisdictions?	Yes			The RCMP is collecting the information for the detection, prevention and suppression of crime. While most information is collected directly, ALPR information is collected directly through the photo and indirectly from other sources when follow up is required. It is consistent with InfoSource, specifically Operational Case Records Bank CMP PPU 005. The nature of police investigations requires confidentiality, secrecy and impartiality. ALPR is a publicized program in British Columbia and the public identities remain anonymous unless follow-up investigation is required for a "Hit" response.
2.4 Have the notice provisions among the jurisdictions been reconciled and have jurisdictional exceptions to the notice provision been identified and reconciled?	Yes			As described in InfoSource, Operational Case Records Bank CMP PPU 005 for the RCMP; the Personal Information Directory as per Sec. 69.2 B.C. *Freedom of Information and Privacy Act*; and through ALPR Policy and Procedures. Traffic Services operate inter-agency units made up of RCMP and Municipal Police members. Notice provisions do not apply to the ALPR as the investigative information is transferred from ALPR through transcription to the PRIME-BC Server(s).
2.5 Have all options to minimize the routine collection of personal information been considered?	Yes			Police work is in the business of collecting limited and specific information. InfoSource Operational Case Records Bank CMP PPU 005 refers. Yes – Unless there is a "Hit", personal information is not collected until a file is opened in the records management system, PRIME-BC, and the ALPR Information is processed through transcription into the RMS
2.6 If personal information that has been collected is to be used for a purpose not previously identified, is consent required?		No		No – when disclosure is consistent with InfoSource, Operational Case Records Bank CMP PPU 005; Section 7 and 8 of the *Privacy Act*; and Provincially Sec 32 of *FOIPPA*. (B.C. *Freedom of Information Protection of Privacy Act*) as indicated in the Provincial PIA for PRIME-BC.
2.7 Have arrangements been made to provide full disclosure of the purposes for which personal information is collected?		No		PIB 005 refers. Any disclosure is in accordance with the Access to Information requests both at a Federal and Provincial Level.

Discussion Points:

Privacy Act Principle 3: Consent

Questions For Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
3.1 Is consent obtained directly from the individual? If not, why not?		No		The RCMP is collecting the information for the detection, prevention and suppression of crime. While most information is collected directly, some information is collected indirectly; consistent with InfoSource, Operational Case Records Bank CMP PPU 005 refers. The nature of police investigations requires confidentiality, secrecy and impartiality. Informing the respondent of the collection could jeopardize an investigation.
3.2 How is consent obtained?			N/A	The RCMP is collecting the information for the detection, prevention and suppression of crime. This information is required to investigate stolen vehicles, prohibited, suspended, unlicensed and uninsured drivers and serious Criminal investigations. On Non hits the data is required as part of ongoing serious criminal investigation although this is limited to plate numbers only at given location, date and time. Vehicle pictures are not retained on non hits and investigators must have a suspect vehicle and associated personal information prior to querying the ALPR database. The non hits are kept for 60 days only. The retention limits and policies have been put in place to balance public privacy and the needs to apprehend serious criminal offenders.
3.2 Does the cross-jurisdictional proposal require an individual's consent to collect, use and/or disclose personal information, and if so, have jurisdictional differences been reconciled?		No		There are no jurisdictional differences in the collection of information in the ALPR.
3.3 Does consent require a positive action by an individual rather than being assumed as a default? s. 5, 7 & 8		No		The RCMP is collecting the information for the detection, prevention and suppression of crime under criminal and provincial statute.
3.4 Where personal information is collected indirectly, is it necessary to obtain consent from the individual to who the information pertains by either the jurisdiction collecting indirectly or the jurisdiction disclosing the information?		No		The RCMP is collecting the information for the detection, prevention and suppression of crime.
3.6 Does the proposal envision possible secondary uses for the personal information collected, and if so, do any jurisdictional consent requirements have to be reconciled?		No		No – there is no proposal for secondary use. All information will be used as part of an ongoing investigation or the initiation of a new investigation.
3.7 Can an individual refuse to consent to the collection or use of personal information for a secondary purpose, unless required by law?		No		The use of limited and specific personal information will be consistent with PIB CMP PPU 005 and all other secondary uses not consistent with the PIB will be reported to the OPC as required by the *Privacy Act* (*PA*).

