I.2 - CPIC Policy

1. CPIC Advisory Committee

1.1 Roles and Responsibilities

a. System policy and procedural matters are approved by the CPIC Advisory Committee. This body is composed of members of major city police departments in Canada and federal and provincial law enforcement representatives, and its chair is appointed by the Commissioner of the Royal Canadian Mounted Police. See CPIC Advisory Committee Charter in Appendix I-2-G.

b. As the policy-making authority, the CPIC Advisory Committee is responsible for establishing:

1. the scope and content of CPIC data banks, files, categories and records;
2. how the system is used and regulated; and
3. the criteria to determine which agencies are eligible to use the system. See Chapter I.2, sec. 4 **Access to CPIC Data Banks** for further details.

1.2 Information Technology (IT) Sub-Committee

a. The IT Sub-Committee's mandate is to:

1. recommend IT policies to the CPIC Advisory Committee;
2. set standards and parameters, including security, for inter-connectivity to the CPIC System for all agencies; and
3. review and recommend information technology standards for the Canadian law enforcement community as they relate to the CPIC system.

b. See Appendix I-2-F: **Information Technology Sub-Committee Handbook** for the Rules of Conduct and IT Sub-Committee Composition.

1.3 Triumvirate

a. The Triumvirate is a body which reports to the Information Technology Sub-committee (ITSC). It is composed of three senior members of the RCMP representing the RCMP Departmental Security of Technical Operations, the Network Services of Infrastructure Engineering and Development and the Director General, CPI Centre. By virtue of his existing National Police Services responsibilities with the CPIC system, the Director General, CPI Centre has been appointed as the Chair of this group. Members of the ITSC have the right to attend meetings of the Triumvirate.

b. The Triumvirate, on behalf of the ITSC, reviews and recommends non-standard CPIC connectivity and general NPSNet connectivity, taking into consideration security, network issues, availability and integrity. Also, as new issues and policy needs are identified by the Triumvirate, it will provide recommendations to the ITSC.

c. Decisions of the Triumvirate are made by consensus. Minutes of all meetings are recorded, kept and maintained by CPI Centre. All activities of the Triumvirate are reported to the ITSC during scheduled meetings. Minutes are provided to the Chair of the ITSC.

d. Decisions of the Triumvirate may be appealed. An agency which is not satisfied with a decision may request, via the Director General, CPI Centre, that the matter be referred to the ITSC, through the ITSC chair, for review. If there is no satisfactory resolution of the issue, the matter shall be referred to the Chair of the Advisory Committee who may make an immediate ruling or decide to bring the matter to the Advisory Committee for discussion and vote. The ultimate authority, should the matter remain unresolved, is the Commissioner of the RCMP.

e. The appeal process is available to both the agency involved and the Triumvirate.

2. CPIC Agency Categories

2.1 Category I: Police Agency

a. **Canadian** - The agency has full peace officer authority provided under a Canadian federal or provincial *Police Act*. The primary role of the agency is law enforcement. The police agency is approved as a Category I agency by the CPIC Advisory Committee on the written advice of the Director General (DG), CPI Centre, RCMP National Police Services and for CPIC purposes, the Canadian Security Intelligence Service (CSIS).

b. **Foreign** - The agency has full peace officer authority provided under a *Police Act*. The primary role of the agency is law enforcement.

2.2 Category II: Agency with Limited Law Enforcement Role

a. The agency has limited law enforcement responsibilities; its authority is provided under specific federal and/or provincial legislation (e.g. *Customs Act, Immigration Act, Railway Act,* provincial *Wildlife Acts*, etc.). Law enforcement is not the primary role of the organization. Agencies granted Category II access will fall under one of the following sub-categories:

1. **Category II (A)** - The agency has a complete range of policing responsibilities including response to complaints from the public, patrol, traffic law enforcement and the investigation of suspected offences which could lead to prosecution under the *Criminal Code of Canada* or other federal/provincial statutes (e.g., Canadian Pacific Railway Police).
2. **Category II (B)** - The agency has investigative responsibilities within the scope of the statutes that it enforces. The investigative powers of the agency go beyond simple monitoring, routine inspection, or enforcement of administrative penalties and must include a range of responsibilities, such as investigating presumed offences likely to be subject to prosecution under the *Criminal Code of Canada* or other federal/provincial statutes (e.g. Customs and Excise, Immigration Canada).
3. **Category II (C)** - The agency is a federal correctional service, provincial correctional service, or a provincial sheriff service.

2.3 Category III: Agency with Role Complementary to Law Enforcement

a. The agency has no direct law enforcement authority but provides assistance to law enforcement agencies.

3. Characteristics of CPIC Data Banks

3.1 Investigative Data Bank Files (Characteristics)

a. Records are entered on CPIC directly by police agencies or other agencies approved by the CPIC Advisory Committee.

b. Data integrity is controlled by the agencies and files are audited by approved audit agencies.

c. Contributing agencies are accountable to the CPIC Advisory Committee.

d. Information in the files is used in direct support of law enforcement investigations.

3.2 Identification Data Bank Files (Characteristics)

a. Records are entered by RCMP Information and Identification Services on behalf of police agencies.

b. Information in the files is used to complement investigative information, for security and reliability checks, and by the courts.

3.3 Intelligence Data Bank Files (Characteristics)

a. Records are entered by members of the police community responsible for the gathering of criminal intelligence.

b. Data integrity is controlled by police agencies and files are audited by approved audit agencies.

c. Contributing agencies are accountable to Criminal Intelligence Service Canada, and to the CPIC Advisory Committee.

3.4 Ancillary Data Bank Files (Characteristics)

a. Records are contributed by police and non-police agencies, e.g. Corrections, Motor Vehicle Branches.

b. Data integrity for records contributed by non-police agencies is outside police control. Data integrity for records contributed by a police agency is the responsibility of that agency. Records contributed to a CPIC-owned file are audited by approved audit agencies.

c. Contributing agencies are accountable to the CPIC Advisory Committee for records contributed to a CPIC-owned file.

d. Information in the files is used to supplement investigative information or to provide information of general interest.

4. Access to CPIC Data Banks

4.1 Access

a. Agencies requesting access to CPIC should contact CPI Centre at RCMP Headquarters or the nearest CPIC Field Operations Section for details on the criteria to determine eligibility.

b. There are three types of access:

1. **Full Access -** The agency can access the Investigative, Identification and Ancillary Data Banks, and the communications system. See also **Interim Full Access**.
2. **Special Access** - The agency has Full Access and, in addition, can access the Intelligence Data Bank.
3. **Limited Access** - The agency is restricted to specific data banks, files, categories within files and/or the communications system. Limited access is governed by the CPIC Advisory Committee.

Interim Full Access

c. On the recommendation of the DG CPI Centre, the Chairperson may grant **interim** Full Access, including the assignment of a terminal originator's number , to any police agency not yet approved by the Committee, provided the following criteria are met:

1. The agency must be a police agency as described in Chapter I.2, sec 2.1 **Category I: Police Agency**
2. The agency must provide reasonable security for CPIC files and documentation, and its communications system.
3. The agency must operate a suitable filing system which contains sufficient documentation to confirm a hit in a reasonable amount of time, 24 hours a day.
4. All personnel having access to the CPIC files and documentation, either directly or through an interface, must be security-cleared through the submission of fingerprints.

Governance of Access

d. Access to Investigative Data Bank files is governed by the CPIC Advisory Committee.

e. Access to Identification Data Bank files is governed by the *Identification of Criminals Act*, supplemented by the Solicitor General's ministerial directive (see Appendix IV-1-A: **Release of Criminal Record Information**), applicable provincial policy (for Province of Ontario Policy, see Appendix IV-1-A: **Release of Criminal Record Information**), and the *Youth Criminal Justice Act*.

f. Access to Ancillary Data Bank files is governed by the owner of the file through the owner's written consent. The owner is responsible for validating the rights of an agency to access the file.

g. Access to Intelligence Data Bank files is governed by the Criminal Intelligence Service Canada and the CPIC Advisory Committee.

4.2 Transactions Available on CPIC

a. The following transactions can be performed on the CPIC system; however, the availability of these transactions to an individual CPIC agency is governed by the Category of the agency, see Chapter I.2, sec 2. **CPIC Agency Categories** and the data bank being accessed.

Maintenance Transactions

1. Maintenance transactions:
    1. Add
    2. Modify
    3. Locate
    4. Unlocate
    5. Remove
    6. Transfer
    7. Merge

Query Transactions

2. Query transactions:
    1. Standard
    2. Special
    3. Unique
    4. Restricted - in some cases, the response merely acknowledges the transaction and in others, the data disclosed is the minimum necessary to verify the existence of a hit.

Off-Line Searches

3. See Chapter II.3, **Off-Line Searches** for details.

Message Transmission

4. Messaging transactions:
    1. Narrative Traffic, also known as Mailbox Message;
    2. Hit Confirmation, also known as Direct Delivery.

4.3 Access and Transactions Available for Category I Agencies

a. Category I agencies have **Full Access** and can perform:
    1. all transaction types in the Investigative Data Bank files;
    2. query transactions in Identification Data Bank files;
    3. query transactions in Ancillary Data Bank files; and
    4. message transmission and reception via the CPIC telecommunications system.
b. Category I agencies may receive **Special Access** only when approved by the Criminal Intelligence Service Canada.

4.4 Access and Transactions Available for Category II Agencies

a. Category II agencies have **Limited Access** and can perform the following transactions:
    1. standard query of the following Investigative Data Bank files: Persons, Vehicles, Marine and Property;
    2. standard query of the Identification Data Bank;
    3. standard query of the Ancillary Data Bank files dealing with vehicle registered owners, driver licence information, wandering persons and inmate records, subject to such approvals as may be required from the appropriate access authorities;
    4. standard maintenance access to Persons, Vehicles, Marine and Property files of the CPIC Investigative Data Bank in accordance with present CPIC policy (e.g. "hit" confirmation availability 24 hours per day, etc.). Maintenance access is restricted to those CPIC files and categories relating to the agency's mandate;
    5. access to the CPIC communications system.
b. Notwithstanding the access and transactions described above, the CPIC Advisory Committee may further restrict or relax access and transaction limitations pursuant to any application for access by a Category II agency.

Memorandum of Understanding (Category II)

c. As soon as a Category II agency has been granted access to CPIC by the CPIC Advisory Committee, CPI Centre provides the agency with a **Memorandum of Understanding (MOU)**, which outlines the specific CPIC access being allowed and requests a commitment from the agency to adhere to CPIC policies. Once the initial MOU between the Category II agency and CPI Centre has been signed, any change to that MOU must be approved by the Director General, CPI Centre.

1. For example, a Category II agency has been granted query access by the CPIC Advisory Committee and has entered into an MOU with CPI Centre. At a later date, the agency decides they want to be able to conduct maintenance transactions. As this would constitute a change to the existing MOU, the agency must send a request to the Director General, CPI Centre, outlining their business case for the change. If all the necessary criteria are met, the Director General, CPI Centre can approve the change(s) to the MOU.

d. See Appendix I-2-B: **List of Approved Category II and III Agencies** for a list of approved Category II agencies and their access rights.

4.5 Access and Transactions Available for Category III Agencies

a. Category III agencies have **Limited Access** but are generally restricted to narrative traffic and instructional data base files only.

b. Notwithstanding the access and transactions described above, the CPIC Advisory Committee may further restrict or relax access and transaction limitations pursuant to any application for access by a Category III agency.

Memorandum of Understanding (Category III)

c. As soon as a Category III agency has been granted access to CPIC by the CPIC Advisory Committee, CPI Centre provides the agency with a Memorandum of Understanding (MOU), which outlines the specific CPIC access being allowed and requests a commitment from the agency to adhere to CPIC policies. Once the initial MOU between the Category III agency and CPI Centre has been signed, any change to that MOU must be approved by the Director General, CPI Centre. See **Memorandum of Understanding (Category II)** in Chapter I.2, sec. 4.4 **Access and Transactions Available for Category II Agencies** for an example.

d. See Appendix I-2-B: **List of Category II and III Agencies** for a list of approved Category III agencies and their access rights.

4.6 CPIC Access Outside Canada

a. All requests for CPIC-accessible terminals outside Canada must be submitted to the Director General, Canadian Police Information Centre, RCMP.

5. Service Level Agreement (SLA) / Use and Installation of CPIC Equipment

5.1 A Service Level Agreement (SLA) has been agreed to and signed between the Canadian Police Information Centre (CPI Centre) and the Chief Information Officer Sector, RCMP (CIO Sector).

The CIO Sector is responsible for the maintenance and support of the CPIC system. It is also the maintenance and support sector for the National Police Services Network (NPSNet) infrastructure over which CPIC data is transmitted. Maintenance and support for the NPSNet are covered under the Standard Service Agreement published by the Network Services Branch, CIO Sector.

Terms of the CPIC Program SLA are defined in Service Level Agreement in Appendix I-2-H.

The CPI Centre is the point of contact for any issue relating to the Service Level Agreement and will be responsible to liaise with the CIO Sector on behalf of the CPIC clients.

5.2 CPIC-supplied hardware, software and communications lines shall be used for CPIC purposes only.

5.3 CPI Centre provides the national communications network, CPIC software and gateway/server (first point of access) at each Category I agency (***Exception:*** RCMP agencies). Category I agencies are responsible for any additional equipment (cluster/Local Area Network or LAN) and/or additional gateways.

a. All other CPIC agencies (Category II and III) are responsible for providing the necessary computer installation to access the CPIC system. The installation includes the internal wiring required for the agency's computer needs, the terminals and printers, and both LAN and communication cards.

b. The Chairperson of the CPIC Advisory Committee has delegated authority to the Director General, CPI Centre, to approve network connections, **other than by an interface**, for previously approved CPIC agencies to the CPIC System and network, currently NPSNet.

5.4 All Category I External Systems (Interfaces) are provided the first point of access.

6. Interfaces

6.1 Interface Definition

a. An interface is any device (other than that provided by the RCMP as CPIC terminal equipment) which acts as a direct communications link between a user or data bank and the CPIC system.

6.2 Interface Approval

a. The following interface requests are subject to the approval of the CPIC Advisory Committee:

1. requests from non-police agencies;

2. requests from agencies where some conflict of policy has been encountered.

b. Interface requests from CPIC agencies that already have access to CPIC and meet the conditions governing interfaces as outlined in Chapter I.2, sec 6.3 **Conditions Governing Interfaces** may be approved by the Chairperson of the CPIC Advisory Committee.

c. For approval of network connections other than by interface, see Chapter I.2, sec 5. **Service Level Agreement (SLA) / Use and Installation of CPIC Equipment**.

6.3 Conditions Governing Interfaces

Location

a. An interface system, including a provincial corrections interface, must be under a **controlled environment** approved by the CPIC Advisory Committee.

1. A controlled environment protects the interface and CPIC from accidental or deliberate compromise of confidentiality, data integrity, and system availability and is governed by written policy. Specific reference must be made to:

1. site organization and administration;

2. personnel having access to the site, computer systems, and communications facilities;
3. the environmental and physical controls in place;
4. control of the computer systems themselves (including hardware, software, and computer operation); and
5. control and protection of communications facilities.

b. The interface system is subject to the same **security, confidentiality, privacy** and **audit procedures** as those in effect for the CPIC system.

c. Information retrieved from data banks interfaced to CPIC is subject to the same security, confidentiality, and privacy provisions as those in effect for CPIC information.

d. The interface system must be connected with the CPIC communications system using **lines and equipment** specified by the RCMP.

Terminals

e. **Terminals** authorized to access the CPIC system through an interface must be:

1. directly connected to the interface or to an approved connection with the interface;
2. identifiable to the external system host through a unique terminal identifier; and
3. in a controlled environment as outlined above.

Mobile Data Terminals

f. **Mobile data terminals (MDTs)** authorized to access the CPIC system through an interface must comply with the following:

1. For each transaction, the MDT must provide the capability for unique terminal identification to the host processor.
2. For each session, i.e. log-on, the MDT must provide the capability for unique user identification, e.g. password, badge number, to the host processor.
3. The host processor must be capable of recognizing valid terminal and user identification and controlling access to system features accordingly.

