TRANSIT POLICE

CANADIAN POLICE INFORMATION CENTRE (CPIC)

Effective Date: September 12, 2005
Revised Date: July 24, 2006, July 9, 2007, June 29, 2011, May 28, 2012
Reviewed Date:
Review Frequency: 2 Years
Office of Primary Responsibility: Informatics Manager

POLICY

[See also: OB180 – Missing Persons, OB280 – Towing of Vehicles, OB290 – Stolen Vehicles]

Definitions

CPIC and CPIC system – The Canadian Police Information Center computer system, a National Police Service administered by the Royal Canadian Mounted Police (RCMP)

CNI – Criminal Name Index

CRS – Criminal Record Synopsis

CR*II* – Criminal Record Level *II*

Chief Officer – The Transit Police Chief Officer or delegate.

Member – A Designated Constable, the Chief Officer or a Deputy Chief Officer of the Transit Police.

Police Act – The BC Police Act, RSBC 1996, c. 367, and the regulations thereto, including the Transit Police Operations Regulation, all as amended from time to time.

Transit Police – The South Coast British Columbia Transportation Authority Police Service.

Authority

1. The Transit Police is approved as a Category *I* CPIC Agency by the Canadian Police Information Centre (CPIC) Advisory Committee as the Transit Police has full peace officer authority provided under the *Police Act* (primary role of the agency is law enforcement).

    1. Category *I* agencies have **Full Access** and can perform**:**
        a. all transaction types in the Investigative Data Bank files;
        b. query transaction in the Investigative Data Bank files;

c. query transaction in Ancillary Data Bank files; and
d. message transmission and reception via the CPIC telecommunications system.

2. Category *I* agencies may receive Special Access only when approved by the Criminal Intelligence Service Canada.

General

2. Information that is contributed to, stored in and retrieved from CPIC is supplied in confidence by the originating agency for the purpose of assisting in the detection, prevention or suppression of crime and the enforcement of law. CPIC information is to be used only for activities authorized by a police agency.

3. Each agency having access to CPIC records is responsible for the confidentiality and dissemination of information stored on the CPIC system. The dissemination of CPIC information from the Transit Police is at the discretion of the Chief Officer and must be in accordance with existing federal and provincial policy and legislation concerning privacy and information.

4. Output obtained from CPIC must not be used as a basis for action without verification by the originator of the initial, or any related, record.

5. CPIC supplied hardware, software and communication lines will be used for CPIC purposes only.

6. Transit Police supervisors and CPIC terminal operators must ensure that narrative traffic facilities are used for official police purposes only.

7. Additional detail is found in the CPIC Reference Manual and CPIC Guideline for Quality Control. Copies are held in the Operations Communication Centre (OCC).

CPIC Advisory Committee

8. The CPIC Advisory Committee approves system policy and procedural matters. This body is composed of representatives of major city police departments in Canada and federal and provincial law enforcement representatives, and is chaired by a member of the Royal Canadian Mounted Police.

9. The CPIC Advisory Committee is responsible for establishing the scope and content of CPIC data banks, how the system is used and regulated and the criteria to determine which agencies are eligible to use the system.

PROCEDURES

TRANSIT POLICE QUERIES

10. Members will, where possible, enter their own CPIC queries in the digital form via a Transit Police PRIME/CPIC computer or police vehicle with a Mobile Data Terminal (MDT). Otherwise, these queries may be made to the CPIC operator in the OCC.

11. Whenever a query is made of the CPIC system, a “Hit” or “Not on File” response is received. The investigating Member is then advised accordingly. In the event of a “Hit”, the terminal operator will confirm the validity of the record by contacting the originating agency. Members must ensure a “Hit Confirmation” is received before concluding their investigation.

ACCESS TO CPIC DATA BANKS

12. The Transit Police is under no obligation to release information but may do so in the interest of law enforcement. The CPIC Reference Manual lists agencies that are authorized to access CPIC data banks. Requests for information are restricted to sworn officers of the agencies and the officers are required to identify themselves.