Page(s) 000062 to\à 000062

Is(Are) exempted pursuant to section(s)
est(sont) exemptée(s) en vertu de(s)(l')article(s)

22(1)(a)(i)

of the Privacy Act
de la Loi sur la protection des renseignements personnels

Privacy Act Principle 4: Use of Personal Information

Questions For Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
4.1 Does the cross-jurisdictional proposal require the collection of more personal information that was previously collected by each jurisdiction?		No		The same information is being gathered regardless of the cross-jurisdictional agency.
4.2 Will individuals be monitored for Quality assurance or security, and if so, will personal information be collected?	Yes			"E" Division Traffic Services has a full time program manager to make sure quality assurance and security is being followed. A's part of the Quality assurance process no personal information will be collected.
4.3 If required, has each jurisdiction identified the authority for the collection of personal information on their behalf?	Yes			The RCMP is authorized to gather personal information as part of ongoing Criminal Code of Canada investigations, *Identification of Criminals Act*, or Provincial Statute investigations. Provincially the authorization is the same under the *Criminal Code of Canada* and *Identification of Criminals Act* and as per the *FOIPPA*. Restrictions have been put on Non Hits to balance privacy concerns and the needs for information to solve serious crimes such as murders and sexual assaults. On Non hits, pictures of the plates only will be retained for 60 days only. To query the ALPR database an ongoing serious investigation with a suspect plate and associated personal information must be provided. Therefore the only added information provided to the investigators will be a vehicle plate at a given location, with a date and time.
4.4 Will measures be taken to ensure public confidence in the privacy practices related to the service when personal information that individuals are likely to consider highly sensitive is collected?			N/A	No highly sensitive information is being collected.

Discussion Points:

Privacy Act Principle 5: Limiting User, Disclosure, and Retention

Questions For Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
5.1 What are the specific authorities to use personal information? If your authority is questionable, then you need to consult your legal advisor as to whether you have the authority to proceed with this proposal.				Authority is provided under "consistent use" in the *Privacy Act.* The collections are authorized by the *Criminal Code of Canada, Identification of Criminals Act* and the common law powers of police officers in order to fulfill their common law duties of the preservation of the peace, the prevention of crime and the protection of life and property.
5.2 Is personal information used exclusively for the identified purposes and for uses that an individual would reasonably consider consistent with those purposes?	Yes			The use of the information falls within "consistent use" under the *Privacy Act.* Information within the ALPR database is kept to a minimum and the information can only be queried if there is an ongoing criminal or provincial statue investigations. On Non-hits and suspect vehicle and associated personal information must be provided before a query is make in the ALPR database and the investigation must be for a serious Criminal Code offence.
5.3 Are the uses of information limited to what a reasonable person would consider appropriate in the circumstances?	Yes			Police investigations fall within "consistent use" under the *Privacy Act.*
5.4 Are personal identifiers, such as the social insurance number, used for the purposes of linking across multiple databases?	Yes			The only personal identifier information used is the vehicle plate number within the ALPR database. On Hits this is consistent use under the Privacy Act. On Non hits severe restriction have been put in place to make sure privacy concerns are balanced with the need for information to solve serious crimes. Plate pictures only are retained therefore there is no ability to identify the driver under any circumstances. The vehicle plate can only be queried if the plate and associated personal information is already known as part of an ongoing serious criminal code investigation.
5.5 Where data linkages such as data matching or profiling occur, are they consistent with the stated purposes for which the personal information is collected?	Yes			Police investigations fall within "consistent use" under the *Privacy Act.* There will be no profiling.
5.6 Do jurisdictional data matching or data profiling policies require the conduct of a formal assessment and/or a review by the Privacy Commissioner?		No		
5.7 Is there a need to reconcile among jurisdictions the length of time records of personal information are retained?		No		ALPR Information for all designated users is held on the servers at "E" Division HQ and purged after sixty days unless there is a "Hit". The non hit information is limited to the picture of the plate only. The vehicle picture is deleted for non hits. On "Hits", the ALPR information is used to generate an occurrence and transcribed to the official occurrence / records management system, PRIME-BC. The partnering agencies agree with the retention period and conditions already set under Federal and Provincial policies and legislation. All PRIME-BC users adhere to the PRIME-BC Policy and Procedures and a standard retention period. PRIME-BC records are subject of review by the PRIME-BC Audit and Compliance Team.