Ancillary Data Banks

g. **Ancillary data banks** may be accessed through CPIC when:

1. The information is of value to police forces throughout Canada.
2. The data bank is connected to the CPIC system through an interface.
3. The data bank is identifiable through a unique

h. The interface agency must **agree in writing** to abide by the conditions contained in the approved CPIC Interface Letter of Understanding.

7. Confidentiality and Dissemination of Information

7.1 General

a. 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 Category I agency or as provided through legislation by a Category II or III agency.

1. 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 is at the discretion of the CPIC agency head or delegate who is releasing the information and **must** be in accordance with existing federal and provincial policy and legislation concerning privacy and information access.

1. In those instances where access is requested and the CPIC agency processing the request is **not** the owner/originator of the record in the CPIC Investigative or Ancillary Data Banks, the agency must consult with the record owner and will identify the owner of the record, when appropriate.

2. A Category II or III agency (see Chapter I.2, sec. 2. **CPIC Agency Categories** for definitions) may not *further* disseminate information obtained from the CPIC system except where that use is consistent with the carrying out of the duties and responsibilities of the Category II or III agency.

3. "Private" organizations shall not be allowed direct access to CPIC information unless they are under the **direct** control and management of an approved CPIC law enforcement agency.

4. The CPIC ***Code of Ethics*** establishes procedures and safeguards to promote the maintenance of good practice and compliance with privacy protection legislation. See Appendix I-2-C: **CPIC Code of Ethics**.

2. The releasing agency **must** have written policy on the dissemination of CPIC information as CPIC information must be protected against disclosure to unauthorized agencies or individuals. Before any CPIC information is released, the agency head or delegate must be satisfied that:

1. the request is a legitimate request and not just one of personal use;

2. the released information will not jeopardize the integrity of the CPIC system or its users;

3. the proper identification procedures, such as personal identification with photograph, have taken place;

4. confirmation, where applicable, with the originating agency has been carried out; and

5. the release conforms with existing policy.

b. The CPIC policy regarding the dissemination of information has been divided into the following distinct areas, namely the Investigative/Ancillary Data Banks and the Identification Data Bank. Requests for the release of information will be for either criminal/investigational purposes or for non-criminal purposes such as security clearances.

c. See Chapter I.2, sec. 7.2 **Release of Investigative and Ancillary Data Bank Information** if the release of information is for private employment purposes.

7.2 Release of Investigative and Ancillary Data Bank Information

a. Information from the Investigative (Persons, Vehicles, Property, and Marine) Data Bank and Ancillary (RO/DL systems, Inmate File, RWRS, etc.) Data Bank may be released at the discretion of the CPIC agency head or delegate.

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

1. confirmation and verification with the record owner (originating agency) has been carried out; and
2. the originating agency has been notified of the reason for the check and has consented to the release; and
3. personal visual identification by the law enforcement agency of the subject of the check has taken place; and
4. the results of the checks are communicated directly to the subject of the check.

The applicable information may be released verbally or in writing. However, printouts should not be released.

c. Any exception to the procedures listed in 7.2.b if not legislatively required or not related to a vulnerable sector purpose on a case-by-case basis is to be approved by the CPIC Tri-Chair Committee which is currently composed of the Director General, CPI Centre and the Chairs of the Information Technology Sub-Committee (ITSC) and Business Requirements Sub-Committee (BRSC).

To apply for an exception:

1. Contact the CPIC Co-ordinator for your region/province with full written details of your request for his/her recommendations

   -Local Field Operations Section

   -Ontario Policing Services Division (Ontario Police Services)

   -Ontario Provincial Police (OPP only)

   -Centre de Renseignements Policiers du Québec (CRPQ)
2. CPIC Co-ordinators will forward your request with their recommendations to the Canadian Police Information Centre for processing.
3. The Tri-Chair Committee will rule on the request.
4. Agency will be notified of the decision by the appropriate CPIC Coordinator.
5. If the request is denied and the agency disagrees, the matter will be referred to the CPIC Advisory Committee via your CPIC co-ordinators.

d. Where approval has been granted, it is incumbent upon the sponsoring agency to enter into a formal MOU outlining the terms and conditions governing the partnership including but not limited to personnel screening, information use and termination clauses. The sponsoring agency must conduct periodic audits of the arrangement.

e. The CPIC Advisory Committee retains the right to withdraw this approval where it is not the interest of the CPIC community to continue with any such arrangement.

CPIC Hard Copy Printout

1. If the CPIC hard copy printout is to be released, any information not applicable to the requester **must** be removed from the printout to protect the privacy rights of others. The applicable information may also be released verbally or in writing.

Young Persons

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

Release to Category II or III Agency

3. If the CPIC information is being released to a Category II or III agency that has not yet received its terminal equipment, dissemination must be in accordance with the agency's access rights as established by the CPIC Advisory Committee. See Appendix I-2-B: **List of Approved Category II and III Agencies** for a list of approved Category II and III agencies and their access rights.

Non-Criminal Purposes

4. If the request for release of any CPIC information is for security and reliability clearances, you **must** have written consent of the subject of the query. The subject must agree to the release of information, identifiable to that person, that may be on the CPIC system.

Criminal or Investigative Purposes

5. If the request for data is for criminal or investigative purposes, the following CAUTION must be given to the requester:

   *"**CAUTION**: This record may or may not pertain to the subject of your enquiry."*

7.3 Release of Identification Data Bank Information

7.3.a Release of Information from Files

1. Information from the files may be released to those agencies listed in Appendix IV-1-A: **Release of Criminal Record Information** with the exception of young offender records which may be released only to Canadian agencies/individuals in accordance with the *Youth Criminal Justice Act.* Young offender records must **not** be released to foreign agencies. Refer to Appendix I-2-B: **List of Approved Category II and III Agencies** for further guidelines.

   Note: In certain circumstances, the disclosure of criminal records that contain only discharges under Section 736 of the *Criminal Code* 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.

2. If the request for data is for criminal or investigative purposes and is not accompanied by fingerprints, then the normal CAUTION must be given to the requester.

   "Caution: This record may or may not pertain to the subject of your enquiry. Positive identification can only be confirmed through submission of fingerprints."

3. 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.

4. If the request for a hard copy response printout of 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. The agency should either submit the fingerprints to RCMP Information and Identification Services or they may certify them to fingerprints contained on their local file provided it has previously been identified to the FPS file.

7.3 b Release of Information from Files

1. Information from Criminal Name Index/Criminal Record Synopsis queries may be released **only** for criminal or investigative purposes to agencies/persons listed in Appendix IV-1-A: **Release of Criminal Record Information.**
2. If the CPIC hard copy printout is to be released for criminal or investigative purposes, the CPIC query format and any information not applicable to the requester **must** be removed from the printout to protect the integrity of the CPIC system. The information may also be released verbally or in writing.
3. If the request for data is for criminal or investigative purposes and is not accompanied by fingerprints, then the following CAUTION must be given to the requester:

*"**CAUTION**: This record may or may not pertain to the subject of your enquiry. Positive identification can only be confirmed through submission of fingerprints."*

4. queries for security and reliability clearances are permitted as authorized in Appendix IV-1-A: **Release of Criminal Record Information** but information must not be released other than to state:
   1. when the response is negative: "Based on the information received, there is no criminal record identified. Information can only be confirmed by fingerprint comparison."; or
   2. when the response contains possible records: "There may or may not be a criminal record in existence. Information can only be confirmed by fingerprint comparison."

Note: Due to the nature of the file and to protect the integrity of the CPIC system, **hard copy printouts** must **not** be given to any agency/individual as the result of requests for security and reliability clearance checks.

7.4 Police Files/Documents

a. Any record placed on the CPIC system must be the subject of a police file maintained by the originator for as long as the record is on CPIC. An agency must be able to confirm its CPIC records promptly, 24 hours a day, 7 days a week. The CPIC file jacket/package file must contain sufficient documentation to establish the accuracy and validity of the CPIC record (i.e., court documents, copies of C-216's, prisoner's reports, driver's licences or Motor Vehicles Branch printouts). Duplicate documentation is not required if the information is already supported on the CPIC file jacket/package or where the agency maintains their files in electronic format."

Note: The Chief Firearms Officers have sole responsibility for the entry of revocations and refusals with respect to firearms. These entries are for information purposes only and do not provide grounds for arrest. The offices of the Chief Firearms Officers are available to confirm these records Monday to Friday during regular business hours only.

Access to Police Files

1. 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, upon a request made to that agency/department, under the federal/provincial access legislation that applies to that agency/department.

Host Agencies

2. Host agencies may maintain CPIC files on behalf of their satellite agencies if appropriate records policy permits such a procedure.

Court Documents

3. 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 that 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 file.
    2. Photocopies or 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".

7.5 Written Authorization for Record Input

a. Input (and extensions to record retention periods) of Persons File of the Investigative Data Bank records category records in the Persons, Vehicle and Boat category must be authorized in writing by the agency head or his/her delegate. Delegation of this authorization must also be in writing.

7.6 Court Disclosure of Police Files

a. Agencies may be required to produce their police files as part of a pre-trial disclosure procedure.
    1. This disclosure would be to the crown as well as defense counsel. Any CPIC printouts stored on the police file would become part of the disclosure.
    2. It is recommended that the CPIC agency ask the Crown to apply to the Court for an order to disallow the defence counsel from using the CPIC material for any other purpose.

b. Agencies should keep this court disclosure in mind when placing CPIC information on their police files.
    1. CPIC data which could jeopardize operational investigations or contravene privacy legislation should not be placed on the police file.
    2. If the CPIC information is put on the police file, agencies should ensure that only information pertaining to the file subject is placed on the file.

c. A CPIC agency which is served with a subpoena for a CPIC record must comply with such a court order, even from a civil court.
    1. The agency should contact the Ontario Policing Services Division (PSD), Centre de Renseignements Policiers du Quebec (CRPQ), or the appropriate CPIC Field Operations Section, for guidance.
    2. The PSD, CRPQ or CPIC Field Ops. Section may contact the legal counsel responsible for obtaining the subpoena to discuss the CPIC policy on back-up documentation and hit confirmation. This discussion may result in the subpoena being quashed.

7.7 Use of CPIC for Licensing/Screening

a. Approved CPIC agencies may use CPIC for licensing purposes provided:
   1. the licensing function of the agency is legislatively mandated;
   2. the agency is legally entitled to receive the full range of CPIC information in carrying out its licensing process, e.g. authority conferred by the *Youth Criminal Justice Act*; and
   3. part of the screening process includes a check of local records, by agreement with the law enforcement agency of jurisdiction.

b. Only CPIC agencies with full law enforcement authority (Category I) should use CPIC for the screening of persons entering into positions of trust. "Positions of trust", for CPIC purposes, means paid or voluntary positions dealing with vulnerable people: children, the elderly and disabled persons. See Chapter I.2, sec.14 **Screening Volunteers and Employees for Positions of Trust with the Vulnerable Sector** for a complete definition.

8. System Security

8.1 Responsibility

a. The security at each user agency having authorized access to CPIC is the responsibility of the agency concerned and must be in accordance with the following CPIC Security Standards.

b. The security of the NPS Network is the responsibility of the RCMP Departmental Security Officer as delegated by the Commissioner of the RCMP.

8.2 Personnel

a. The minimum acceptable standard for all employees having direct access to CPIC information is a criminal records check through Information and Identification Services using Fingerprint Form C-216C, or by a technician who has been certified by the RCMP on the use of the Automated Fingerprint Information System (AFIS).

   1. A criminal records check on new employees who will have direct terminal access to CPIC must be conducted prior to offering employment.
   2. For employees of Category II and III agencies, a local indices check must be conducted by the Category I agency for their jurisdiction.
   3. All job-related application forms must clearly state the necessity for a criminal records check as a fundamental condition of employment.
      1. In addition, the agency may wish to refer employees to Appendix I.2-A: **Acknowledgement of Restrictions Respecting the Handling of CPIC Material, Records and Information**.
   4. An agency must maintain proof of security screening for examination by CPIC auditors when required.

b. Each agency is responsible for ensuring that unauthorized personnel, including terminal maintenance technicians, are:

   1. properly identified;
   2. accompanied by an authorized person (i.e., a person capable of providing assurance that no unauthorized access to data has taken place) at all times while on agency premises; and
   3. restricted to Instructional Mode transactions if operation of the terminal is required.

c. User ID

- The User ID field is a user login name that identifies an individual in an organization as the originator of a CPIC request.
- The User ID should be unique and cannot be reassigned. Agencies must keep track of the use of this identifier.
- The first 11 characters on the User ID field should be used (left justified).
- The User ID field must be populated automatically by the interface, made transparent to the users and unmodifiable by them.
- The User ID will be logged for auditing purposes.

8.3 Terminal Location

a. Each terminal must be in a location where its operation is restricted to authorized personnel and may only be left unattended under the following security-controlled conditions.

1. Under exceptional and unusual circumstances, the terminal may be placed on HOLD to allow the receipt of unsolicited traffic.
2. When unattended or being serviced by a technician, the terminal may be placed on alternate route and left ON.

See Chapter II.1, sec. 4.1 **General Information about Unattended Terminals and Alternate Routing** for details.

8.4 Hard Disk

a. Because the hard disk drive in a CPIC terminal is a storage medium for CPIC information, appropriate steps must be taken to protect that information from infection by computer virus programs and/or tampering or removal whenever a terminal's hard disk drive is being serviced. See Appendix I-2-E: **Computer Virus Prevention Procedures**.

1. Whenever a terminal's hard disk drive is being serviced, the maintenance contractor shall be supervised by a qualified person (i.e., person capable of providing assurance that no unauthorized access to data has taken place) responsible to the agency.
2. When a problem is reported on a hard disk drive containing CPIC information:
    1. The maintenance contractor is permitted to test, diagnose, and (if not a confirmed mechanical failure) perform a low-level format, format and partitioning of the existing hard drive.
    2. If it is necessary to exchange the hard drive, the contractor must remove the defective hard disk drive and turn it over to the CPIC agency. **Under no circumstances** is the contractor allowed to remove the hard disk drive from the agency premises.
3. If it is necessary to install a replacement hard drive, the maintenance contractor shall:
    1. install the replacement unit on site and run associated diagnostics; and
    2. format the hard disk drive in preparation for the restoration of the system by the CPIC user from back-up diskettes.
4. If the base unit is defective, the maintenance contractor shall install the hard disk drive on site in a new base unit.

5. After the maintenance contractor has installed a replacement hard disk drive, the defective disk drive should be:
   1. destroyed, if unfit for repair; or
   2. "de-gauzed", if being sent for repair, to minimize the risk of data remaining on the drive

   Note: It is expensive to properly de-gauze a hard drive; therefore, destroying it may be more cost-effective or

   3. sent to the local switcher/DSX site for disposal.
6. Records of all hardware maintenance activity should be retained for a minimum of one year.

8.5 Virus Protection

Computer viruses are malicious programs which are designed to make unauthorized changes to computer workstations and data. To protect the CPIC information on the workstation and prevent the spread of viruses, appropriate steps must be taken to protect the workstation from computer virs programs.

8.6 Security Audit

a. The Audit Team, in addition to auditing the validation of records (see Chapter I.2, sec.10 **CPIC Agency Audits**), shall:
   1. examine personnel and site security at terminal and interface locations to ensure that CPIC security standards are being maintained; and
   2. at the direction of the CPIC Advisory Committee, conduct a special audit of records and security at any terminal, satellite or interface location in Canada and submit an audit report accordingly.

8.7 Hard Copy Waste

a. All terminal hard copy waste must be burned, shredded or mulched to prevent disclosure of information to unauthorized persons. Agencies using non-security cleared personnel, such as commercial shredding companies, must ensure that on-site and off-site destruction of waste is done under direct supervision of security cleared personnel.

8.8 Mobile Data Terminals/Workstations

a. A mobile data terminal's (MDT's) access to the CPIC System by other than a "direct-connect device" or through an interface by a "remote access device" shall be restricted to Query Only.

b. Police departments using or planning to use MDTs must consider the following points to reduce the vulnerability of MDTs to security violations:
   1. Develop MDT security that is independent of vehicle security.
   2. Lock the vehicle when not in use.
   3. Ensure the MDT is lockable, both keyboard and screen.
   4. Install a direct view security screen.