13. Routine access to CPIC data files through the Transit Police is restricted to the following police agencies:

    1. Royal Canadian Mounted Police;
    2. Provincial police forces;
    3. City police forces; and
    4. Municipal police forces approved by the CPIC Advisory Committee.

14. Access to CPIC information or network interface (i.e. Motor Vehicle Branch) through the Transit Police is restricted, unless authorized by the Chief Officer, or in an emergency, the Watch Commander. The Watch Commander (or Chief Officer’s designate) approval must be documented and forwarded to the Chief Officer for information.

15. CPIC Information or Network Interface information must not be disclosed to TransLink and subsidiary employees, contractors and consultants (this excludes Transit Police Members and authorized Transit Police civilian staff). This non-disclosure includes, but is not limited to, bus operators, station attendants and transit security staff.

RELEASE OF INFORMATION AND SECURITY

Investigative and Ancillary Data Banks

16. Information may be released at the discretion of the Chief Officer.

17. If the CPIC hard copy printout is to be released (to authorized persons pursuant to CPIC policy), the CPIC query format and any information not applicable to the requestor must be removed from the printout to protect the integrity of the CPIC

system and the privacy rights of others. The applicable information may also be released verbally or in writing.

18. Information pertaining to young persons may be released only to Canadian agencies/individuals in accordance with the provisions of the Youth Criminal Justice Act (YCJA). Information pertaining to young persons must not be released to foreign agencies.

19. Requests for release of any CPIC information for security and reliability purposes must have the written consent of the subject of the query.

20. If the request for data is for criminal or investigative purposes, the following CAUTION must be given to the requestor. “CAUTION: This record may or may not pertain to the subject of your enquiry.”

Identification Data Bank – CR*II*

[See also: OD180 – Young Persons]

21. Young person records may only be released to Canadian agencies/individuals. Young person records must not be released to foreign agencies.

    NOTE: *In certain circumstances, the disclosure of criminal records that contain only discharges under s. 736 of the Criminal Code of Canada and/or non-convictions may have adverse consequences on an individual’s reputation, employment, mobility or access to services. Accordingly, caution must be exercised when disclosing these records in connection with non-criminal inquiries, especially border crossings*.

22. If the request for CR*II* data is for criminal or investigative purposes and is not accompanied by fingerprints, then the normal caution must be given to the requestor. “CAUTION: This record may or may not pertain to the subject of your enquiry. Positive identification can only be confirmed through the submission of fingerprints.”

23. If the CPIC hard copy printout is to be released, the CPIC query format must be removed from the printout to protect the integrity of the CPIC system. The information may also be released verbally or in writing.

24. If the request for a hard copy response printout of CR*II* data is for non-criminal purposes (e.g., government employment, border crossing card, visa, etc.), the individual's identity must be confirmed by fingerprints before release of the record can occur.

    1. To confirm fingerprints, the Member will contact Court Liaison.

Identification Data Bank – CNI/CRS

25. Information may be released to authorized agencies/individuals only for criminal or investigative purposes.

26. If the CPIC hard copy is to be released for criminal or investigative purposes, the CPIC query format and any information not applicable to the requestor must be removed from the printout to protect the integrity of the CPIC system. The information may also be released verbally or in writing.

27. If the request is for criminal or investigative purposes and is not accompanied by fingerprints, the following caution must be given to the requestor. “CAUTION: This record may or may not pertain to the subject of your enquiry. Positive identification can only be confirmed through the submission of fingerprints.”

28. Queries for security and reliability are not permitted by the Transit Police.

SERVICE FILE

29. Any record placed into the CPIC system must be the subject of a police file maintained by the originator for as long as the record is on the CPIC system. Whenever a record is entered onto or removed from the CPIC system data files, such information must be contained on the PRIME General Occurrence file (GO) file.