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
5.8 Will personal information be processed, disclosed or retained outside of Canada?	Yes			ALPR is within a closed network with no external sharing. When information is transferred to the RMS (PRIME-BC) through transcription, information sharing within Canada is already subject of a MOU. Eventually information may be shared, disclosed and retained internationally only in accordance with the signing of an International MOU agreeing to the conditions of the MOU and the Policy and Procedures set for Prime-BC, which is consistent with Treasury Board and RCMP Policy, as well as Federal and Provincial Statutes and policies.
5.9 What are the specific authorities to disclose personal information? If your authority is questionable, then you need to consult your legal advisor as to whether you have the authority to proceed with this proposal.				InfoSource, Operational Case Records Bank CMP PPU 005 and Section 8 of the *Privacy Act* refers.
5.10 If required, is there a cross-jurisdictional procedure to govern the destruction of personal information?	Yes			Under the provisions of the formalized MOU for LEIP, which binds parties to the PRIME-BC Policy and Procedures, all agencies agree with the retention period / schedules and conditions already set under Federal and Provincial policies and legislation.
5.11 If personal information is to be used for a new purpose, is the new purpose authorized and documented?	Yes			Refer to Section 3.7.
5.12 Is there a need for a cross-jurisdictional agreement if data matching or data profiling is proposed as part of the electronic service delivery proposal?		No		The only data matching in the ALPR is to license plate numbers. InfoSource, Operational Case Records Bank CMP PPU 005 refers. A formalized MOU is in place.
5.13 Do you have an Agreement in place that covers data matching or data profiling activities?	Yes			The only data matching in the ALPR is to license plate numbers. InfoSource, Operational Case Records Bank CMP PPU 005 refers. A formalized MOU is in place
5.14 Are any limitations on the use and disclosure of personal information set out in law or policy reinforced by the information and information technology architecture of the information technology architecture of the information systems?	Yes			Within the IM/IT systems, Release Tracking, Audit logs, Quality Assurance, Automated Built-in System edits and Business Rules, random reviews, and scheduled audits etc. represent functionality to monitor and track information transfer.

Discussion Points:

Ref: 5.4 – The linkages occur during CPIC and Motor Vehicle Branch queries conducted on the ALPR through the CPIC functionality. Any other personal identifiers are in the O/RMS PRIME-BC, and not in the ALPR.

Privacy Act Principle 6: Accuracy of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
6.1 Will steps be taken to ensure that the personal information is accurate, complete and up-to-date? s. 6(2)	Yes			The ALPR information is obtained through CPIC and the Motor Vehicle branch. If there is a "Hit", the information is verified and an occurrence is opened then transcribed to the RMS (PRIME-BC) which is designed to allow data entry and correction of personal information at the point of contact (i.e. law enforcement personnel), thus ensuring that information in the system is accurate, complete and up-to-date. Additionally, PRIME-BC will be subject to data integrity audits.
6.2 Is a record kept of the source of the information used to make changes, e.g. paper or transaction records?	Yes			Both CPIC and the Motor Vehicle Branch information is subject to Time/Date/User Stamp, Audit Log, "RMS Release Tracking", records all transactions, including the source.
6.3 Where applicable, is there a procedure, automatically or at the request of an individual, to provide notices of correction to third parties to whom personal information has been previously disclosed? S. 12(2)(c)?		No		There is no procedure in place to "notify" third parties of a correction. Core information is from databases external to ALPR and any correction would be done in the originating system: Motor Vehicle Branch, CPIC and subsequently in the O/RMS (PRIME-BC). In support of this, no enforcement action is to be taken on the information unless validated by the originating agency. However, all corrections will be flagged on the electronic records management file in PRIME-BC, so any third party with access to PRIME-BC will also access the new information or correction.
6.4 Have cross-jurisdictional responsibilities for accuracy been identified?	Yes			There is one process in place across all jurisdiction on how the information is stored and accessed.
6.5 Have any cross-jurisdictional differences in accuracy requirements been identified and reconciled?	Yes			There is a common Policy in place to govern the use of ALPR used by all Police Agencies. In addition to the common standard (PRIME-BC Reference Standard), Electronic Caveat Messaging within the system and the MOU dictates no enforcement action is to be taken on the information unless validated by the originating agency.
6.6 Is there a record of decisions and reasons for refusing a request to correct a record of personal information?	Yes			Electronic audit trail will provide an electronic chronology of all additions, modifications and deletions to the information. Requests for review of errors or omissions & corrections will be recorded as a supplement to the ALPR file in PRIME-BC.
6.7 Is there a clearly defined process by which an individual may access, assess and discuss or dispute the accuracy of the record? Please briefly describe the steps.	Yes			Request under the *Access to Information Act / Freedom of Information and Protection of Privacy Act / Privacy Acts* permits access through the RCMP ATIP authority or the Provincial Privacy Authority under *FOIPPA* as described in the information banks published in InfoSource and the Provincial Personal Information Directory.