5. Provide the capability for backlogging incoming messages, showing a "message waiting" indicator on screen. The operator must request the message before it is shown.
6. Control service status and file access on-line from the communications controller.
7. Program the MDT host processor to limit the number of failed attempts to sign on or call up information.
8. Be cautious when non-police personnel are in MDT-equipped vehicles.
9. Develop procedures to deal with both vehicle and MDT maintenance and repair.
10. Note that data transmitted over the air is not protected by encryption. The lack of security of MDT systems must be stressed. Secure data/voice transmission schemes should be considered where practical.

8.9 Access to the Internet

9. Discipline of the System

9.1 Maintenance

9.1 The maintenance of accurate, up-to-date information is the responsibility of the CPIC agency contributing such information. RCMP National Police Services (NPS) does not assume any responsibility for the authenticity of information entered in the system.

9.2 Hit Confirmation

9.2 Information in the CPIC system is for investigational purposes only, and does not positively identify an article of property or a person. Output from CPIC must therefore not be acted upon without verification with the originator of any related record.

9.3 Breaches of Procedure

9.3 Repeated or serious breaches of established procedures shall be referred to the CPIC Advisory Committee for necessary action.

9.4 Policy Violation Investigations

9.4 Complaints of CPIC policy violations shall be reported to the appropriate CPIC Field Operations Section, PSD or CRPQ, with an information copy being sent to the DG CPI Centre. The user agency or agencies involved shall investigate thoroughly and expediently all complaints of CPIC policy violations.

a. If the complaint is resolved by the agency, the results of the investigation, including corrective or disciplinary action taken, shall be reported to the DG CPI Centre for the record and the annual report to the Advisory Committee, via their local Field Ops., PSD or CRPQ.

b. If the complaint cannot, for whatever reason, be resolved by the agency, the DG CPI Centre shall have an investigation conducted through the:

1. appropriate CPIC Field Ops. Section; or
2. PSD, if the agency is in Ontario; or
3. CRPQ, if the agency is in Quebec.

c. Any serious, flagrant or continuous breaches of CPIC policy that cannot be resolved to the satisfaction of the Chairperson of the CPIC Advisory Committee, shall be brought before the Advisory Committee for its consideration and decision.

10. CPIC Agency Audits

10.1 A physical audit shall be performed at each CPIC agency to verify records, review CPIC file control, examine personnel and site security and verify compliance with CPIC policy.

a. All new Category II(B) agencies shall be audited within one year of gaining access to CPIC.

10.2 A summarized report of all audits shall be submitted to the CPIC Advisory Committee by the PSD, Sûreté du Québec (SQ), and CPIC Field Services Analysis Section, NPS, at least once a year.

10.3 Audits shall be conducted by:

a. personnel authorized by the PSD, for all municipal and provincial police agencies in Ontario;

b. personnel authorized by the SQ for all municipal and provincial police agencies in Québec;

c. CPIC Field Ops. Sections, for all RCMP agencies, DND military police, and provincial, regional, or municipal police forces outside Ontario and Quebec; and

d. CPIC Field Services Analysis Section, when requested to assist the auditors noted above.

10.4 Definition of CPIC Audit Terms

10.4 The following definitions shall be used by CPIC auditors:

Prime Record

a. A prime record is a record that can be entered on the CPIC system independently.

Secondary Record

b. A secondary record is a record that can only be entered on the CPIC system when linked to a prime record by cross-referencing.

Invalid Record

c. An invalid record is a prime record:

1. not having substantive documentation in a supporting file ;
2. containing incorrect index field data that could result in an erroneous hit or that could affect the results of the record in such a way that the system would output an erroneous "No Hit on File" response;
3. with an unauthorized entry;
4. that does not conform to the ***CPIC Reference Manual*** category definition;

5. that, for audit purposes, cannot be supported with substantive documentation by an agency within 30 minutes of the request to produce the documentation.

Field for Correction

d. Field for Correction is any secondary record or any field of a prime record that:

1. can be verified as incorrect when checked against the documentation on the agency file, or
2. is not entered in accordance with CPIC policy, or
3. does not contain information that is available from the agency file.

Omission Rate

e. The omission rate is the system-generated percentage of optional fields not completed by the user agency, whether or not the information was actually available in the police file.

10.5 Conduct of an Audit

10.5 Auditors shall:

a. audit the validity and accuracy of records entered on the CPIC system;

b. determine the system knowledge and proficiency of the agency personnel;

c. examine security screenings of personnel;

d. examine security at the terminal and/or interface site to ensure that minimum CPIC standards are being maintained;

e. conduct a follow-up verification within six months after the audit to ensure that minimum CPIC standards are being maintained;

f. ensure that policy and guidelines in the ***CPIC Reference Manual*** are adhered to by all agencies;

g. compile and distribute a report outlining their findings after each audit;

h. where justified, recommend a re-audit.

10.6 Responsibilities of the Audited Agency Head

10.6 The Head of a CPIC user agency being audited must:

a. make available to the auditors all applicable police files to confirm the validity for entering given records on the CPIC system ("police file" is described in Chapter I.2, sec. 7.4 **Police Files/Documents**; however,

1. in the case of microfilmed documents and police reports, it will be sufficient for the auditors to view the data on the microfilm reader without requiring the agency to print the hard copy;
2. in the case of automated record systems containing all documentation and police reports, it will be sufficient for the auditors to call up the data for viewing on the video display without requiring the agency to print the hard copy.

b. make available the police file or audit able record for **two months** after the record entry has been removed from CPIC, or until a subsequent validation has occurred;

c. render all necessary assistance to the auditors to enable a complete physical audit of their police files;

d. produce agency policy, directives or post orders, concerning the dissemination of CPIC information;

e. produce ***CPIC Reference Manuals*** and validation lists for the auditor's inspection upon request;

f. allow the auditors access to all CPIC terminals and interface sites to check security standards;

g. ensure that the personnel security screening procedures are strictly adhered to, as outlined in section 8;

h. attend, or designate a delegate to attend, the briefing and debriefing by the CPIC audit team;

i. submit a report to the auditing unit, when requested, detailing corrective actions taken with respect to problems identified;

j. remove or correct, at the request of an auditor, a record entry that does not conform with the ***CPIC Reference Manual***.

10.7 CPIC Field Services Analysis Section

10.7 CPIC Field Services Analysis Section, NPS, shall conduct periodic checks on the operational data base to detect inaccurate or invalid data.

10.8 Audit Cycle

10.8 The former two-year audit cycle has been replaced by a "risk analysis" strategy with a maximum four-year cycle for on-site audits.

a. CPIC Field Ops. Managers have the right to conduct an audit or re-audit even if it does not meet the 4-year cycle. They do not require the approval of the CPIC Advisory Committee Chairperson to do so.

10.9 The Chairperson of the CPIC Advisory Committee may request that a specific agency be audited by that agency's appropriate auditor, i.e. PSD, SQ, CPIC Field Ops. Section or CPIC Field Services Analysis Section.

10.10 An agency head may request an audit of his/her agency's records at any time, provided sufficient reasons (e.g., new personnel, unusual incidents) are given.

11. Narrative Traffic Use and Abuse

11.1 CPIC Field Services Analysis Section shall monitor narrative traffic log tapes and shall notify the agency concerned of all flagrant abuses of the system.

11.2 Agency supervisors and terminal operators must ensure that narrative traffic facilities are used for official police purposes only.

a. Narrative messages of an administrative nature must be authorized by the agency head or his/her designate. Administrative messages are to be disseminated only to those agencies having a vested interest in them. CPIC message switching facilities are not to be used for the transmission of personal messages.

11.3 The use of CPIC broadcast messages is restricted to urgent operational matters of regional, provincial or national importance.

CPIC national broadcasts of the type identified in chap. II.1, para. 2.1.b must be authorized and prepared either by the DG CPI Centre, or his delegate, or by Operations Branch, RCMP CIO Sector and transmitted by the Central Help Desk.

Note: Guidelines on the transmission of broadcast messages are outlined in Chapter II.1, para. 2 of this Reference Manual and also in the CPIC National Directory and must be adhered to.

12. Masterfiling

12.1 The practice of masterfiling shall be implemented by all CPIC user agencies when entering data on a person who is arrestable and/or for whom a warrant or apprehension order has been issued. See. ch. III.4, sec. 1.1 for a complete definition of the WANT category.

a. With masterfiling, the individual agency shall add a WANT record and any subsequent WANT files on that subject shall be added to the existing record through the MODIFY transaction.

b. On the CPIC system, the masterfiling method allows only one WANT record per agency for each subject.

c. For agencies who do not cross-reference same category records, it is encouraged that the CORE concept be used.

Note: Only one record entry per category will be permissible to attach to the same CORE in the following categories: MISSING, AND PAROLEE.

12.2 In the Persons File, use of during an add transaction will initiate a search for possible duplicate records. If duplicate records are identified, they must be amalgamated into one record. See ch. III.4, sec.2.1- **ONFILE**.

13. Screening Volunteers and Employees for Positions of Trust with the Vulnerable Sector

13.1 Definition of "Positions of Trust"

a. For CPIC purposes, "positions of trust" means paid or voluntary positions dealing with vulnerable people. Vulnerable people can include children, youth, senior citizens, people with physical, developmental, emotional, social, or other disabilities, but will also include people who have been victims of crime or accident, those who are addicted or dependent on addictive substances, and those who are otherwise left with little or no defence against persons who would harm them.

Note: Vulnerable people are individuals who are at ***greater risk*** of being harmed than the general population, because of their age, disability or handicap, or circumstances, whether temporary or permanent.

13.2 Responsibility for Screening

a. Only CPIC agencies with law enforcement authority (Category I) should use CPIC for the screening of persons entering into positions of trust.

13.3 Screening Procedures

a. Do not conduct a query on a person entering into a position of trust without first receiving a signed consent form. See Appendix I-2-D: **A "Best Practices Screening Model"** for details of screening practices.

Important: Signed consent forms must be retained in accordance with the provisions of the relevant Federal, Provincial or Territorial privacy legislation and agency retention and disposal schedules.

b. Complete the REMARKS field with the file number.

c.

d. In the written response (police clearance/certificate), clearly indicate whether or not the clearance is for employment with the vulnerable sector or for general employment purposes. This will ensure that the volunteer organization is aware of what checks were conducted.

13.4 Completing Form C-216 (Criminal Prints) in Cases of Sex-Related Offences

a. Identify any sex-related offence (adult or child victim) or family violence offence, irrespective of the actual charge and any court-imposed Publication Ban.

   1. This action will accommodate situations that result from "plea bargaining", convictions on a lesser charge and instances where the police know that the offence was sex-related but charges for a sex offence were not possible.

b. It is strongly recommended that CPIC agencies fingerprint all persons charged for a sex offence which can proceed by dual procedure, i.e. summary conviction or indictable.

13.5 Completing Form C-216C (Non-Criminal Prints) in Cases of Flagged Pardoned Sex Offences

   a. If completing form C-216C in response to the canned message received with a flagged pardoned sex offender record (see Chapter I.2, sec. 13.3 **Screening Procedures**), indicate this situation on the form.

Appendix I-2-A: Acknowledgment of Restrictions regarding CPIC access

Acknowledgement of Restrictions Respecting the Handling of CPIC Materiel, Records and Information

In this document:

- **"CPIC"** and **"CPIC system"** mean the Canadian Police Information Centre computer system, a National Police Service administered by the Royal Canadian Mounted Police;
- **"information"** includes knowledge of the contents of the CPIC system that has been acquired from the CPIC system or by virtue of a person's access to or employment in connection with the CPIC system, and also includes knowledge of the operation of the CPIC system;
- **"materiel"** means equipment, apparatus and supplies used in connection with the operation, use or maintenance of the CPIC system;
- **"records"** means correspondence, memoranda, papers, books, manuals, maps, photographs, films, microfilms, sound recordings, video recordings, computer cards and tapes and disks, and any other or all other information- or image-bearing materiel regardless of physical form or characteristics, that are made, received or preserved by any person in connection with the operation, use or maintenance of the CPIC system.

I acknowledge that I am fully aware of my responsibilities to safeguard all CPIC materiel, records and information with which I am entrusted or which I encounter by virtue of my employment.

I agree that all CPIC materiel, records and information with which I am entrusted must be dealt with in a manner that ensures it will not be disclosed to unauthorized persons, in particular:

1. CPIC materiel and records must not be removed from the confines of the office without the approval of my supervisor, and when any such materiel or records are removed, a record must be kept detailing what is being removed and to where it is being removed;
2. after working hours, all CPIC records and, where possible, materiel, must be secured from access by unauthorized persons;
3. all CPIC materiel and records connected with or arising out of my work must be kept in accordance with the preceding paragraphs 1 and 2;
4. all CPIC materiel and records must be turned in to my supervisor prior to my transfer or termination of my employment;
5. all CPIC information which I may acquire or to which I may have access at any time cannot, without lawful authority, be communicated or revealed to any other person or published in any form.

I acknowledge that I have read the foregoing instructions and acknowledgements and that I am fully aware that any breach of them could result in lawful sanctions including dismissal from my employment.

Witness Signature	Employee's signature
Witness Name (printed)	Employee's name (printed)

Termination Of Services

(To be completed when the Employee terminates his/her services)

Witness Signature	Employee's signature
Witness Name (printed)	Employee's name (printed)

I, the Employee above, declare that I have not in any way retained any CPIC materiel or records, and that I will continue to protect the confidentiality of all CPIC information in accordance with the above acknowledgement.

Appendix I-2-B: List of Category II and III Agencies

List of Category II and III Agencies (as of April 1, 2008)

The following agencies have received approval from the CPIC Advisory Committee to access the various CPIC data banks and/or communications system. In some instances, the Advisory Committee has imposed restrictions or has limited the access to those data banks.

AGENCY	CAT.	ACCESS	GROUP ID.
Federal			
Canada Border Services Agency, Borders Intelligence Division and Immigration Warrant Response Centre	II (B)	Enhanced	
Canada Firearms Centre / Chief Provincial Firearms Officers [opt out Provinces/Territories only]	III	Restriction 2	
Canada Revenue Agency, Enforcement and Disclosures Directorate, Criminal Investigations Division	II (B)	Standard	
Citizenship and Immigration Canada, Operational Management and Coordination	II (B)	Standard	
Correctional Service Canada, Correctional Services Division	II (C)	Standard	
Environment Canada, Enforcement Branch, Environmental Enforcement Directorate	II (B)	Standard	
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Strategic Research and Analysis Branch	III	Restriction 8	
Fisheries and Oceans Canada, Conservation and Protection Operations Branch	II (B)	Standard	
Foreign Affairs and International Trade Canada, Passport Canada, Passport Security Bureau	III	Restriction 9	
Industry Canada, Competition Bureau, Criminal Matters Branch and Fair Business Practices Branch	II (B)	Standard	

AGENCY	CAT.	ACCESS	GROUP ID.
National Parole Board, Clemency and Pardons	II (B)	Standard	
Parks Canada, Law Enforcement Section, Ecological Integrity Branch, National Parks Directorate	II (B)	Standard	
Transport Canada, Security and Emergency Preparedness Directorate, Intelligence Division	III	Restriction 7	
Alberta			
Alberta Department of Justice, Correctional Services Division	II (C)	Standard	
Alberta Gaming and Liquor Commission, Special Operations Division	II (B)	Standard	
Alberta Ministry of Government Services, Consumer Services Branch, Registries and Consumer Services Division	II (B)	Standard	
Alberta Motor Vehicle Industry Council, Investigations	II (B)	Standard	
Alberta Registry Services, Special Investigations Unit	II (B)	Standard	
Alberta Securities Commission, Enforcement Division	II (B)	Standard	
Alberta Solicitor General and Public Security, Public Security Division, Security Services Branch	II (A)	Standard	
Alberta Sustainable Resource Development, Fish and Wildlife Division, Enforcement, Field Services Branch	II (B)	Standard	
British Columbia			
British Columbia Ministry of Children and Family Development, Youth Justice Division, Youth Custody Services (Burnaby)	II (C)	Standard	
British Columbia Ministry of Employment and Income Assistance, Prevention and Loss Management Services	II (B)	Standard	
British Columbia Ministry of Environment, Conservation Officer Service	II (B)	Standard	
British Columbia Ministry of Finance and Corporate Relations, Financial Institutions Commission, Investigation Department	II (B)	Standard	
British Columbia Ministry of Small Business and Revenue, Strategic Initiatives and Administration Division, Special Investigations Branch	II (B)	Standard	
British Columbia Ministry of the Attorney General, Corrections Branch	II (C)	Standard	