    1. The green CPIC file jacket file must contain sufficient documentation to establish the accuracy and validity of the CPIC record (e.g., court documents, copies of Form C-216, prisoner’s reports, driver’s license or Motor Vehicle Branch printouts, criminal record).

30. A record placed on the CPIC system is deemed to be under the control of the agency/department making the entry. Access to that record can only be granted by the contributing agency/department, under the federal/provincial access legislation that applies to that agency/department.

31. All CPIC agencies are to obtain original documents from the courts to support their CPIC Person entries; however, subject to legislation, if the document is only available via photocopy, facsimile or electronically, then the document may be used for CPIC entry purposes.

    1. If the original court document is not available, add a suitable notation to the agency file outlining the reason(s) the original document is not present on the file.

    2. Photocopies of other reproduction of these court documents can be further disseminated under controlled circumstances and should be clearly identified as true copies.

    3. Upon receipt of the “original copy” of an electronic document from the court, stamp/initial/date it to indicate that it is the “original copy.”

Written Authorization for Record Input

32. To request input (and extensions to record retention periods) of Special Interest Police (SIP) category records in the Persons File of the Investigative Data Bank and Surveillance Persons, Vehicle and Boat category records in the Surveillance File of the Intelligence Data Bank, the Member will complete the designated request form (Transit Police Form OZ230).

33. The input request will be authorized in writing by the Watch Commander. The Inspector Operations may authorize the entry and then follow-up with notification to the Watch Commander of the issued authorization.

34. The Member will submit the authorized form into the CPIC designate in the Record Services Section (RSS) for entry on CPIC. Once entered, the CPIC designate will attach the authorization form to the inside left side of the green CPIC jacket.

35. When making an ADD, MODIFY or REMOVAL transaction, the CPIC operator must place their initials and employee number on the hardcopy CPIC printout, which is then stapled to the inside left cover of the green CPIC jacket.

Masterfiling

36. The Transit Police will implement the practice of masterfiling when entering data on a person who is arrestable and/or for whom a warrant or apprehension order has been issued.

    NOTE: *With masterfiling, add of a WANT record and any subsequent WANT files on that subject will be added to the existing record through the MODIFY transaction. On the CPIC system, the masterfiling method allows only one WANT record per agency for each subject.*

Court Disclosure of Police Files

37. In accordance with recent court decisions, agencies may be required to produce their police files as part of a pre-trial disclosure procedure. Members should keep this court disclosure in mind and CPIC data that could jeopardize operational investigations or contravene privacy legislation should not be placed on the police file. However, the information can be placed on a non-disclosure file. If CPIC information is placed on the police file, Members should ensure that only information pertaining to the file subject is placed on the file.

    1. For example, associated vehicles or persons in the SIP category procedure will be kept in the green CPIC jacket. This procedure is administrated by Court Liaison.

System Security

38. As the head of a CPIC approved agency, the Chief Officer is ultimately responsible for the Transit Police adherence to all policies and procedures regarding the protection and use of CPIC systems and data, including CPIC Security Standards.

39. All Transit Police personnel having direct terminal access to CPIC complete the following requirements prior to access being permitted:

    1. undergone a criminal record check through the RCMP Information and Identification Services Directorate using Fingerprint Form C-216C (included in Transit Police enhanced security clearance required for hiring);

    2. sign Transit Police Form AZ260 – Acknowledgement of Restrictions Respecting the Handling of CPIC Materials, Records and Information (Form AZ260); and

    3. review the CPIC Code of Ethics (CPIC Appendix 1-2-C) which establishes procedures and safeguards to promote the maintenance of good practice and compliance with privacy protection legislation.

40. Support Services Division personnel will be responsible for:

    1. providing newly hired personnel, who will have direct terminal access to CPIC, with Form AZ260 to sign and a copy of the CPIC Code of Ethics;

    2. retaining the original signed Form AZ260 on the individual's personnel file; and

    3. maintaining the master record of Form AZ260s.