Privacy Act Principle 7: Safeguards

Questions For Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
7.1 Has a Threat and Risk Assessment been completed?	Yes			A Threat Risk Assessment has been completed and signed off by RCMP Departmental Security on ALPR.
7.2 Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented with cross-jurisdictional conflicts identified and reconciled?	Yes			The ALPR Server is located in RCMP "E" Division Headquarters and the non-hit information is only kept ninety days before being purged. "Hit" Information is kept two years on the ALPR Servers but the information from the "Hit" is made subject of a General Occurrence (GO) in the records management system (Prime-BC). Security requirements for the collection, use, disclosure and storage of personal information are governed by the GOC Security Policy, by the policy on Privacy and Data Protection and ALPR Policy and the Prime-BC Policy and Procedures Manual. The RCMP and British Columbia Police Agencies have agreed to follow the requirements outlined therein.
7.3 Are staff of the electronic delivery service trained in the requirements for protecting personal information and are they aware of the relevant policies regarding breaches of security or confidentiality?	Yes			The ALPR program coordinator with "E" Division traffic Services as well as the Informatics employee that will be overseeing the database are well aware of the Privacy Act and the need to properly protect personal information from unauthorized disclosure. "E" Division Traffic Services assumes responsibility for ensuring that these standards are upheld and that breaches of security or confidentiality are reported and investigated. DSB provides and has made available information and guidelines on the protection and handling of personal information. Security requirements for the collection, use, disclosure and storage of personal information are governed by the GOC Security Policy, by the policy on Privacy and Data Protection and the ALPR Policy and Prime-BC Policy and Procedures Manual. The RCMP ATIP Branch, upon request of the PCO may assist the PCO with investigations of any breach of privacy. Municipal Police are governed by the ALPR Policy and requirements under *FOIPPA*. Security requirements are also outlined in the Policy and Procedures for PRIME-BC.

Questions for Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
7.4 Are there controls in place for any process to grant authorization to modify (add, change or delete) personal information from records?	Yes			ALPR information is downloaded from CPIC or the ICBC Driver's database and cannot be modified, or changed. Information is deleted as per existing policies. Non-hits are deleted every 60 days and Hits are kept for two years or as per a records management, PRIME-BC occurrence. *Note: Should a broadcast be received from the Operational Communications Centre (OCC) with respect to new: amber alert, the ALPR user may key in the license plate(s) to the ALPR terminal. The data keyed is alpha-numeric license plate numbers only.* After ALPR Information is made subject of a records management, PRIME-BC occurrence, Tables of Authority designating rights to add, change, amend or delete information are given on a "need-to" basis dependent on job description/ requirement. Any changes are electronically recorded via electronic audit trail with the date, time and User_ID of the employee making the change(s). This applies to all, RCMP and Municipal Police Agencies. Access to specific information is managed by custom-built "role based access control" functionality within the system. The role based access control system links to the users Entrust credentials and assigned roles. Credentials are stored on approved hardware tokens and are accessed by a password. This guarantees a two factor authentication for RCMP Members. ("**Something you know** e.g. a PIN and **something you own** e.g. a token"). RCMP authorized staff have access on a "need to know" and "right to know" basis only. "Hit" information from the ALPR is transferred to the O/RMS, where the retention of information is compliant with the *Privacy Act* (Federal and Provincial) depending on agency and the *Library and Archives of Canada Act.*
7.5 Is the system designed so that access and changes to personal information can be audited by date and user identification?	Yes			ALPR information is stored in the system with a date/time stamp and when a "Hit" causes a general occurrence to be created in PRIME-BC, user identification is recorded as to who has created/modified or viewed the information. The user ID and date/time stamp will indicate the last update.
7.6 Are user accounts, access rights and security authorizations controlled by a system or record management process?	Yes			Access rights to ALPR database are not granted to the User's. *Note: Should a broadcast be received from the Operational Communications Centre (OCC) with respect to new: amber alert, the ALPR user may key in the license plate(s) to the ALPR terminal.* The data keyed is alpha-numeric license plate numbers only. Otherwise, the information is preloaded into the ALPR from a USB External Storage Device (USB Thumb Drive). At day's end the USB External Storage Device (USB Thumb Drive) is removed from the ALPR unit and downloaded to the ALPR Server(s). Refer to 7.4