AGENCY	CAT.	ACCESS	GROUP ID.
British Columbia Ministry of the Attorney General, Court Services Branch	II (C)	Standard	
British Columbia Ministry of the Attorney General, Gaming Policy and Enforcement Branch	II (B)	Standard	
British Columbia Ministry of Public Safety and Solicitor General, Security Programs Division	III	Restriction 7	
British Columbia Securities Commission, Enforcement Division	II (B)	Standard	
Insurance Corporation of British Columbia (ICBC), Special Investigations Unit	II (B)	Standard	
Manitoba			
Manitoba Department of Finance, Taxation Division, Special Investigations Unit	II (B)	Standard	
Manitoba Gaming Control Commission, Gaming Integrity Branch, Investigations and Registration Investigations Units	II (B)	Standard	
Manitoba Justice, Aboriginal and Community Law, Public Safety Investigation Unit	II (B)	Standard	
Manitoba Justice, Corrections Division, Adult and Youth Corrections Services	II (C)	Standard	
Manitoba Public Insurance Corporation, Special Investigation Unit	II (B)	Standard	
New Brunswick			
New Brunswick Department of Natural Resources and Energy, Regional Resources Division	II (B)	Standard	
New Brunswick Department of Public Safety, Safety Services Division, Licensing and Records Branch	III	Restriction 7	
New Brunswick Department of the Solicitor General, Correctional Services Division	II (C)	Standard	
Newfoundland and Labrador			
The High Sheriff of Newfoundland and Labrador, Court Security Division	II (C)	Standard	

AGENCY	CAT.	ACCESS	GROUP ID.
Nova Scotia			
Nova Scotia Department of Justice, Correctional Services	II (C)	Standard	
Nova Scotia Department of Justice, Public Safety Investigations Section, Public Safety Division	II (B)	Standard	
Nova Scotia Department of Justice, Security Programs, Policing and Victim Services Division	III	Restriction 7	
Nova Scotia Department of Natural Resources, Enforcement Division	II (B)	Standard	
Ontario			
Ontario Ministry of Children and Youth Services, Youth Justice Services Division	II (C)	Standard	
Ontario Ministry of Community Safety and Correctional Services, Correctional Services Division	II (C)	Standard	
Ontario Ministry of Community Safety and Correctional Services, Ontario Police College, Aylmer, Ontario	III	Restriction 1	
Ontario Ministry of Consumer and Commercial Relations, Investigation and Enforcement Section	II (B)	Standard	
Ontario Ministry of Environment, Investigation and Enforcement Unit	II (B)	Standard	
Ontario Ministry of Finance, Special Investigations Branch	II (B)	Standard	
Ontario Ministry of Financial Institutions, Financial Services Commission of Ontario, Investigations Unit	II (B)	Standard	
Ontario Ministry of Natural Resources, Enforcement Branch	II (B)	Standard	
Ontario Ministry of the Attorney General, Special Investigations Unit	II (B)	Standard	
Ontario Ministry of the Solicitor General and Correctional Services, Private Investigators and Security Guard Registration and Investigations Branch	II (B)	Standard	
Ontario Ministry of Transportation (MTO), Carrier Safety and Enforcement Branch	III	Restriction 6	
Ontario Securities Commission, Enforcement Branch	II (B)	Standard	
Quebec			

AGENCY	CAT.	ACCESS	GROUP ID.
École nationale de police du Québec	III	Restriction 1	
Ministère de la Sécurité publique du Québec, Direction des services de sécurité et de protection (DSSP)	II (B)	Standard	
Services Correctionnels du Québec (SCQ)	II (C)	Standard	
Société d'Assurance Automobile du Québec (SAAQ)	III	Restriction 5	
Saskatchewan			
Saskatchewan Environment and Resource Management, Enforcement and Compliance Branch	II (B)	Standard	
Saskatchewan Finance, Investigations and Enforcement Unit, Revenue Division	II (B)	Standard	
Saskatchewan Financial Services Commission, Enforcement Branch, Securities Division	II (B)	Standard	
Saskatchewan Government Insurance, Securities and Special Investigations Unit	II (B)	Standard	
Saskatchewan Highways and Transportation, Transport Compliance Branch	II (B)	Standard	
Saskatchewan Justice, Adult Corrections and Public Safety	II (C)	Standard	
Saskatchewan Justice, Safer Communities and Neighbourhoods (SCAN)	II (B)	Standard	
Saskatchewan Justice, Law Enforcement Services Branch (for the Private Investigators and Security Guards Program and the Vehicle Impoundment Against Sexual Exploitation Program)	III	Restriction 3	
Saskatchewan Liquor and Gaming Authority, Regulatory Compliance Division, Compliance Branch	II (B)	Standard	
Yukon Territory			
Yukon Department of Justice, Community and Correctional Services Branch, Whitehorse Correctional Centre (WCC)	II (C)	Standard	
Various			

AGENCY	CAT.	ACCESS	GROUP ID.
Atlantic Police Academy, Charlottetown, P.E.I.	III	Restriction 1	
Calgary Transit, Protective Services	II (B)	Standard	
Canadian National Police, Department of Investigations	II (A)	Standard	
Canadian Pacific Railway Police Service	II (A)	Enhanced	
City of Ottawa Transit Services (OC TRANSPO), Transit Law Enforcement Unit	II (A)	Standard	
Insurance Bureau of Canada, Investigative Services	III	Restriction 4	
Niagara Parks Commission, Niagara Parks Police Service	II (B)	Standard	
Toronto Community Housing Corporation, Security Services Department	II (A)	Standard	
Toronto Transit Commission, Corporate Security Department	II (A)	Standard	
University of Saskatchewan, Department of Campus Security	II (A)	Standard	
University of Toronto Police Services	II (A)	Standard	

Restriction Notes:

1. Access to the CPIC Instructional Data Base and narrative traffic facilities only.
2. Access for operational queries and CPIC Communications system (narrative traffic). Query and maintenance of FIP persons and property records.
3. Access to the CPIC Communications system and direct access ONLY to the Identification and Ancillary Data Banks with the following exclusions: *Youth Criminal Justice Act* records, federal and provincial Corrections records.
4. Access to the CPIC Communications system (narrative traffic) and operational queries of the Vehicle File.
5. Access to the CPIC Communications system (narrative traffic) only.
6. Access to the Investigative, Identification and Ancillary Data Banks.
7. Access for operational queries of CPIC Persons File, the Identification Data Bank files and the CPIC Communications system.
8. Access to the Investigative, Identification and Ancillary Data Banks with the following exclusions: *Youth Criminal Justice Act* records.
9. Access for operational queries to the Investigative, Identification and Ancillary Data Banks, the CPIC Communications system, and standard maintenance of the Persons File and Property File of the Investigative Data Bank specifically for the maintenance of lost or stolen passports and related secondary records.

Appendix I-2-C: CPIC Code of Ethics

1. Introduction to CPIC Code of Ethics

1.1 Purpose of the Code of Ethics

This Code of Ethics for CPIC users establishes procedures and safeguards to promote the maintenance of good practice and compliance with privacy protection legislation as may be enacted within the various jurisdictions of Canada and the federal Privacy Act, proclaimed July 1, 1983.

Computers have become essential and have already proved to be of benefit to the police in their service to the public but, as a large proportion of the data held on police computers relates to individuals, it is also essential that a framework be established to ensure public confidence in police computer operations. This *Code of Ethics* establishes that framework.

The collection, maintenance and use of personal information by the Canadian police community must be limited to that which is required to uphold and enforce the laws of those collective jurisdictions within which the information is accumulated. The responsibility then falls on each contributor and each recipient of information to ensure the principles which constitute this *Code of Ethics* are followed and upheld while the information is in their possession.

The Canadian Police Information Centre provides a central repository into which the various police jurisdictions within Canada enter electronic representations of information they collect and maintain. Not all information in the CPIC data banks is personal information. That which is, however, deserves to be protected from abuse of the privilege accorded by its availability to authorized recipients. No single piece of legislation is able to offer an umbrella under which personal information stored in CPIC data banks could be sheltered against the abuses most often associated with the collection and distribution of personal information. The gathering and maintenance of personal information contained within the CPIC data banks is subject to the governing legislation of the jurisdiction under which it is gathered.

This could be any one of the federal, ten provincial, three territorial, or myriad municipal governments within Canada. Many jurisdictions have no specific legislation which ensures the protection of personal privacy in the realm of data collection, maintenance and distribution. In the absence of an all-encompassing rule of law, compliance with the spirit of fair information handling practices is demanded of those senior administrators who govern the operations and policies of the Canadian Police Information Centre.

1.2 Scope of the Code of Ethics

This *Code of Ethics* is a general statement and does not set out detailed rules which must be followed by each participant police jurisdiction. However, the CPIC Advisory Committee, by their endorsement of this *Code of Ethics*, resolves to promote these general principles through positive and direct action within their respective jurisdictions. Jurisdictions will be encouraged to create local procedures, by way of written directives to their membership, which reflect the principles enunciated here. Jurisdictions are further encouraged to establish methods of promulgating these principles through training sessions, audits and managerial reviews.

For its part, as custodian of the data banks, the Royal Canadian Mounted Police, through CPI Centre, agrees to incorporate this *Code of Ethics* into the *CPIC Reference Manual*; to incorporate the principles contained herein into various training courses and documents provided to trainees; to incorporate into its *Audit Standards Procedures Manual*, direction to auditors to examine, evaluate and report on the degree to which these principles have been applied in each agency they are responsible to audit; and to vigorously promote the principles of this *Code of Ethics* at every appropriate opportunity.

2. Principles Of Data Gathering, Maintenance And Distribution

2.1 PRINCIPLE 1

"Information to be contained in personal information must be obtained in a fair and lawful manner and in accordance with legislation which permits it to be gathered and held."

2.1.1 Interpretation

Information which identifies a person and which constitutes personal information shall be deemed to have been collected fairly and lawfully if it is obtained:

a. from a person who is the subject to whom the personal information pertains and provides it voluntarily;

b. in accordance with any legislative provisions; or

c. from a person who is under a legal obligation to supply it.

2.1.2 Obtaining Information

In the process of collecting personal information for law enforcement purposes, it is often inappropriate or impractical to inform the person who is the subject of personal information being collected, the purpose for which the personal information is required. This most often applies on those occasions in which the whereabouts of the subject of the personal information is unknown, due to an attempt to evade legal prosecution for a breach of the law.

Persons causing personal information to be added to computerized police records must always be in a position to show the source of that information and the reason for the entry, either from computer or manual records or other official documents.

Personnel acting on behalf of a law enforcement jurisdiction are permitted to obtain, record and hold personal information where its purposes are related to the following broad category definitions:

a. the prevention, detection or suppression of crime;

b. the enforcement of any law;

c. the apprehension or prosecution of offenders;

d. the assessment or collection of taxes or fines imposed under any enactment or by a court of law; or

e. the provision of assistance to or protection of the public.

2.1.3 Agreements for Use of Personal Information not under Police Control

Where personal information is obtained from a third-party source without the knowledge of the person to whom the personal information pertains, the purposes must be consistent with either (a),(b),(c),(d) or (e) above.

The use of personal information from third-party non-police data banks, i.e. Provincial and Territorial Motor Vehicles Bureau, is authorized for purposes of law enforcement, by federal/provincial/territorial agreements. Nevertheless, CPIC will execute individual memoranda of agreement with the custodians of those non-police data banks and will make this agreed use a matter of public record by way of publication in the *Infosource.*

2.2 PRINCIPLE 2

"Personal information in the CPIC computerized data banks shall be held and used only for one or more specified and lawful purposes."

2.2.1 Interpretation

Personal information shall not be treated as held for a specified purpose unless that purpose is described in particulars of the Infosource, unless the purpose for which that personal information is held is specifically exempt from registration under the federal Privacy Act or an Act of a province, territory or municipality.

2.3 PRINCIPLE 3

"Personal information held for any purpose or purposes shall not be used or disclosed in any manner inconsistent with that purpose or those purposes."

2.3.1 Interpretation

Personal information shall not be considered as used or disclosed in contravention of this Principle unless:

a. used other than for a purpose as described in the Infosource, or its provincial or municipal counterparts in relation to the data; or

b. disclosed other than to a person described by the CPIC Reference Manual as being an authorized recipient of the data.

2.3.2 Use of Personal Information

Personal information contained in the CPIC computerized data banks which is retained for a purpose or purposes listed in the Infosource, shall not be used as "tombstone data" around which a separate record in another automated data bank will be created (data matching) except:

c. where the other automated data bank is already listed in the Infosource as one of the several data banks of the Canadian Police Information Centre, or is a data bank legally exempt from registration in the Index; and

d. each separate record is created at the time a contributor first makes an entry and each record is considered "owned" by the same contributor, whether or not the records reside in the same data bank.

2.3.3 Disclosure

It is essential that any disclosure of personal information should be authorized at the appropriate level and be in accordance with instructions specifically drafted for that purpose. These instructions MAY BE MORE RESTRICTIVE than the authorized disclosure regulations shown in the **CPIC Reference Manual**.

Disclosure of computerized information may take many forms, including viewing records on computer screens, computer printout, typewritten material which includes information taken from computerized records, by word of mouth or by radio transmissions.

It is essential that all agencies authorized to access CPIC data banks provide guidelines as to the release of information containing personal information. These guidelines must state to which organizations, agencies, persons or authorities information may be disclosed, by whom and in what circumstances.

There will be instances of disclosure of personal information where no specific guidelines exist, as in:

a. threats to National Security, where disclosure is for the purpose of safeguarding national security;

b. international agreements (i.e. Interpol) where the disclosure is clearly for law enforcement purposes;

c. disclosure required by enactment or a court order;

d. disclosure for legal advice or for use in legal proceedings;

e. disclosure to the data subject or to a person acting on behalf of the data subject;

f. disclosure at the request of or with the consent of the data subject;

g. disclosure urgently required to prevent injury or damage to the health of any person or persons.

2.4 PRINCIPLE 4

"Personal information shall be accurate and where possible, kept up to date."

2.4.1 Interpretation

Any question of whether personal information is accurate or not, will be acted upon at the earliest opportunity.

2.4.2 Methods of Assurance

The personal information in CPIC data banks is always subject to normal human failings such as mis-spelling, transposition and others due to the numerous agencies involved in entering data. Work standards differ and the checks and balances in one unit may be stronger than in another.

In order to combat these pitfalls, CPIC standardizes training courses for operators (entry personnel) then follows up with comprehensive audits and monthly validation reports of entered data for each agency that is permitted to add personal information. To avoid as much as possible instances where data, which is inaccurate, could lead to a problem, a directive known as "Hit Confirmation" is in place. This requires that no action be taken, based on a record in CPIC, without the agency making the hit first confirming its validity and accuracy with the agency owning the entry.

Agencies authorized to make entries containing personal information to the CPIC data banks must institute work reviews or verification processes which assure the highest possible degree of accuracy in their entries.

Agencies must also observe the requirement to review their validation printouts, both for accuracy and timeliness of the data.

Agencies are also encouraged to adopt procedures which will ensure, as far as possible, that inaccurate personal information is not entered into a data bank by:

a. ensuring that the source of the information is reliable;

b. taking steps to verify information, if possible, with another source or if reasonable, with the data subject at the time of collection; and

c. ensuring that procedures for data entry and the automated processes which may form a part thereof, do not themselves introduce inaccuracies.

Where inaccuracies do come to light, the Canadian Police Information Centre, for its part, commits to taking all steps at its disposal to lessen any damage or distress caused to a data subject by ensuring that inaccurate information is corrected as soon as possible.

As well, CPIC, through its logging facilities, will wherever possible assist any agency which is prepared to commit to the same obligation and endorsement of this *Code of Ethics*.

2.5 PRINCIPLE 5

"Personal information held on CPIC data bases for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

2.5.1 Assurances

There are in existence, several enactments of legislation which determine the length of time a record belonging to a department of the federal government may be retained. Those records on CPIC which are entered by any agency subject to this legislation, are governed by these rules. CPIC is fully compliant in this respect. Beyond this, in order to meet the spirit of the above principle, CPIC depends on its Reference Manual Standards and on periodic audits to ensure that no personal information is held in CPIC data banks longer than is necessary for the purpose it was entered. Any agency who properly completes the task of "monthly validation" using the printouts supplied by CPIC, will also be compliant.