41. Transit Police personnel will ensure that unauthorized personnel, including terminal maintenance technicians, are:

    1. properly identified;

    2. accompanied by an authorized Transit Police staff person (i.e., a person capable of providing assurance that no unauthorized access to data has taken place) at all times while on Transit Police premises; and

    3. restricted to Instruction Mode transactions if operation of the terminal is required.

Hard Copy Retention and Distribution

42. The retention and distribution of a CPIC query and narrative hard copy is as follows:

    1. The hard copy of a query generated as a result of a field check will only be held for the Member if a request for the hard copy is made at the time of the query. In absence of a request, the hard copy will be shredded.

    2. A hard copy requested by a Member will be placed in the Member CPIC tray located in the OCC. The hard copy will be collected by the Member prior to the end of shift. In the event a hard copy is not collected, the OCC CPIC operator will take possession for distribution to the Member's personal mail slot.

3. The OCC Dispatcher will place all CPIC hard copy associated to a new CPIC file in a green folder, which will then be placed in the RSS – CPIC designate tray located in the OCC.

4. The RSS – CPIC designate will review the CPIC files for quality control and operational purposes, and process as appropriate.

5. All CPIC communications received on behalf of an individual Member will be placed in the Member's CPIC tray located in the OCC, for secure forwarding to the Member. In exigent circumstances the OCC Dispatcher will notify the Watch Commander and/or the Member directly of the communication being received, so that appropriate action can be taken.

6. Unsolicited CPIC communications will be placed in the Watch Commander CPIC tray located in the OCC. As deemed appropriate by the Watch Commander, the information contained in the hard copy will be provided to shifts at briefing, with the Supervisor, on completion of the briefing, initialing beside the appropriate shift number. After all shifts have received the information:
   a. the hard copy will be forwarded to the Watch Commander;

   b. the Watch Commander will review the unsolicited CPIC communication and determine if the hard copy should be retained, if the information is of significant issue (i.e. person dangerous to police), or shredded;

   c. the hard copy will be retained on the clipboard located in the Watch Commander's office and a copy of the retained communication will be provided to the OCC to place on the OCC CPIC clipboard; and

   d. clipboard entries will be purged after three months and the Watch Commander and OCC assigned responsibility to ensure the purging is done for their respective clipboards.

Hard Copy Waste

43. CPIC computer terminal hard copy (printed output) waste must be destroyed [e.g., burned, shredded (via in-house shredder or "Shred-It" bin), or mulched] to prevent dissemination of information to unauthorized persons, and this waste disposal operation must be conducted under the direct supervision of authorized personnel.

Unauthorized Persons

44. When it is necessary to provide information produced from the CPIC computer system to unauthorized persons (e.g., Crown Counsel) it must be only in the form of a duplicate copy. All printouts that may be used or seen by other than Members and authorized personnel will have the Transit Police Terminal Identifiers removed and will be stamped with the following:

    "Property of the South Coast British Columbia Transportation Authority Police Service. This police report is supplied to you for information of your department

only. It is not to be made known to any other agency or person without written permission of the South Coast British Columbia Transportation Authority Police Service."

1. All CPIC hard copies forwarded to court will also be so marked, and then duplicated with only the duplicate copy leaving the police office. The original copy of any printout will not leave the control of the Transit Police.

Access to CPIC Terminals

45. [redacted]

Audit

46. The CPIC Field Operational Section should undertake a physical audit of the records of the Transit Police at least once in every four-year period. Under the "risk analysis" strategy, audits, or re-audits, may occur more frequently.

Further Dissemination

47. The need for any further dissemination of information must be at the discretion of the Attorney General of the Province of British Columbia or the Solicitor General of Canada.

Access to CPIC/PRIME

48. The Chief Officer can give permission for this access to designated persons and prescribe limitations to the access.

Access by Various Agencies

49. The following chart is a useful tool when determining the access of various agencies. This information has been obtained from CPIC Field Operational Section. Category II agencies have limited law enforcement responsibilities, with authority provided under specific federal or provincial legislation.