Questions for Analysis	Yes	No	N/D or N/A	Provide Details
7.7 Is user access to personal information limited only that required to discharge assigned functions?	Yes			The only personal information stored in the ALPR database in the vehicle plate number. Only informatics personnel have the right to delete information in the database based on exiting retention policies. Police officers based on a "Hit" on a vehicle license plate number can open a file and link personal information to the license plate as part of an ongoing investigation. A file is opened in the records management system, PRIME-BC. For PRIME-BC the System Administrator through the Tables of Authority designates rights to add, change, amend or delete information are given on a "need to" basis dependent on job description. Any changes are electronically recorded via electronic audit trail with the date, time and User_ID of the employee making the change(s). This applies to all, RCMP and Municipal Police Agencies. Access to specific information is managed by a custom-built role based access control system. The role based access control system links to the users Entrust credentials and assigned roles. Credentials are stored on approved hardware tokens and are accessed by a password. This guarantees two factor authentications ("**Something you know** e.g. a PIN and **something you own** e.g. a token"). RCMP authorized staff gets access on a "need-to-know, right-to-know" basis only.
7.8 Are there contingency plans and documented procedures in place to identify security breaches or disclosures of personal information in error?	Yes			There are policies in place to make sure the license plate number can only be linked to personal inofmration as part of an ingoing investigation. After "Hit" information is entered onto PRIME-BC electronic tracking mechanisms are in place within the systems, and ALPR and PRIME-BC and Policy and Procedures address security breaches and erroneous disclosures of personal information. All security breaches or disclosures of personal information whether in error or not are subject to Security Incident Reports. The ALPR information is not a "record", and as indicated previously, the ALPR information is transferred to the O/RMS where there is physical security for any written/electronic records and physical security for the database server for the O/RMS. On Non-Hits severe restriction have been put in place on the collection and query of this data. The plate picture only is retained for only 60 days. To query a license plate the investigator must have a serious criminal code violation and already have the plate and associated personal information before a query can be made within the ALPR database. Therefore on Non-Hits the only information provided is a vehicle plate at a given location with and date and time. The ALPR database cannot be the initial link to personal information this has to have been done on an ongoing investigation prior to the query. Ther eis no ability to link the plate to the driver since the vehicle picture is not retained. The Program mangers and informatics employee are well aware of the procedures and all Qeries must be authorized by the OIC "E" Division Traffic Services or his delegate.
7.9 Are there documented procedures in place to communicate security violations to jurisdictions, data subjects and if appropriate law enforcement authorities?	Yes			Refer to 7.4
7.10 If sensitive personal information will be used in the electronic delivery of services, have technological tools and system design techniques been considered which may enhance both privacy and security, e.g. encryption, technologies of anonymity or pseudo- anonymity or digital signatures?	Yes			On plate numbers only are kept within the ALPR database. No linkage to personal information is made within the database. Only after the ALPR "Hit" information is made subject to a General Occurrence in PRIME-BC. After entry into PRIME-BC, role based access controls, levels of access controls (drilling down into the data), "Need to Know" and "Right to Know" criteria, User_ID and Passwords are used. PKI token authentication, firewalls, and private network ensure system security, integrity and data protection and this is the target for the entire end-to-end system and will be the case when and if the ALPR information is processed via the MWS applications. The TRA together with the SOS and Interview Guide have been forwarded to Departmental Security for review.
7.11 Have criteria been established for determining and authorizing "need to know" access to personal information?	Yes			Within the ALPR database plate numbers only are allowed. No linkage to private information is allowed within the database unless a hit is recorded. At the time personal information is retained within the PRIME RMS.

Privacy Act Principle 8: Openness

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
8.1 Describe how the results of any privacy impact assessment or audit will be made available to the public.				All audits are publicly available as per Treasury Board guidelines and vetted PIA Executive Media "Summary" has been provided to ATIP, and once forwarded to PCO may be placed on website.
8.2 Will the cross-jurisdictional electronic Service delivery project make available information on policies and practices related to the management and handling of personal information, including how personal information is used and how access is provided to the individual?	Yes			Not outside the law enforcement community, however policies and practices may be made available consistent with the exemptions in the *Access to Information Act*. The RCMP AM III.11 and AM III.12 are available to the public and provide explanations on the management and handling of personal info as well as TB InfoSource which describes all the RCMP PIBs.
8.3 Where applicable, have jurisdictional Directories of Records (or equivalent) been updated?			N/A	The Government of British Columbia does have the "Personal Information Directory" which is similar to InfoSource but research on the Internet indicates that this directory has not been updated recently.
8.4 Have communications products and/or a communications plan been developed to fully explain to the public how their personal information will be managed, including how it will be protected, as part of the cross-jurisdictional electronic delivery of services proposal?		No		"E" Division Traffic Services and Police Services are both in the process of adding the ALPR study on their web sites explaining the benefits of the ALPR program and the type of information that is retained. The RCMP will be making public announcement once the new ALPR system is identified and purchased. There has been no change in the management or protection of personal information.

Discussion Points:

Privacy Act Principle 9: Individual's Access to Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
9.1 Is the system designed to ensure that access by an individual to all of their personal information can be achieved with minimal disruption to operations?	Yes	No		Individuals may make a request to access their personal information through ATIP but will not have direct access to the ALPR as it is a closed environment. Designated police personnel only have access and only through role based access controls. All ALPR "Hit" information is made subject of a file in the O/RMS. ATIP as a concurrent user can access the system data in PRIME-BC, which receives all the ALPR "Hit" data, without affecting operations. Release Tracking in the O/RMS logs the transactions for any disclosed information.
9.2 Has the cross-jurisdictional service delivery project documented how requests for personal information covered or not covered by a privacy law will be processed?		No		"As per TB Guide Lines Informal Access may be considered." The information is entered into the ALPR and if a "Hit" is received, it is then transferred to the O/RMS and is the responsibility of the agency that generates the general occurrence in the RMS (PRIME-BC). Any requests for information involving a non-RCMP jurisdiction will be processed through the Provincial FOIPPA Offices and all requests for RCMP information are referred to ATIP. The Policy and Procedures for PRIME-BC covers record responsibility and disclosure.
9.3 Are there documented procedures developed or planned on how to initiate privacy request of request for the correction of personal information?	Yes			Only after the ALPR "Hit" information is moved into the O/RMS, then "As per TB Guide Lines Informal Access may be considered." The information entered into the ALPR and then transferred to the O/RMS is proprietary to the agency for which the information was taken. Any requests for information involving a non-RCMP jurisdiction will be processed through the Provincial FOIPPA Offices and all requests for RCMP information are referred to ATIP. The Policy and Procedures for PRIME-BC covers record responsibility and disclosure.
9.4 Are the individual's access rights assured for all the data sets of all the parties in the information life cycle, including each jurisdiction, private sector partners and/or complaint procedures?	Yes			Only the ALPR "Hit" information is moved into a records management, PRIME-BC, file; then as per the *Privacy Act*. Should an individual submit an access request to ATIP and the file information contains information from a non-RCMP Provincial jurisdiction, PRIME-BC policy places the onus on the releasing agency (RCMP) to send written notification to the provincial police agency that their information could be disclosed under the *Privacy Act*. It is up to the originating agency at that point to respond with any objections.
9.5 Are all custodians aware of the cross-jurisdictional service delivery practices regarding the individual's right of access and any requirement to advise the individual of formal and informal appeal and/or complaint procedures?	Yes			Federal and Provincial legislation, policies and procedures. Should individuals apply for access to information to the wrong Privacy Office; the Privacy authority will direct them appropriately. Response from the RCMP ATIP authority would be in the format they deem appropriate.
9.6 Have procedures been established to provide individuals with access in a "routine" manner to their personal information collected by the cross-jurisdictional service delivery project?	Yes			Refer to Section 9.2

Discussion Points:

Privacy Act Principle 10: Challenging Compliance

Questions For Analysis	*Yes*	*No*	*N/D or N/A*	*Provide Details*
10.1 Are complaint and/or appeal procedures established for the cross-jurisdictional electronic service delivery proposal including the identification and resolution of any jurisdictional privacy law complaint and/or appeal conflicts?	Yes			The *Privacy Act* and the Policy on Privacy and Data Protection establishes the procedures for complaints and appeals. "The RCMP ATIP Branch upon request of the PCO may assist the PCO with investigation of any breach of privacy." Procedures for the non-RCMP municipal Police are established under the *FOIPPA* and processed through the Provincial Privacy Office.
10.2 Has a procedure been established to log and periodically review complaints and their resolution with a view to establishing improved information management practices and standards?	Yes			This procedure will be performed during the Privacy, Security, Quality Assurance and Compliancy Reviews by the PRIME-BC Audit and Compliance Team, and the PRIME-BC Privacy and Security Team; and on a regular basis by the supervisory quality assurance of material prior to passing through transcription to the O/RMS. This also forms part of the product enhancement process for all the vendor clientele.
10.3 Have independent privacy oversight and review mechanisms been established for the cross-jurisdictional service delivery proposal?	Yes			The PRIME-BC Privacy and Security Team together with the National RCMP Audit and Evaluation may initiate audits as requested. The PRIME-BC Policy and Procedures provides a Quality Assurance and accountability process.
10.4 Have oversight agencies, including privacy commissioners, issued reports or opinions on issues that would be relevant to the cross-jurisdictional electronic service delivery proposal? If yes, please provide a summary of the above in the details column and append to the final report.			N/A	

Discussion Points:

18. PRIVACY RISK MANAGEMENT PLAN

The privacy issues and/or risks identified in this report are described below. Reference number refers to the question number and discussion in the Privacy Analysis Questionnaire contained in section 17 of this PIA.

The ALPR "receiver" of CPIC and Motor Vehicle Branch (electronic) information and after photographing license plates, runs them against the CPIC and ICBC Information and is a "collector" for investigative information for various police agencies. Police agency personnel are able to check a high volume of license plate numbers in a short period of time, allowing peace officers to spend more time on the road, visible to the public. ALPR users automatically query license plates and run them against the downloaded resource information from CPIC or ICBC Driver's databases. This will assist the police to be more effective and efficient and help the public to have safer communities.