2.5.2 Personal Information Held by Law Enforcement Agencies

The circumstances in which CPIC is required to operate its automated data banks make it impossible to lay down hard and fast, absolute rules about how long items of personal information, which form part of a CPIC record, should be retained.

For example, it is clear that Criminal Records information supported by fingerprints will be retained as directed by the *Identification of Criminals Act*, the *Criminal Records Act* and the *Youth Criminal Justice Act*. These records and their associated personal information exist exclusively in the Identification data bank of CPIC.

The personal information contained in the Investigation and Intelligence data banks are treated quite differently. In most instances, the taking of a required action by an officer, as detailed on the computerized record, will necessitate the immediate cancellation and removal of that personal information. An example would be when a warrant is executed as a result of an arrest. Failure to remove such data when the purpose for the record has been served will result in irrelevant, excessive and out-of-date data being held. The *CPIC Reference Manual* is quite specific in this regard and again, the actions of record owners are monitored through monthly validation lists and periodic audits.

Of necessity and in keeping with its purpose, the personal information held in CPIC's Intelligence data bank is generally informational as opposed to actionable. It is gathered and retained for the general purposes of prevention, detection and suppression of crime, therefore is not always subject to removal as a result of some action being taken. The need to retain or remove such data can only be judged from the nature of the information, the person to whom it relates and the circumstances prevailing at the time in question. Nevertheless, the CPIC rules of verification and audit apply equally to this data when viewed in light of its accuracy, relevance to purpose, or excessiveness. Such records containing personal information should be reviewed (annually is suggested) from an "intelligence" perspective and removed if no longer of relevance.

CPIC does not have the right to impose retention rules on the data storage facilities of agencies who are the contributors to CPIC data banks. Once removed from the CPIC data banks, personal data belonging to a contributor is beyond our influence. Acceptance of this *Code of Ethics*, however, implies that the same stringent data handling practices CPIC imposes on itself, will be promulgated to the greatest degree possible, within the agencies it serves.

2.6 PRINCIPLE 6

(a) "In those instances where a CPIC Agency is registered as the record owner, an individual is entitled to request access from that agency who, without undue delay or expense:

(i) may grant disclosure of that information, where appropriate; and

(ii) where appropriate, such data may be corrected or erased.

(b) In those instances where access is requested and that CPIC agency is not the registered owner of a record in the CPIC data banks, the agency will consult with the record owner and will identify the owner of the record, when appropriate.

Nothing in either (a) or (b) above overrides the exemption provisions of the federal Privacy Act or of any provincial or territorial legislation which might apply."

2.6.1 Criteria Necessary for Compliance

Persons making requests must adequately identify themselves and provide sufficient information for it to be determined that the individual making the request is, in fact, the subject of the CPIC data bank record. Where the owner of a CPIC data bank record establishes that additional information is required to satisfy the link of a data bank record to the individual making the enquiry, additional information may be sought.

Before refusing to comply with a request, on the basis of insufficient information having been provided, a record owner will ensure that:

a. the individual can be reasonably expected to give, or obtain the further information requested; and/or

b. the data bank record cannot be obtained without the further information being supplied.

When a request is made through an agent acting on behalf of an individual, permission for the agent to act on the subject's behalf should be provided in writing, otherwise a record owner may refuse to release information to the agent. Such requests may also be confirmed with the record subject before a release is authorized.

2.6.2 Correction and Erasure

When it is established and confirmed that a record in the CPIC data banks contains personal information which is incorrect in its content and therefore does not accurately reflect the personal information of the subject to whom it pertains, CPIC agency personnel will take action immediately to have the personal information corrected.

Since all personal information in the CPIC data banks must be substantiated by a record held by the record owner, this original source of data must be first corrected and followed by a correction to the CPIC data bank entered by the record owner.

A CPIC data bank record containing personal information may be removed at the subject's request if:

a. some enactment or legislation provides for its removal;

b. the personal information is irrelevant or no longer required for the purpose for which it was gathered.

Nothing in the above statements gives an individual any right to have a CPIC data bank record containing personal information removed merely because the subject of the data would prefer that the owner of the record not keep that information about the individual.

2.7 PRINCIPLE 7

"Appropriate security measures will be taken to prevent unauthorized access to, or alteration, destruction or disclosure of, personal information and against accidental loss or destruction of personal information."

2.7.1 Interpretation

Regard shall be had:

a. to the nature of the personal information and the harm that would result from such access, alteration, disclosure, loss or destruction; and

b. to the place where the personal information is stored, to security measures programmed into relevant computer equipment and to measures taken for ensuring the reliability of staff having access to the personal information.

2.7.2 Essential Elements of Compliance

Access to personal information is permitted only for purposes necessary for the efficient discharge of legitimate law enforcement duties. Personal or private use of personal information stored in CPIC data banks and in police computer systems is strictly forbidden.

Where possible, records of transactions must be kept which identify the persons responsible for initiating and handling a request for records containing personal information.

As custodians of personal information, law enforcement agencies have an obligation to protect that personal information while it is in their care. Law enforcement, by its very nature, requires agencies, at times, to infringe on the rights of others, for instance when arresting and incarcerating subjects. In exercising the powers given under the rule of law, there must be no appearance of abuse of that power nor any unjustified excesses in relation to those elements which come into play in the process. Most often, the abuses referred to are those elements such as loss of freedom, personal possessions and dignity. Law enforcement authorities must train themselves to also consider personal information in that light. To hold personal information when

there is no right or need to do so is also looked upon as an unnecessary abuse of the legislated authority granted under the rule of law.

This Advisory Committee to the Canadian Police Information Centre recognizes its obligations both under the law and to the law. There exists within our collective minds the realization that one clear set of rules, applied to us all, is not a hardship but rather a guarantee that the spirit of privacy legislation will be endorsed and respected no matter where in Canada persons come into contact with the agencies of law enforcement.

Appendix I-2-D: Using CPIC for screening purposes

Part I - A: "Best Practices Screening Model"

The following elements can be adapted by local groups and police agencies to best respond to the needs of their communities for screening volunteers and employees who work with vulnerable people.

1. The hiring organization would first determine what types of offence and what time frame would be cause for refusing the services of a job applicant or would be grounds for a dismissal, e.g., the relevancy of a shoplifting offence committed 15 years earlier, as compared with a serious violent offence against a vulnerable person any time.
2. A "job description" would be developed that would identify the expected involvement of a person with vulnerable people, e.g., a member of the Board of Directors, a member conducting the meetings with vulnerable people, and the possibility of the volunteer driving a vulnerable person to/from an activity.
3. Based on the job description, the organization would conduct a risk analysis and initiate the screening process for those positions which would have direct contact with vulnerable people.
4. When a person offers his/her services, the organization should interview the person to ensure they realize that a screening will occur and that a police records check will form part of that screening and may divulge the existence of a CPIC record, a criminal record and/or a pardoned record.
5. The organization should also request that the applicant supply character references and the organization should contact these references to determine suitability. The results of all these checks would form part of a follow-up interview of the applicant by the organization.
6. In addition to an initial screening, the organization should also have policy in place for the routine updating of the screenings, again based on risk analysis. It could be that an agency director might only be screened once every five years; however, a volunteer with direct contact with vulnerable people might be screened every one or two years, or more frequently.
7. Local police services would work with local agencies and employers, ideally through a memorandum of understanding (MOU) outlining their respective obligations in providing and seeking a police records check (including, for example, the type of screening response to be released by the police; an accepted consent to disclosure form; to whom the response would be released; and the obligations of the volunteer agency/employer to protect the privacy of the volunteer/employee by implementing records maintenance procedures).
8. An individual, who is seeking employment in a position dealing with vulnerable people and has been accepted as a successful candidate for the position, would be required to sign a consent to disclosure form provided to him/her by the volunteer agency/employer and would personally take it to the local police agency and provide appropriate identification, including photo ID. The police would then conduct a thorough CPIC and local police database check.
9. Police would then release a written response to the individual indicating that, based on the information provided, the individual does not have a criminal record or that the individual may have a criminal record and verification can only be provided through a fingerprint search. It should be clearly indicated whether or not the clearance is for general employment purposes or for employment with the vulnerable sector. It should also be noted that, as an alternative, some police services choose to return the screening report directly to the agency where the applicant has signed a waiver in

accordance with the *Privacy Act* consenting to third party disclosure to the paid or volunteer employer. However, *Youth Criminal Justice Act* records, pardoned criminal records, and other local police arrest and investigative information may not be able to be released directly to third parties.

10. An individual who is given a positive response may show it to the volunteer agency/employer. Based on current information, an individual who is given an unfavourable response will likely weed himself/herself out because he/she knows that a fingerprint search will disclose a record for an offence that would be relevant to the position sought, including the existence of a pardoned record.
11. Alternatively, the individual will deny having a criminal record. The subject will submit to a fingerprint search, with a covering letter from the organization if for a volunteer position. The fingerprint search will then provide verification. If a criminal record is disclosed, the individual may discuss it with the agency/employer on the basis that the record is not relevant to the position sought (for example, a 10-year-old conviction for theft under $1000 is not likely to be relevant to a position involving access to vulnerable people).

Those communities currently using this approach to carry out screenings believe that there are several advantages to such a model:

- The police do not expurgate the criminal record and would not, therefore, be exposed to subsequent accusations that they did not disclose certain convictions that the particular volunteer agency would have considered relevant.
- Disclosure of the record to the individual himself/herself does not constitute publication and does not raise privacy concerns because the information does not go directly to the volunteer agency/employer and limits opportunities for inappropriate use of the information by the volunteer agency/employer.
- Disclosure of the record to the individual would allow a young offender, seeking a position dealing with vulnerable people, to obtain disclosure of his/her young offender record in accordance with the *Youth Criminal Justice Act*.
- Disclosure of the record to the individual would also allow a person with a pardoned criminal record, seeking a position dealing with vulnerable people, to obtain disclosure of his/her pardoned criminal record in accordance with the *Criminal Records Act*.
- The expense of a fingerprint search is only incurred by the individual or volunteer agency/employer at the "second" level of screening if the initial police criminal records check indicates a possible record.
- It promotes community policing and encourages volunteer agencies/employers to develop comprehensive screening and continuing supervision policies, of which police criminal records checks are but one component, in consultation with local police agencies.
- It avoids delays in obtaining the results of criminal records checks that would necessarily result with the implementation of a "central" clearinghouse for the entire country.

Form 1 - Consent for a Criminal Record Check

If you have access to the RCMP Intranet, you can find this form at the location listed below. Note that the ICS Viewer must be installed on your computer. Instructions for installation are available on the site.

http://infoweb.rcmp-grc.gc.ca/cio/bs/im/bpas/Forms/ics_index/ICS/3923e.xfd

Royal Canadian Mounted Police / Gendarmerie royale du Canada
Canadian Police Information Centre / Centre d'information de la Police canadienne

Form 1

CONSENT FOR A CRIMINAL RECORD CHECK FOR A SEXUAL OFFENCE FOR WHICH A PARDON HAS BEEN GRANTED OR ISSUED

This form is to be used by a person applying for a position with a person or organization responsible for the well-being of one or more children or vulnerable persons, if the position is a position of authority or trust relative to those children or vulnerable persons and the applicant wishes to consent to a search being made in criminal conviction records to determine if the applicant has been convicted of a sexual offence listed in the schedule to the Criminal Records Act and has been pardoned.

Identification of the Applicant

Surname	Given Name(s)	Sex
		◯ Male ◯ Female

Date of Birth (Y-M-D)	Place of Birth	Current Address

Previous addresses, if any, within the last 5 years

Reason for the Consent

I am an applicant for a paid or volunteer position with a person or organization responsible for the well-being of one or more children or vulnerable persons.

Description of the paid or volunteer position	Name of the person or organization

Details regarding the children or vulnerable person(s)

Consent

I consent to a search being made in the automated criminal records retrieval system maintained by the Royal Canadian Mounted Police to find out if I have been convicted of, and been granted a pardon for, any of the sexual offences that are listed in the schedule to the Criminal Records Act.

I understand that, as a result of giving this consent, if I am suspected of being the person named in a criminal record for one of the sexual offences listed in the schedule to the Criminal Records Act in respect of which a pardon was granted or issued, that record may be provided by the Commissioner of the Royal Canadian Mounted Police to the Minister of Public Safety and Emergency Preparedness Canada, who may then disclose all or part of the information contained in that record to a police force or other authorized body. That police force or authorized body will then disclose that information to me. If I further consent in writing to disclosure of that information to the person or organization referred to above that requested the verification, that information will be disclosed to that person or organization.

Signature of Applicant	Date (Y-M-D)

Canada — A National Police Service of the Royal Canadian Mounted Police

RCMP GRC 3923e (2006-07)

Form 2 - Consent to Disclosure of Record

If you have access to the RCMP Intranet, you can find this form at the location listed below. Note that the ICS Viewer must be installed on your computer. Instructions for installation are available on the site.

http://infoweb.rcmp-grc.gc.ca/cio/bs/im/bpas/Forms/ics_index/ICS/3924e.xfd

Canadian Police Information Centre Form 2

CONSENT TO DISCLOSURE OF RECORD

This form is to be used by a person who has consented to a search being made in criminal conviction records by completing the form called "Consent for a Criminal Record Check for a Sexual Offence for Which a Pardon Has Been Granted or Issued" and who wishes to consent to the disclosure of information obtained in that search to the person or organization who requested the search.

Identification of the Person Consenting

Surname	Given Name(s)	Sex
		◯ Male ◯ Female

Date of Birth (Y-M-D)	Place of Birth	Current Address

Previous addresses, if any, within the last 5 years

Reason for the Consent

I am an applicant for a paid or volunteer position with a person or organization responsible for the well-being of one or more children or vulnerable persons.

Description of the paid or volunteer position	Name of the person or organization

Details regarding the children or vulnerable person(s)

Consent

I consent to information contained in a criminal record, found as a result of a criminal record check for a sexual offence for which a pardon has been granted or issued, being disclosed by a police force or other authorized body to the person or organization referred to above to whom or to which I am applying or have applied for a paid or volunteer position.

I understand that as a result of giving this consent, that information will be disclosed by the police force or other authorized body to the person or organization, even though a pardon has been granted or issued for the offence.

Signature of Applicant	Date (Y-M-D)

Canada A National Police Service of the Royal Canadian Mounted Police

RCMP GRC 3924e (2001-11) ICS

Appendix I-2-E: Computer Virus Prevention Procedures

Appendix I-2-F: ITSC Charter

A. Introduction

The **CPIC Information Technology Sub-Committee** is a successor to the Interface Sub-Committee which had been created in 1972 by the CPIC Advisory Committee (A/C). The IT Sub-Committee was formed by the members of the CPIC A/C during their November 1996 meeting in Ottawa. Members of the A/C were asked to identify representatives for the IT Sub-Committee. A CPI Centre technical representative was also identified. The establishment of the IT Sub-Committee was approved by the CPIC Advisory Committee in January 1997, to ensure appropriate technical input from federal, provincial and municipal law enforcement agencies in the operation of CPIC.

B. Rules of Conduct

The following Rules of Conduct provide a mechanism for the conduct of the IT Sub-Committee's activities. They provide terms of reference for the Sub-Committee, establish its composition, clarify the roles of the Chair and the Vice-Chair, and establish how meetings will be convened and conducted.

TERMS OF REFERENCE

Mandate and Responsibilities

The Information Technology Sub-Committee is a sub-committee under the direction of the CPIC Advisory Committee. It is responsible for recommending the IT policies to the CPIC Advisory Committee and recommending standards and parameters, including security and network security, inter-connectivity protocol and data sharing standards to the CPIC system for all agencies and to review and recommend information technology standards for the Canadian law enforcement community as it relates to the CPIC system and NPSNet.

> **Triumvirate Mission Statement:** A sub-committee under the direction of the Information Technology Sub-Committee (ITSC), composed of the Director General, CPI Centre (Chair), the Officer in Charge RCMP Departmental Security and the Officer in Charge Network Services, Chief Information Officer Sector. The Triumvirate's mandate is to review requests for connection to CPIC and to provide interim approval of security posture pending endorsement at ITSC.