NOTE: *Category II (A) agency has a complete range of policing responsibilities (e.g., Canadian Pacific Railway Police). Category II (B) agency has investigative responsibilities within the scope of the statutes that it enforces (e.g., Immigration Canada). Category II (C) agency is a federal correctional service, provincial correctional police service, or a provincial sheriff service.*

Frequently contacting for CPIC information	[redacted]
CP Police	
BC Highways Dept.	
ICBC/SIU	
Area Firearms Officer	
BC Min. Envir, Lands & Parks Enforce. Branch	
Revenue Canada Customs	
Citizenship and Immigration Canada	
Dept. of Fisheries and Oceans	
Canada Parks Law Enforcement	
Min. Child. Family and Community Service	
Local By-Law Enforcement Officers	
Gas Bar Operations	
Local Towing Companies	
Corporate Security	
Security Guards (Banks, parking lots, apartment, shopping mall, etc.)	
Bank/Credit Card Investigators	
TransLink Employees	

(excluding Transit Police staff)									

Along with the chart this advisory applies:

1. Any release of criminal record information outside the law enforcement community may be a violation of one or more of the following federal acts pertaining to the protection of privacy: Federal Privacy Act, Criminal Records Act, or YCJA.

2. Provincial government agencies that are not sanctioned CPIC agencies may be permitted, under provincial agreement, to obtain certain information from the CPIC system. Guidance on the release of information to "secondary access agencies" can be found in RCMP national and division Operational Manual Policy regarding "Information Sources." Each request for information should be on a case-by-case, need to know basis and should be fully documented so as to withstand any possible future challenge pertaining to the legitimacy and lawfulness of any query and possible release of information. Some areas within the above table have been left blank by design, as it is up to the Chief Officer to determine what information will be released.

WANDERING PERSONS REGISTRATION

50. The Alzheimer Society of Canada and its provincial chapters are the principal source for records entered into the WANDERING PERSONS database, which is uploaded, to the CPIC system.

51. Families and support care service personnel frequently look to their local police department for information regarding programs directed to the safe return of persons suffering from dementia should they wander.

52. Pertinent biographical data on person suffering from dementia is available to the law enforcement community through a standard CPIC query using Keywords [redacted] if the person has registered with the Alzheimer Society of Canada.

53. Should the Transit Police receive inquiries regarding the Alzheimer WANDERING PERSON REGISTRY, registration forms are available on the internet @ www.alzheimer.ca or from any one of the local Alzheimer of Canada chapters (the addresses of which are also available through the web site).

54. Questions concerning CPIC and the WANDERING PERSONS REGISTRY should be directed to CPIC Field Operations BC/Yukon at [redacted]

CPIC RETENTION SCHEDULE

55. The expiry dates set for Transit Police CPIC entries is set forth in this policy. This retention schedule is in adherence with CPIC Policy and the flexibility contained within those guidelines.

    ***NOTE*:** *CPIC requires an expiry date in accordance with CPIC Policy. If the CPIC entry is not given an expiry date when entered, the CPIC system will generate an expiry date or it will reject the CPIC entry until an expiry date is assigned.*

    1. Where there is an exigent circumstance involving a Transit Police file, and a Person, Vehicle or Property should be added to CPIC but does not fall within the CPIC retention schedule, Transit Police personnel will consult with the Watch Commander.

PERSONS FILE:

Accused
UTA / RECOG

Warrants
Criminal Code Offences
Provincial Code Offences

Prohibited

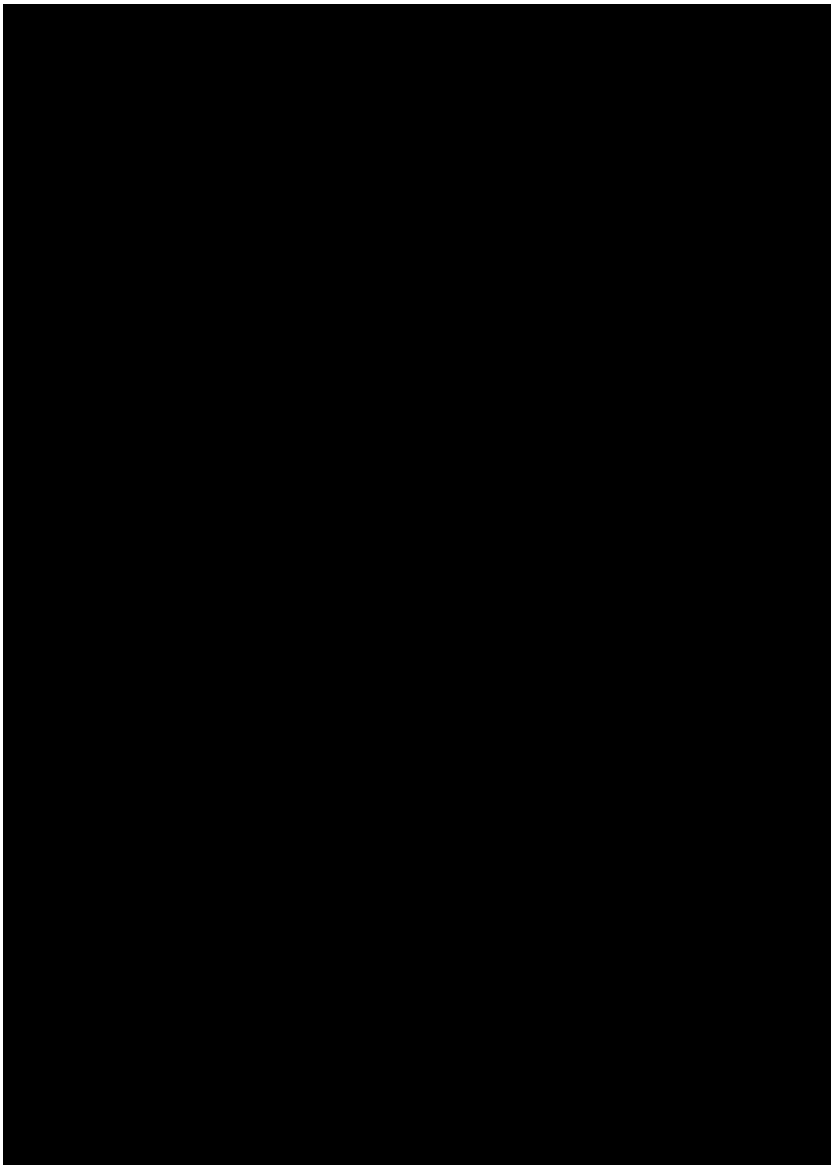
Missing

Special Interest to Police
/ Surveillance

VEHICLE FILE:

Abandoned
Crime

Licence Plates /
Validation Tags (Valtag



Stolen

Surveillance

VIN Plate / Veh Part(s)

[redacted]

MARINE FILE:

All Marine File entries to CPIC: Boat (Stolen), Boat (Abandoned), Motor (Stolen) are to be reported to the JPD in the area from which the Boat and/or Motor was stolen or abandoned.

PROPERTY FILE:

[redacted]

Articles
Value under $5000
Value $5000 - $10,000
Over $10,000

Guns
Restricted Weapon
Other firearms

Security
Passport – valid
Passport – expired
Police / Military ID
Motor Vehicle Documents
Money Order /
Travelers Cheques
Firearms Acquisition
Canadian Citizenship
Indian Status Card
Immigration Papers
Counterfeit Cdn/US currency

The Transit Police will **not** be adding the following security to CPIC:

- Drivers Licence
- Birth Certificates
- Social Insurance Number
- BC ID Cards
- Credit Cards

Recovered Property [redacted]

Key References

CPIC – Transit Police Memorandum of Understanding (Category I) [May 2011]
CPIC Policy Manual
CPIC Site Audit Report 2011