18.1 Privacy Risk Mitigation

18.1.1 Unclear Control of Personal Information (1.2; 1.5; 1.6)

Information from the ALPR in the form of data information is moved from the ALPR environment through to the ALPR Servers. When a "Hit" occurs, a general occurrence is opened in PRIME-BC and the information moved from a transcription queue to the O/RMS, PRIME-BC. It is an integrated database (repository), the Police O/RMS for British Columbia, where all necessary law enforcement data can be entered, electronically queried and ultimately shared with law enforcement partners in their crime prevention and crime fighting roles. From an operational perspective, the RCMP has both custody and control of personal information while that information is resident in both the ALPR, in PRIME-BC and MNI, and extracts information contributed to the NIII (IQT/PIP). The RCMP currently controls the access to its current system (PIRS/PROS/PRIME-BC) through MOU commensurate with security access control. The ALPR application does not hold or store any personal information until a "Hit" occurs. After this, the ALPR information is the commencement of the generation of an occurrence in the PRIME-BC or O/RMS. The RCMP intends to continue exercising any control over personal information disclosure to any law enforcement partners who may opt for accessing PRIME-BC in the future, and has developed a MOU for this purpose. The MOU between the RCMP and other law enforcement agencies would be a method of identifying any aspects of RCMP control over personal information disclosed to them. This Memorandum of Understanding is a useful vehicle that describes the responsibilities of the parties. The MOU addresses topics such as:

- Authorities that allow any sharing of personal information in the future.
- Access privileges.
- Responsibilities from an RCMP point of view on the program custodian.
- Feedback and audit of access privileges to other law enforcement agencies.
- Restrictions on use of personal information.
- Restrictions on disclosure of personal information to third parties.
- RCMP details on receiving audit or compliance checks affection RCMP personal information and privacy.
- RCMP details related to contingency plans and documented procedures to identify and respond to security breaches or disclosures of personal information in error.

- RCMP details related to documented procedures to communicate security violations to the data subject, law enforcement authorities and relevant program managers.

- Security procedures for the collection, transmission, storage and disposal of personal information.

Mitigation: The RCMP has developed a Memorandum of Understanding for collection, use and disclosure of personal information with any other law enforcement agencies, which may wish to access the Province of British Columbia and RCMP "E" Division Police Records Information Management Environment in the future.

18.1.2 *Use of Anonymous Data*

ALPR information moved to PRIME-BC may be used for purposes of planning, forecasting, training and/or evaluation. Consideration must be given to the use of anonymous rather than personal information for the functions outlined above.

Mitigation: The RCMP will ensure the use of anonymous rather than personal information from PRIME-BC for purposes of program planning and evaluation and human resources forecasting and training.

18.1.3 *Summary of PIA*

The Policy on Privacy Impact Assessment requires that a Summary of the PIA be publicly available. Once the translated PIA Executive Media Summary has been received back from Translation Section, the vetted PIA Summary in both official languages will be sent electronically to web@rcmp-grc.gc.ca for posting to the national site.

Mitigation: The ATIP Authority for the RCMP will establish a formal Departmental process to publish PIA summaries on the website in order to make them publicly available.

18.2. Communication Plan

An executive media summary of the Automatic License Plate Recognition (ALPR) System PIA will be published on the RCMP website in order to make it publicly available. This will be done after the summary has been translated and returned to "E" Division. The vetted PIA Summary in both official languages will be sent electronically to web@rcmp-grc.gc.ca for posting to the national site.

18.3. Conclusion

The privacy issues and/or risks identified in this PIA have been resolved through the development and documentation of appropriate procedures and processes, ALPR Policy and the PRIME-BC Policy and Procedures Manual, Charter for PRIME-BC, the Governance Model, and the MOU. The Policy Manuals for PRIME-BC consistent with RCMP Policy and the security measures consistent with the Government of Canada Security Policy. The ALPR Policy (OM25-100) is an integral part of RCMP Operational Policy. The Policy and Procedures are living documents that are continually updated to ensure they are consistent with Legislation, and Federal Government and RCMP Policies, and the Director of Police Services for the Province of British Columbia has staffed a full time position, a Staff/Sgt. from the RCMP, to manage the policy and procedures.

The automatic License Plate Recognition (ALPR) functionality will permit full electronic management of information, from download of CPIC and ICBC Driver's database information, the photographing and running of the license plate numbers against the downloaded information. This will allow Police Officers to concentrate their efforts on identifying the high risk drivers on our roadways that are causing serious injuries and fatalities. These are drivers that are uninsured, unlicensed prohibited or suspended from driving. The ALPR will also allow the RCMP to quickly locate stolen vehicles. It is hoped that once the ALPR is rolled out Province wide it will greatly improve road safety province wide by increasing the perception of apprehension for those driver who choose to ignore the law and continue to drive even after they have lost their driver's licenses.