Scope

The IT Sub-Committee will focus on:

- developing and recommending policy with respect to connectivity, security, infrastructure and standards related to the CPIC System;
- reviewing and addressing technological concerns related to all aspects of networked access to NPSNet, LANS, WANS, and/or Mobile Work Stations, Mobile Data Terminals, and Mobile Intelligent Terminals;

- providing ongoing technical advice related to technical options to assist in implementing new business requirements;
- providing recommendations to the CPIC Advisory Committee as to the acceptability of a request by an approved Agency to interface to CPIC and also interconnect, e.g., WAN to WAN and LAN to WAN. Such recommendations would include as a minimum, a technical assessment and a security assessment. The IT Sub-Committee may give interim approval on these requests;
- advising/providing recommendations to the CPIC Advisory Committee regarding technical issues related to the present operations and future development of the CPIC system and its related infrastructure.

Standards

Technical standards recommended by the IT Sub-Committee should be the standards that take into consideration the evolutionary nature of information technologies and the stage at which CPIC users are at in this evolution.

Reporting

The IT Sub-Committee reports via the Chairperson to the CPIC Advisory Committee. Reports shall be presented to the CPIC Advisory Committee at its regular meetings.

Amendment to Rules of Conduct

Proposed amendments to the IT Sub-Committee Rules of Conduct must be received by the Chair in bilingual format at least 20 working days before the meeting at which the amendment will be considered. Amendments will be made by adoption of a motion containing the exact wording of the change and the effective date of change. A two-thirds majority of the voting members present is required for the motion to pass. Acceptance, amendment, or suspension of these Rules of Conduct shall be affirmed by a two-thirds majority of the voting members. The agreed upon motion will then be forwarded to the Chair of the CPIC Governance Sub-Committee for consideration and furtherance to the CPIC Advisory Committee for approval.

COMPOSITION

Membership

The IT Sub-Committee shall be composed of a Chair and no more than 11 voting members, from a variable number of members relative to the participating agencies, to be accepted by the Chair.

Participation on the IT Sub-Committee must be confirmed and approved by the Chair of the IT Sub-Committee.

Participating Members

Participating members are members whose contribution to the work of the IT Sub-Committee is sought because of a requirement for their technical support or for their general contribution in terms of exchange of information and liaison with specific organizations. Participants may be; from rotating agencies, invited by the Chair, or invited by a voting member if approved by the Chair. Invited participants are welcomed on a per meeting basis. These persons shall not be allowed to vote. The number of participating members will be limited. They will be accepted by the Chair of the CPIC IT Sub-Committee. They will attend meetings at their own expense unless otherwise directed, in writing, by the Chair. Financial authority rests with the Director General of the CPI Centre.

Voting Members

All voting members must have thorough knowledge of IT issues, and be informed as to law enforcement and/or criminal justice issues as they relate to their respective agencies or associations.

Roles and Responsibilities of Voting Members

Provide the IT Sub-Committee with information on specific issues, new requirements or concerns of law enforcement and criminal justice agencies; and inform, obtain input, and discuss with their constituencies and other stakeholders they represent.

Term of Appointment

Members shall be appointed for a minimum period of two years, commencing the day following their appointment. Should a member resign or have to be replaced because he or she cannot attend regular meetings, a replacement shall be designated by the parent organization. The following Table outlines the ITSC membership:

Table 1 - CPIC IT Sub-Committee Membership

	Voting Members	Participants
Chairperson		
Federal Government Departments:		
Public Safety Canada		
RCMP/Chief Information Officer Sector	1	1
RCMP Criminal Intelligence Service Canada (CISC)	1	1
RCMP Canadian Police Information Centre (CPIC)		1
RCMP OIC Departmental Security		
Correctional Services Canada (CSC)	1*	
Canada Border Services Agency (CBSA)	2 year appt./rotational	
Atlantic Provinces:		
Municipalities	1 2 year appt./rotational	
Québec:		
CRPQ	1	
Sûreté du Québec	1*	
Quebec Association of Chiefs of Police	2 year appt./rotational	

Ontario:		
Ont. Min. of Community Safety & Correctional Svcs (PSD)		1
Ontario Provincial Police	2*	2 year rotational
Ontario Association of Chiefs of Police	2 year appt./rotational	
Toronto		
Prairie Provinces:		
Manitoba	1*	
Saskatchewan	2 year appt./rotational as decided by regions	
Alberta		
British Columbia:		
Ministry of the Attorney General & Correctional Svcs	1	
BC Municipalities	1*	
	2 year appt./rotational	
Others:		
FBI/CJIS		1
Total	**11**	**5**

** Agencies participating on rotational appointments for the purpose of voting, when not filling a voting seat, may attend as a participant.*

Distribution Analysis

Distribution by Jurisdiction	**Membership** (Voting Members)
Federal	3
Provincial/Municipal	8
Total	**11**

CHAIR AND VICE-CHAIR

Nomination of Chair

The Chair of the IT Sub-Committee will be appointed by the Chair of the CPIC Advisory Committee upon recommendation from the IT Sub-Committee. Should the IT Sub-Committee fail to make a recommendation, the Chair of the CPIC Advisory Committee will appoint the new Chair of the IT Sub-Committee.

Qualifications of Chair

The Chair of the ITSC must be a voting member or from a voting agency on a regional rotation of either the IT Sub-Committee or the CPIC Advisory Committee who has a broad understanding of technical issues addressed by the CPIC Advisory Committee and has served on either committee for a period of at least one year.

Roles and Responsibilities of the Chair

- prepares and approves for distribution, meeting agendas for regular and other meetings of the Sub-Committee, along with all supporting documentation, to all Sub-Committee members;
- ensures that documentation required for meetings will be presented in an informative and actionable format;
- conducts regular and other meetings in a manner that will ensure participation and equal opportunity to speak for all members;
- ensures group discussion remains focused on subject matter and that the Rules of Conduct are adhered to;
- initiates action on decisions and recommendations made at meetings to ensure that proper and timely consideration is given by the CPIC Advisory Committee on these matters;
- liaises with the Chair of the CPIC Advisory Committee and the Chair of the Governance Sub-Committee, and represents the IT Sub-Committee at meetings of the CPIC Advisory Committee, Business Requirements Sub-Committee and meetings of other organizations as required;
- appoints a member of the IT Sub-Committee as a Vice-Chair;
- prepares an annual work plan and budget for the IT Sub-Committee and reports periodically to the Chair of the Advisory Committee on progress made against set objectives.
- prepares an Annual Report to the CPIC Advisory Committee that reflects the activities of the ITSC and the Security Working Group during the past year.

Term of Office of Chair

The Chair will be appointed for a minimum two year term. A temporary vacancy in office of the Chair shall be filled by the Vice-Chair. A permanent vacancy in office will require the nomination of a new Chair.

If the Chair is from an agency on a regional rotation, his/her region shall remain on the Sub-Committee for the term of the Chair, pending approval of their Regional Committee.

The Chair does not vote except in a tie situation.

Nomination of Vice-Chair

A Vice-Chair may be appointed by the Chair of the IT Sub-Committee, from amongst the membership, for a minimum of two years.

Qualifications of Vice-Chair

The Vice-Chair must be a voting member of the IT Sub-Committee.

Roles and Responsibilities of the Vice-Chair

The Vice-Chair replaces the Chair in his or her absence. The Vice-Chair may have a designate from his/her region attend the IT Sub-Committee meetings to represent that region, while the Vice-Chair is replacing the Chair.

The Vice-Chair may also represent the Chair at CPIC Advisory Committee meetings at the request of the Chair.

MEETINGS

Regular Meetings

Regular meeting of members is the normal mechanism for the conduct of IT Sub-Committee business, for debating issues, and for making recommendations to the CPIC Advisory Committee on technical matters. Regular meetings shall be held as needed to a maximum of two annually.

Other Meetings

Other meetings may also be called by the Chair to address specific issues or items of interest to the IT Sub-Committee in between regular meetings. Such meetings will normally involve only those members that have a direct interest in discussing these issues or items. These other meetings will usually be video conferences and telephone conferences. All Sub-Committee members must be notified 10 working days in advance if a formal vote committing the IT Sub-Committee is to be held during this meeting as a result of deliberations.

Quorum

A quorum of the IT Sub-Committee shall consist of a simple majority of the total number of voting members, which may include proxies. No meeting will be held and no vote taken if less than the required number of members for a quorum are present.

Proxies

A member may designate another representative from his or her agency / region as a representative for a specific meeting. The person should have sufficient technical knowledge of the issues being discussed. Proxies must be identified by the voting member to the Chair in writing prior to the meeting.

Location of Meetings

Meetings will be held in the National Capital Region. An alternative location may be suggested by the members and put to a vote. Expenses for meetings held outside of Ottawa will be the responsibility of the Sub-Committee members.

Notice of Meetings

Notice of all regular meetings shall be provided to participating and voting members by the Secretariat of the IT Sub-Committee no less than 30 working days prior to the date set for that meeting.

Agenda and Documentation

The Chair of the IT Sub-Committee, with appropriate input from the membership, will be the final arbiter of all agenda items. The agenda for the meeting shall be set and sent, along with relevant documentation, to all members of the IT Sub-Committee at least 10 working days prior to a meeting. Documents requiring translation should be sent to the Secretariat at least 40 working days prior to a meeting.

Attendance at Meetings

During their tenure, members shall attend all meetings. If a member fails to attend two consecutive meetings, the chair shall contact the member's agency to discuss whether the named representative can/should continue as the agency's representative.

Observers

Meetings are closed to the public and the media. Observers are welcome to attend meetings by invitation only and participate at the discretion of the Chair.

Conduct of Meetings

Due to the necessary interaction between members and requirement for visual presentations, the majority of meetings should be conducted face-to-face, unless alternatives are presented by the Chair.

All meetings shall be conducted in compliance with these Rules of Conduct. Should there be a procedural issue not covered by these Rules of Conduct, the Chair will then refer to Robert's Rules of Order (latest revision).

Language of Work

Both official languages, English and French, are recognized languages of work for the IT Sub-Committee. Specific working mechanisms will be established by the Chair.

Voting Procedures

Motions may only be made by voting members, and may be seconded by another voting member. A vote will be taken subsequently, after discussion and at the call of the Chair. Amendments will be allowed by the Chair. Members can accept, reject, or abstain from voting on the motion. Unless a secret or a registered ballot is requested by a voting member, all votes shall be open, e.g., through a show of hands. Votes shall be decided by a simple majority of members present.

Votes made at a video conference or telephone conference meeting will be registered votes. Votes shall be decided by a simple majority of the IT Sub-Committee by voting members taking part in that vote.

In certain circumstances, the Chair may require that a ballot be conducted by either electronic mail or letter. In such circumstances, the exact wording of the proposal will be issued by the Secretariat and only returns made within a specified time frame of that issuance will be considered. Votes shall be decided by a simple majority of IT Sub-Committee members voting that are present.

An action previously voted upon at any IT Sub-Committee meeting and adopted may be reconsidered at the next meeting, if so directed by the Chair of the CPIC Advisory Committee or if a voting member who voted in the direction of the motion moves to have the past action reconsidered because new information is available. All voting members present should vote again on the issue. Motions to reconsider require a two-thirds majority.

Minutes of Meetings

Minutes of meetings shall be recorded, kept, and maintained by the Secretariat. Draft minutes will be distributed to voting and participating members of the IT Sub-Committee, for confirmation and approval, within 20 working days following the meeting. Once a final version of the minutes has been approved by the Chair of the IT Sub-

Committee they shall be distributed to members of the IT Sub-Committee through the most convenient mechanism. They will also be made available to members of the CPIC Advisory Committee and all the Sub-Committees.

Minutes of the meeting shall include: time, date, Chair's name and venue, names of all present, all agenda items discussed and a record of voting decisions reached, a list of follow-up items including name(s) of person(s) responsible for particular items and a due date, time meeting ended, and for regular meetings; date, time, and place of the next meeting.

Records of the IT Sub-Committee

All records, transcripts, minutes, agendas, presentation materials, and other documents relating to the IT Sub-Committee functions, shall be administered and/or maintained by the Secretariat.

C. Working Group Processes

In order to produce results in an effective and efficient manner, it is important that the IT Sub-Committee members develop a common approach for addressing the technical issues pertaining to CPIC activities. The following suggestions must be considered in this light.

Commitment of Participating Organizations

Considering that members will be appointed by a number of organizations that have a common interest in an effective and efficient use of CPIC, it is expected that organizations and agencies appointing voting members select persons who have thorough knowledge of IT, and that these persons be in a position to influence their communities. It is imperative that organizations who agree to nominate a member also agree to provide this member with sufficient time to meet their responsibilities as members of the Sub-Committee. It is also important that the member be provided with means to access their colleagues on the Sub-Committee via electronic mail.

Experts' Support Services

As requested by the Sub-Committee Chairperson, experts may be called to analyze and provide recommendations on specific issues of concern to the Sub-Committee.

Work Planning

Effective work will be facilitated if members of the IT Sub-Committee have a clear idea of what is to be done and how it will be done. The IT Sub-Committee, being a support group to the CPIC Advisory Committee, it will receive from the CPIC Advisory Committee general and specific guidance as to the work to be done. Some suggestions will also be made on the basis of members' knowledge of their technical environment and its evolution. This may at times generate conflicting demands on the agenda of the Sub-Committee. Therefore, it would be appropriate that issues presented by the CPIC Advisory Committee be reviewed on a yearly basis by the Sub-Committee, that priorities be established, that a work plan be prepared for the conduct of activities during the year ahead, and that progress be monitored quarterly in order to ensure that activities are conducted as planned.

More specifically, work planning might include items such as: information/policies required, and technical documents to be reviewed (i.e., Network Security, IT Security Policy, Policy on Acceptable Use of Network, Connectivity/Authorization Processes, Technical Issues for CPIC Security, MOUs, Organizational Issues for CPIC Security, Virtual Private Networks, Wireless Technologies). CPIC/NPSNet issues are other examples of interest. This might include: review and approval of national standards suggested by standards organizations, Committees, Associations and Working Groups (such as CPEG, CACP etc.) and adoption, where possible, of compatible standards, common implementation processes and approaches.

Preparation of Proposals

In order to ensure that recommendations made to the CPIC Advisory Committee reflect a thorough understanding

of the situation and of the consequences of decisions to be made, it is important that a common format be used for presentation of proposals to the IT Sub-Committee. This common format would consist of the following:

- **Summary** including a recommendation (in both English and French). The summary should contain the following information: subject matter, originator (member, agency, telephone/fax/e-mail address), date of submission, issue being addressed, analysis, order of magnitude of costs, implications for CPIC, impact, and a recommendation for the IT Sub-Committee.

The summary should generally be no longer than four pages in bilingual format. Supportive or explanatory information shall be appended to the summary.

- **Supportive or explanatory information.** Documents required to support the summary as presented above shall be appended to the summary. It is not expected that they be bilingual. However, it is expected that the originator will be able to provide additional information upon request to ensure that all persons involved have a clear understanding of the issues being addressed.

Review Process and Preparation of Meetings

Prior to being submitted for discussion and recommendation by the Sub-Committee, a Working Document could be posted on the CPIC Internet/Web site for review by all interested persons. Comments and reactions could be made on the Web site and a dialogue could be conducted. It is expected that this approach would give more perspective to the issue or problem being considered, help refine the recommendation to be made, and eventually result in a better acceptance of the decision by all stakeholders.

In terms of delays, and as soon as technically feasible, it would seem that the proposal being considered could be posted on the Web site for a period of 20 working days prior to being submitted to the IT Sub-Committee on a formal agenda. Posting on designated sites could be made by the CPIC Secretariat who would also, at the same time, send an e-mail to all members to inform them that this item is now on the site. Until then, the most efficient way of transmitting information should be used by the CPIC Secretariat.

It is expected that before IT Sub-Committee meetings, voting members and participants will:

- provide relevant agenda items to the Secretariat and/or the Chair (at least 30 working days prior to a meeting);
- ensure that relevant documentation is provided to the Secretariat; and
- make the necessary travel and hotel arrangements to attend the meeting.

Participation at Meetings, Discussion and Approval of Recommendations

Proposals will be usually discussed and voted on at a regular meeting of the IT Sub-Committee.

Votes will be decided by a simple majority except in the case of a revote as per the ITSC Charter, Voting Procedures, which states 'r;that all motions to reconsider require a two-thirds majority'.

Once approved, recommendations will be forwarded to the Chair of the CPIC Advisory Committee for consideration and approval by the CPIC Advisory Committee and subsequent implementation.

D. Administrative and Technical Support

Secretariat services required by the Sub-Committee will be provided by the CPI Centre on the basis of arrangements to be reviewed annually, as required, by the CPIC Advisory Committee

Roles and Responsibilities of the Secretariat

The role of the Secretariat is to assist the Chair in the conduct of activities, and most particularly to:

- organize meetings, obtain facilities, supplies etc.;
- distribute notices of meetings at least 30 working days prior to meetings;
- obtain agenda items and relevant documentation, produce agendas and distribute these documents at least 10 working days prior to the meetings;
- administer the operational budget, maintain accounts, etc.;
- prepare IT Sub-Committee meeting minutes and distribute a draft to members within 20 working days of the meeting for confirmation/comments and approval;
- record, keep, and maintain minutes, presentation materials, technical documentation, standards and policies that have been discussed/adopted, etc.;
- provide for translation, editorial, technical writing assistance, and communication services if required; and
- assist IT Sub-Committee members in disseminating information to their constituents.

E. Financial Arrangements

Travel Arrangements

Transportation, meal and accommodation expenses incurred by the Chair and voting members of the IT Sub-Committee will be reimbursed by the CPI Centre as per current Federal Treasury Board guidelines, unless held outside of the National Capital Region.

Compensation

ITSC members shall receive no salary or other honorarium for their services. Membership is on a voluntary basis.

Funding of Secretariat Services

Funding of basic Secretariat Services for the CPIC IT Sub-Committee will be provided and managed by the Canadian Police Information Centre.

Appendix I-2-G CPIC Advisory Committee Charter

A. Introduction

The **Canadian Police Information Centre (CPIC) Advisory Committee** and its participating agencies enhance public safety* in Canada by ensuring that the electronic representation of information collected and maintained by these agencies is available and accessible in an accepted format and on a timely basis, for use by partner agencies, in a cooperative, volunteer basis, in support of improved decision making and collective effectiveness.

In the spirit of cooperative participation, the CPIC Advisory Committee, its sub-committees and the participating agencies are dedicated to ensuring that the provisions contained in this Charter are achieved. (See Appendix A for Participating Agencies Obligations and Code of Ethics.)

* **Public Safety:** An environment in which everyone is protected from criminal, hazardous and unsafe acts or situations as mandated by the participating agencies.

BACKGROUND INFORMATION

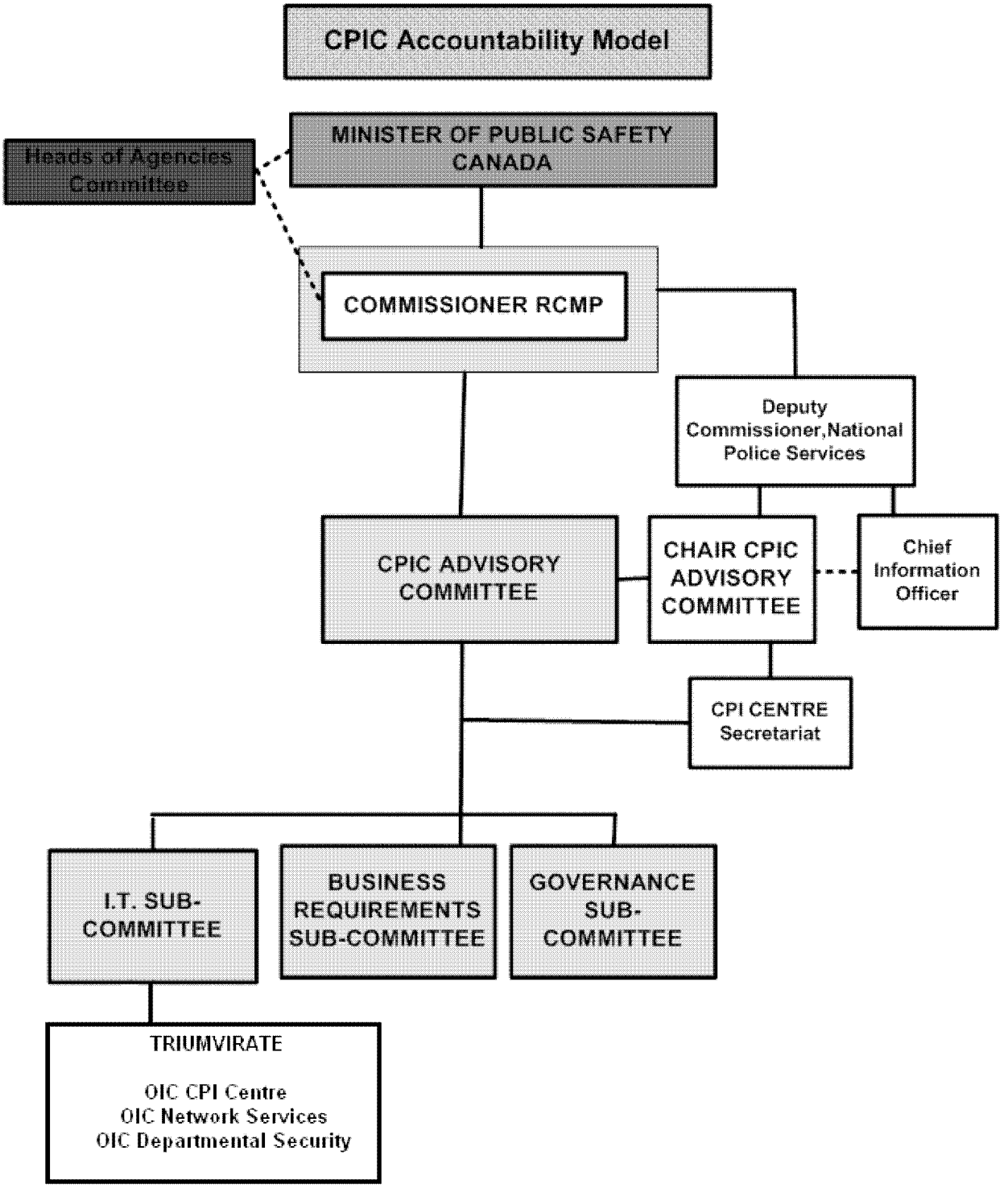
In order to combat organized crime, the federal Attorney General and Provincial Attorney Generals held several meetings in 1966, which resulted in the creation of the Canadian Police Information Centre (CPIC). The CPIC system was approved by Treasury Board in 1967 as "a computerized information system for law enforcement use to provide all Canadian law enforcement agencies (municipal, provincial and federal) with information on crime and criminals". (Treasury Board, Program Approval File, 16 June 1967).

CPIC was established based on Treasury Board Minutes for the provision of CPIC as a National Police Service under the RCMP Act - Sections 5, 21(2). Refer to: Treasury Board Minutes 670388, August 16, 1967 (authorizing the establishment of CPIC); Treasury Board Minutes 690706 July 11, 1969 (authorizing the establishment of the CPIC Advisory Committee); Treasury Board Minutes 720381, July 25, 1973 (amended 1994); Treasury Board Minutes 823301, October 20, 1995 (modernization of the CPIC network); Treasury Board Minutes 827145, April 15, 1999, and Treasury Board Minutes 828896, March 29, 2001.

Since the 1970's, CPIC has been the focal point for information sharing within the police community. In the 1990's it became an information sharing mechanism between police and other agencies of the criminal justice system, law enforcement and regulatory agencies, and the national security sector. The Royal Canadian Mounted Police (RCMP), on behalf of the Canadian law enforcement community, operates the Canadian Police Information Centre under the aegis of the National Police Services (NPS) Program.

This Committee is composed of members of police departments in Canada and federal and provincial law enforcement representatives. Its Chair is appointed by the Commissioner of the RCMP.

The following organizational chart depicts the CPIC accountability process stream:


CPIC Accountability Model
MINISTER OF PUBLIC SAFETY CANADA
Heads of Agencies Committee
COMMISSIONER RCMP
Deputy Commissioner,National Police Services
CPIC ADVISORY COMMITTEE
CHAIR CPIC ADVISORY COMMITTEE
Chief Information Officer
CPI CENTRE Secretariat
I.T. SUB-COMMITTEE
BUSINESS REQUIREMENTS SUB-COMMITTEE
GOVERNANCE SUB-COMMITTEE
TRIUMVIRATE
OIC CPI Centre
OIC Network Services
OIC Departmental Security

The RCMP Chief Information Officer (CIO): is accountable to the Deputy Commissioner, National Police Services for the provision, management and availability of the RCMP network, which includes CPIC and other network extensions to other agencies and police services commonly referred to as the National Police Services Network (NPSNet). The CIO will ensure the network will continue to be a shared infrastructure consistent with Treasury Board Minute 823301, dated October 20, 1995.

The National Police Services Network (NPSNet): provides a national police service, through which every accredited police organization and criminal justice/law enforcement agency in Canada can be linked using CPIC. The NPSNet is not limited in its use. It serves both the CPIC community and the RCMP corporate infrastructure.

- The NPSNet is an integral and key service delivery component of the CPIC Program; and
- CPIC is a mission critical system to the law enforcement and criminal justice community across Canada and is the number one priority traffic on the NPSNet.
- A NPSNet strategic plan will be developed and regularly updated by the RCMP in consultation with, and endorsed by the CPIC Advisory Committee.
- CPIC Advisory Committee defines minimum standards of service delivery for CPIC that is provided by the NPSNet.
- CPIC Secretariat representing the CPIC community, * participates in all decisions relating to all changes to NPSNet that have the potential to impact CPIC.

CPIC ADVISORY COMMITTEE SUB-COMMITTEES

Information Technology Sub-Committee (ITSC): As a sub-committee under the direction of the CPIC Advisory Committee, the ITSC is responsible for recommending information technology policies. The ITSC recommends interface, technology, security and data standards and parameters for all agencies connecting to CPIC.

The ITSC also reviews and recommends information technology standards for the Canadian law enforcement community as they relate to the CPIC system. (See ITSC Charter)

Triumvirate: A sub-committee under the direction of the Information Technology Sub-Committee (ITSC), composed of the Director General, CPI Centre (Chair), the Officer in Charge, RCMP Departmental Security, and the Officer in Charge Network Services, Chief Information Officer Section. The Triumvirate's mandate is to review requests for connection to CPIC and to provide interim approval of security posture pending endorsement at ITSC.

Business Requirements Sub-Committee (BRSC): A sub-committee under the direction of the CPIC Advisory Committee. It is tasked to work and support CPIC activities and reviewing changes or additions to system processes, functionality and policy. (See BRSC Charter)

CPIC Governance Sub-Committee: A sub-committee under the direction of the CPIC Advisory Committee. It is responsible for the planning, review and assessment of the evolutionary changes to the CPIC Advisory Committee and its sub-committees, within the context of their stated roles and responsibilities. (See Governance S-C Charter)

Participating Agencies: Participation will be determined by the CPIC Advisory Committee based on the following criteria:

> *Mandate of the agency and legislated requirements, and agreement by the agency to the stated principles and policies of the Charter.*

Examples of agencies that could use CPIC include:

- agency with full peace officer authority (the primary role of the agency is law enforcement);
- agency with limited law enforcement responsibilities (law enforcement is not the primary role of the organization);

- agency with no direct law enforcement authority but provides assistance to law enforcement agencies;
- agency with a role in the criminal justice system.

CPI Centre Secretariat: The CPIC Secretariat manages the day-to-day operations of CPIC on behalf of the aforesaid steward and CPIC Advisory Committee to ensure that policies and objectives are met and an optimum level of service is provided to the user community. It also performs a secretariat role for the CPIC Advisory Committee and its sub-committees. Further, the Secretariat coordinates a strategic planning/business requirements/change management process and ensures that an effective regional consultation process is in place.

B. Rules of Conduct

The following Rules of Conduct provide a mechanism for the conduct of the CPIC Advisory Committee's activities. They provide **terms of reference** for the Committee, establish its **composition**, clarify the role of the **Chair**, and establish how **meetings** will be convened and conducted.

TERMS OF REFERENCE

Mandate and Responsibilities

The Commissioner of the RCMP, on behalf of the National Police Service, is the governance authority for the Canadian Police Information Centre. The Canadian Police Information Centre Advisory Committee provides advice and recommendations to the Commissioner of the RCMP for:

- establishing the scope, content and policy of the CPIC Program;
- determining eligibility criteria for participating agencies;
- ensuring the integrity, accessibility and viability of the sustained delivery of the CPIC;
- ensuring that adequate controls are defined and implemented to assure * compliance to policies, procedures, and guidelines approved by the CPIC Advisory Committee;
- ensuring that CPIC data banks fulfill their design purpose;
- reviewing and establishing priorities concerning the services to be developed and provided to users;
- promoting the integration of law enforcement information systems in Canada, with the aim of ensuring that such systems are both complementary and compatible with CPIC;
- considering and developing the CPIC position on issues directly related to its development as a law enforcement and criminal justice information system.

Reporting

The CPIC Advisory Committee, through its Chairperson, is accountable to the Commissioner of the RCMP who is the steward of National Police Services, as defined within the RCMP Act. The Minister of Public Safety Canada is accountable for the RCMP.

Amendment to Rules of Conduct/Charter

Proposed amendments to the Advisory Committee Rules of Conduct must be received by the Chair in bilingual format at least 20 working days before the meeting at which the amendment will be considered. Amendments will be made by adoption of a motion containing the exact wording of the change and the

effective date of change. A two-thirds majority of the voting members present is required for the motion to pass. Acceptance, amendment, or suspension of these Rules of Conduct shall be affirmed by a two-thirds majority of the voting members.

Governance of CPIC is an evolving process and it will require regular review to ensure that it continues to meet our collective needs. To this end, an annual review of this Charter will be undertaken by the Governance Sub-Committee. Charter amendments will be prepared by the CPIC Governance Sub-Committee and presented by the Chair of the CPIC Governance Sub-Committee for CPIC Advisory Committee approval.

COMPOSITION

Membership

The CPIC Advisory Committee shall be composed of a Chair and no more than 31 voting members and of a variable number of participating members to be accepted by the Chair.

Voting Members

All voting members must have a thorough understanding of the CPIC Advisory Committee purpose, mandate and functions along with knowledge of the operational law enforcement and/or criminal justice community as they relate to their respective agencies or associations and their role in enhancing public safety in Canada.

Roles and Responsibilities of Voting Members

Provide the Advisory Committee with information on specific issues, new requirements or concerns of law enforcement and criminal justice agencies in conjunction with the CPIC Advisory Committee Charter's 'r;Mandate and Responsibilities'.

Term of Appointment

Members shall be appointed for a minimum period of two years, commencing the day following their appointment. Should a member resign or have to be replaced because he or she cannot attend regular meetings, a replacement shall be designated by the parent organization.

The following table outlines the CPIC Advisory Committee Membership:

Table 1 - CPIC Advisory Committee Membership

	Voting Members	Participants
Chairperson		
Police (23)		
Regional: Atlantic Region	3	
Quebec Region	4	
Ontario/Nunavut Region	4	
Prairies/NWT Region	5	
Pacific Region	3	

	Voting Members	Participants
National: Criminal Intelligence Service Canada (NPS)	1	
CPI Centre Secretariat (NPS)	1	
Canada Firearms Centre (NPS)	1	
Federal: RCMP Federal and International Operations	1	
Other Criminal Justice (8)		
Regional: Atlantic Region	1	
Quebec Region	1	
Ontario/Nunavut Region	1	
Prairies/NWT Region	1	
Pacific Region	1	
Federal: Public Safety Canada (PS)	1	
Public Safety Canada portfolio:		
Correctional Services Canada	1	
Canada Border Services Agency	1	
TOTAL	**31**	

NOTATIONS:

i) Within this document, "region" refers to the following:

Atlantic Region = NS, NB, PEI, NL and Labrador

Quebec Region = QC

Ontario/Nunavut Region = ON and NU

Prairies/NWT Region = MB, SK, AB and NWT

Pacific Region = BC and YK

Federal Region = all Federal seat holders (police and criminal justice)

ii) Rotation of regional representation will be determined at the regional level.