References

Legislation

Access to Information Act (R.S., 1985, c. A-1)
Freedom of Information and Protection of Privacy Act - British Columbia
Library and Archives of Canada Act (2004, c. 11)
Personal Information Protection and Electronic Documents Act (2000, c. 5)
Privacy Act (R.S., 1985, c. P-21)

Policy and Procedures

PRIME-BC Policy and Procedures
PRIME-BC Reference Standard
RCMP Admin Man III.11 - Information Access
RCMP Admin Man III.12 – Privacy Impact Assessment
RCMP OM 16_4 (E Div) - Closed Circuit Video Equipment
RCMP OM 25 Supplement (E Div) - ALPR Policy
RCMP OM 25.100 (E Div) - ALPR Policy

Miscellaneous

Howe, Robert J. (2007) "*ALPR - Threat Risk Assessment and Statement of Sensitivity*"
Charter and Governance Model for PRIME-BC
Memorandum of Understanding (MOU) - Information Sharing - LEIP
Cohen, Dr. Irwin M.; Plecas, Dr. Darryl; McCormick, Amanda V. (2007) "*A Report on the Utility of the Automated License Plate Recognition System in British Columbia*"

Appendix A

GOC PKI: ENTRUST

ENTRUST Corporate: Company Profile and description of services

Entrust provides the broadest set of enhanced security capabilities with automated management that allows "end-to-end security" to be conducted consistently and seamlessly across applications, platforms, and devices. Entrust enhanced security capabilities are built on "identification", "entitlements", "verification", "privacy" and "security management" which allows "highly sensitive transactions" such as government health care and financial transactions to be conducted electronically.

Canadian Federal Government departments and Canadian Crown Corporations are using Entrust Internet Security services to ensure the security and confidentiality of their eBusiness management.

"end-to-end security"

"end-to-end security" refers to Entrust's particular encryption protection which secures sensitive information and transactions at their start and finish locations, and not only in transit. With Entrust, an email (for example) remains encrypted in transit, as well as in both the sender's and recipient's mail folders – time stamped, digitally (and thus legally) signed, and encrypted. Anyone, then, attempting to manipulate the content of the information at the user's physical workstation, would be unable to do so without valid authentication.

"identification"

Delivers confidence in the identification of all parties in a business transaction, regardless of the user's location.

"entitlements"

Maintains close relationships with the customers, citizens, partners and employees by giving them exactly what they need, exactly when they need it, without risking exposure to unauthorized use of or access to resources.

"verification"

Combines digital signatures with customer receipts to provide verification of a transaction and an auditable trail for non-repudiation.

"privacy"

Increases privacy of online transactions: from the moment a keystroke or mouse click submits data on a Web portal to its final destination in back-end applications. Protects important information through the entire lifecycle of the transaction.

"security management"

Meets the challenges of online business with reduced costs and ease-of-use for both end users and administrators, regardless of the application or platform.

Architecture

The following detailed architecture diagram is intended to serve solely as "reference"

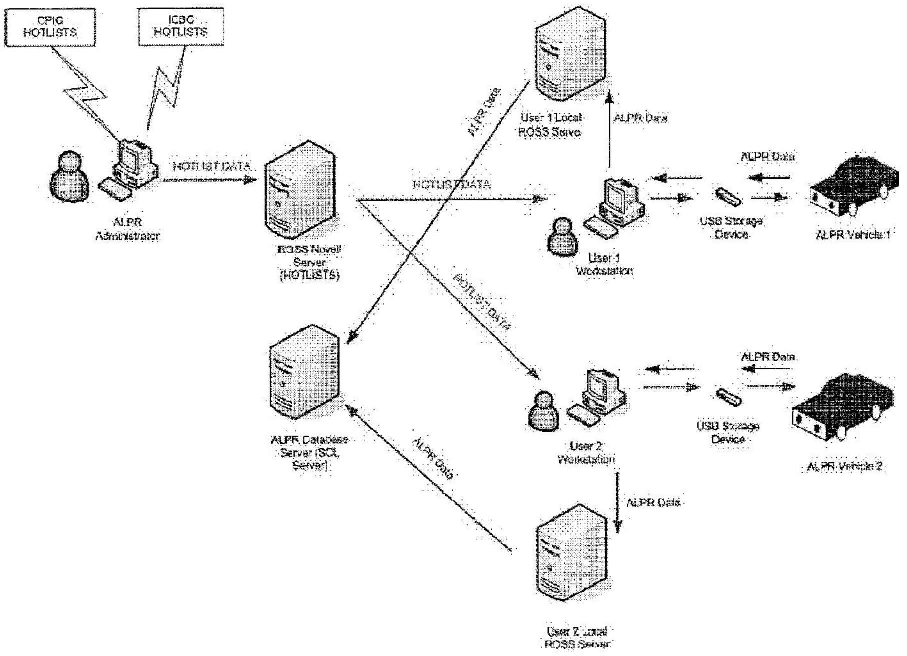


Figure 12: ALPR Architecture