CHAIR

Nomination of Chair

The Chair of the CPIC Advisory Committee is appointed by the Commissioner of the RCMP.

Roles and Responsibilities of the Chair

- prepares and approves for distribution, meeting agendas for regular and other meetings of the Committee, along with all supporting documentation, to all Committee members;
- ensures that documentation required for meetings will be presented in an informative and actionable format;
- conducts regular and other meetings in a manner that will ensure participation and equal opportunity to speak for all members;
- ensures group discussion remains focused on subject matter and that the Rules of Conduct are adhered to;
- initiates action on decisions and recommendations made at meetings;
- liaises with the Chairs of the Information Technology, Business Requirements, and Governance Sub-Committees, and meetings of other organizations as required;
- prepares an annual work plan and budget for the Committee, and reviews reports, workplans and budgetary requirements of Sub-Committees;
- prepares an Annual Report for the Commissioner of the RCMP on activities related to the Advisory Committee, it's Sub-Committees and other related meetings and working groups.

MEETINGS

Regular Meetings

Regular meeting of members will be the normal mechanism for the conduct of Advisory Committee business, for debating issues, and for making decisions related to system policy and procedural matters. A minimum of one meeting shall be held annually.

Other Meetings

Other meetings may also be called by the Chair to address specific issues or items of interest to the Advisory Committee in between regular meetings. Such meetings may involve only those members that have a direct interest in discussing these issues or items. These other meetings will usually be video-conferences and telephone conferences. All Committee members must be notified 10 working days in advance if a formal vote committing the Advisory Committee is to be held during this meeting as a result of deliberations.

Quorum

A quorum of the Advisory Committee shall consist of a simple majority of the total number of voting members, which may include proxies. No meeting will be held and no vote taken if less than the required number of members for a quorum are present.

Proxies

A member may designate another representative from his or her agency or region as a representative for a specific meeting. The person should have sufficient knowledge of the issues being discussed. Proxies must be identified by the voting member to the Chair, in writing, prior to the meeting.

Location of Meetings

Meetings will be held in the National Capital Region. An alternative location may be suggested by members and put to a vote. Expenses for meetings held outside of Ottawa will be the responsibility of the Advisory Committee members.

Notice of Meetings

Notice of all regular meetings shall be provided to participating and voting members by the CPIC Secretariat no less than 30 working days prior to the date set for that meeting.

Agenda and Documentation

The Chair of the Advisory Committee, with appropriate input from the membership, will be the final arbiter of all agenda items. The agenda for the meeting shall be set and sent, along with relevant documentation, to all members of the Advisory Committee at least 10 working days prior to a meeting. Documents requiring translation should be sent to the Secretariat at least 40 working days prior to a meeting.

Attendance at Meetings

During their tenure, members shall attend all meetings. If a member fails to attend two consecutive meetings, the chair shall contact the member's agency to discuss whether the named representative can/should continue as the agency's representative.

Observers

Meetings are closed to the public and the media. Observers are welcome to attend meetings by invitation only and participate at the discretion of the Chair.

Conduct of Meetings

Due to the necessary interaction between members and requirement for visual presentations, the majority of meetings should be conducted face-to-face, unless alternatives are presented by the Chair.

The CPIC Advisory Committee, its sub-committees, and the regional meetings shall be conducted in compliance with these Rules of Conduct. Should there be a procedural issue not covered by these Rules of Conduct, the Chair will then refer to Robert's Rules of Order (latest revision).

Language of Work

Both official languages, English and French, are recognized languages of work for the Advisory Committee. Specific working mechanisms will be established by the Chair.

Voting Procedures

Motions can only be made by voting members, and may be seconded by another voting member. A vote will be taken subsequently, after discussion and at the call of the Chair. Amendments will be allowed by the Chair. Members can accept, reject, or abstain from voting on the motion. Unless a secret or a registered ballot is requested by a voting member, all votes shall be open, e.g., through a show of hands. Votes shall be decided by a simple majority of members present.

Votes made at a video-conference or telephone conference meeting will be registered votes. Votes shall be decided by a simple majority of Advisory Committee members present.

In certain circumstances, the Chair may require that a ballot be conducted by either electronic mail or letter. In such circumstances, the exact wording of the proposal will be issued by the Secretariat and only returns made within a specified time frame of that issuance will be considered. Votes shall be decided by a simple majority of Advisory Committee members partaking in the vote.

An action previously voted upon at any Advisory Committee meeting and adopted may be reconsidered at the next meeting, if so directed by the Chair of the Advisory Committee or if a voting member who voted in the direction of the motion moves to have the past action reconsidered because new information is available. All voting members present should vote again on the issue. Motions to reconsider require a two-thirds majority.

Minutes of Meetings

Minutes of meetings shall be recorded, kept and maintained by the CPI Centre Secretariat. Once a final version of the minutes has been approved by the Chair of the CPIC Advisory Committee they shall be distributed to members of the Advisory Committee through the most convenient mechanism. They will also be made available to the Chair of the CPIC Sub-Committees and other parties as directed by the Chair.

Minutes of the meeting shall include: time, date, Chair's name and venue, names of all present, all agenda items discussed and a record of voting decisions reached, a list of follow-up items including name(s) of person(s) responsible for particular items and a due date, time meeting ended, and for regular meetings; date, time, and place of the next meeting.

Records of the Advisory Committee

All records, transcripts, minutes, agendas, presentation materials, and other documents relating to the Advisory Committee functions, shall be administered and/or maintained by the CPIC Secretariat.

C. Working Group Processes

As the policy-making authority, and in order to produce results in an effective and efficient manner, it is important that Advisory Committee members develop a common approach for addressing issues pertaining to CPIC activities. The following suggestions must be considered in this light.

Commitment of Participating Organizations

Considering that members will be appointed by a number of organizations that have a common interest in an effective and efficient use of CPIC data banks, it is expected that organizations and agencies appointing voting members select persons who have a thorough knowledge of the law enforcement/support line of business. It is imperative that organizations who agree to nominate a member also agree to provide this member with sufficient time to meet their responsibilities as members of the Committee. It is also important that the member be provided with means to access their colleagues on the Committee via electronic mail.

Experts' Support Services

As requested by the Committee Chairperson, experts or resource persons may be called to analyze and provide recommendations on specific issues of concern to the Committee.

Preparation of Proposals

In order to ensure that recommendations made to the CPIC Advisory Committee reflect a thorough understanding of the situation and of the consequences of decisions to be made, it is important that a common format be used for presentation of proposals to the Committee.

This common format would consist of the following:

- Summary including a recommendation (in both English and French). The summary should contain the following information: subject matter, originator (member, agency, telephone/fax/e-mail address), date of submission, issue being addressed, analysis, order of magnitude of costs, implications for CPIC, impact, and a recommendation for the Advisory Committee.

  The summary should generally be no longer than four pages in bilingual format. Supportive or explanatory information and a work plan shall be appended to the summary.

- Supportive or explanatory information. Documents required to support the summary as presented above shall be appended to the summary. It is not expected that they be bilingual. However, it is expected that the originator will be able to provide additional information upon request to ensure that all persons involved have a clear understanding of the issues being addressed.

Review Process and Preparation of Meetings

Prior to being submitted for discussion and recommendation at the Advisory Committee a Working Document could be posted on the CPIC Internet/Web site for review by all interested persons. Comments and reactions could be made on the Web site and a dialogue could be conducted. It is expected that this approach would give more perspective to the issue or problem being considered, help refine the recommendation to be made, and eventually result in a better acceptance of the decision by all stakeholders.

In terms of delays, and as soon as technically feasible, it would seem that the proposal being considered could be posted on the Web site for a period of 20 working days prior to being submitted to the Advisory Committee on a formal agenda. Posting on designated sites could be made by the CPIC Secretariat who would also, at the same time, send an e-mail to all members to inform them that this item is now on the site. Until then, the most efficient way of transmitting information should be used by the CPIC Secretariat.

It is expected that before Advisory Committee meetings, voting members and participants will:

- provide relevant agenda items to the Secretariat and/or the Chair (at least 30 working days prior to a meeting);
- ensure that relevant documentation is provided to the Secretariat; and
- make the necessary travel and hotel arrangements to attend the meeting.

Participation at Meetings, Discussion and Approval of Recommendations

Proposals will be usually discussed and voted on at a regular meeting of the Advisory Committee.

Votes will be decided by a simple majority of voting members present, except in the case of a revote as per the Advisory Committee Charter, Voting Procedures, which states 'r;that all motions to reconsider require a two-thirds majority'.

D. Administrative and Technical Support

Secretariat services required by the Advisory Committee are provided by the CPI Centre on the basis of arrangements which are reviewed annually, as required, by the CPIC Advisory Committee and the Commissioner of the RCMP who is the steward of National Police Services.

Roles and Responsibilities of the Secretariat

The role of the Secretariat is to assist the Chair in the conduct of activities, and most particularly to:

- organize meetings, obtain facilities, supplies etc.;
- distribute notices of meetings at least 30 working days prior to meetings;
- obtain agenda items and relevant documentation, produce agendas and distribute these documents at least 10 working days prior to the meetings;
- administer the operational budget, maintain accounts, etc.;
- prepare Advisory Committee meeting minutes and distribute a draft to the Chair of the Advisory Committee within 20 working days of the meeting for confirmation/comments and approval;
- record, keep and maintain minutes, presentation materials, technical documentation, standards and policies that have been discussed/adopted, etc.;
- provide for translation, editorial, technical writing assistance, and communication services if required; and
- assist the Advisory Committee members in disseminating information to their constituents.

E. Financial Arrangements

Travel Arrangements

Transportation, meal and accommodation expenses incurred by the Chair and voting members of the Advisory Committee will be reimbursed by the CPI Centre as per current Federal Treasury Board guidelines, unless held outside the National Capital Region.

Compensation

Advisory Committee members shall receive no salary or other honorarium for their services. Membership is on a voluntary basis.

Funding of Secretariat Services

Funding of basic Secretariat Services for the Advisory Committee will be provided and managed by the Canadian Police Information Centre.

Appendix A

CPIC PARTICIPATING AGENCIES OBLIGATION

Law enforcement and criminal justice agencies have an obligation to treat personal information according to the law. The CPIC Advisory Committee recognizes its obligations, both under the law and unto the law. There exists, within the partner agencies, the realization that one clear set of rules applies to all and is not a hardship but rather a guarantee that the spirit of privacy legislation will be endorsed and respected no matter where in Canada persons come into contact with the agencies of the law enforcement and criminal justice system.

CODE OF ETHICS

The Code of Ethics for CPIC users establishes procedures and safeguards to promote the maintenance of good practice and compliance with privacy protection legislation as may be enacted within the various jurisdictions of Canada.

The Code of Ethics is a general statement and does not set out detailed rules that must be followed by each participant jurisdiction. However, the CPIC Advisory Committee, by its endorsement of this Code of Ethics, resolves to promote the following general principles through positive and direct action within their respective jurisdictions. Jurisdictions will be directed to create local policies and directives which reflect the principles enunciated here. Jurisdictions are further encouraged to establish methods of promulgating these principles through training sessions, audits and managerial reviews.

For its part, as custodian of the data banks, the Royal Canadian Mounted Police, through the CPIC Advisory Committee, agrees to incorporate this Code of Ethics into the CPIC Reference Manual (currently found in Appendix I-2-C of the CPIC Reference Manual); to incorporate the listed principles contained herein into various training courses and documents provided to trainees; to incorporate into its Audit Standards Procedures Manual, direction to auditors to examine, evaluate and report on the degree to which these principles have been applied in each agency they are responsible to audit; and to vigorously promote the principles of this Code of Ethics at every appropriate opportunity.

Principles of Data Gathering, Maintenance and Distribution

(See current CPIC Reference Manual Appendix I-2-C for explanation of each.)

Principle 1: Personal information must be obtained in a fair and lawful manner and in accordance with legal authority which permits it to be gathered and held.

Principle 2: Personal information in the CPIC computerized data banks shall be held and used only for one or more specified and lawful purposes.

Principle 3: Personal information held for any purpose or purposes shall not be disclosed in any manner inconsistent with that purpose or purposes.

Principle 4: Personal information shall be accurate and where possible, kept up to date.

Principle 5: Personal information held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6:

(a) In those instances where a CPIC agency is registered as the record owner, an individual is entitled to request access from that agency who, without undue delay or expense:

(i) may grant disclosure of that information, where appropriate; and

(ii) where appropriate, may correct or remove such data.

(b) In those instances where access is requested and that CPIC agency is not the registered owner of a record in the CPIC data banks, the agency will consult with the record owner and will identify the owner of the record, when appropriate.

Nothing in either (a) or (b) above overrides the exemption provisions of the federal *Privacy Act* or of any provincial or territorial legislation that might apply.

Principle 7: Appropriate security measures will be taken to prevent unauthorized access to, or alteration, destruction or disclosure of, personal information and against accidental loss or destruction of personal information.

Appendix I-2-H: Service Level Agreement of the CPIC Program

Service Level Agreement Between CPIC and CIO Sector

Documentation Information

File Name	**GIT 1485-11-23 (I & I S, CPI Center)** **GV 255-10 (CIO Sector)**

Leveraged Documents and Other Sources of Information

- CPIC Service Level Management & Current State of Service Levels 2003
- CPIC Requirements Management Policy 2003
- Standard Service Agreement for the National Police Services Network 2003
- Charter of the CPIC Governing Council (Draft) 2003
- An Agreement on Support Objectives Between the RCMP and Canada Customs and Revenue Agency - Contraband and Intelligence Services 2000
- Memorandum of Understanding Between the RCMP and the Department of Justice Relating to the Performance of Functions and Duties in Support of Operations of the Canadian Firearms Registration System and Associated Equipment 2000
- Central Help Desk Severity / Escalation Procedures 1999
- Service Agreement for Automated Criminal Intelligence & Information System Addendum 1 2003
- An Agreement On Support Objectives Between the RCMP (Informatics Directorate) and the Correctional Service Canada 2000
- Treasury Board of Canada Secretariat Policy on the Use of Electronic Networks 1998
- Service Level Agreement Between the Ontario Provincial Police Information Technology and Telecommunications Section and Local Police Services within the Ontario Municipal and Provincial Police Automation Cooperative 2001

1. Introduction

This Service Level Agreement (SLA) is between the Canadian Police Information Center (CPI Center) and the Chief Information Officer Sector (CIO Sector).

The Director General, CPI Center, represents all Agencies who access and use the CPIC Program. CPI Center is the requirement representative between the user community and the CIO Sector.

The CIO Sector is responsible for the maintenance and support of the CPIC Program. It is also the maintenance and support sector for the National Police Services Network (NPSNet) infrastructure over which CPIC data is transmitted. Maintenance and support for the NPSNet are covered under the Standard Service Agreement published by Network Services Branch, CIO Sector, Version 1.4 June 10, 2003 and amendments thereto.

Generally, the CPIC User Communities are Law Enforcement and Criminal Justice Agencies who have access to the CPIC Program and its ancillary data bases. For example, a law enforcement agency includes, but not limited to, a police service (Royal Canadian Mounted Police, Ontario Provincial Police, etc . . .); a Criminal Justice Agency includes, but not limited to, a federal and provincial government agency (Correctional Services Canada, Insurance Corporation of British Columbia, etc . . .). A CPIC user is also defined as a person or organization exchanging information with the CPIC Program.

1.1 Purpose

This SLA is to define, in general terms, the support expectations and arrangement between the CPI Center and the CIO Sector for the CPIC Program.

1.2 Scope

This SLA will focus on the points listed below.

- The availability and performance of the CPIC Program
- Change management - software and maintenance upgrades
- Technical support
- Problem Management and Classification
- Reports and manuals
- Back Up and Recovery

2. Availability and Performance of the CPIC Program

2.1 Availability & Performance by User Community

There will be no planned outages of the CPIC Program during peak hours unless there are extenuating and/or exceptional circumstances. Local maintenance can be accomplished during normal business hours (peak hours) when coordinated and when acceptable to the CPIC Agency affected.

Table 1 below is intended to capture the relative weight to an Agency's requirement for the CPIC Program availability and performance. For example, full law enforcement agencies will have a higher relative availability and performance requirement than agencies who support law enforcement.

User Community	Availability	Performance
Law Enforcement agencies & CIIDS/OCCs/GoNet - includes mission critical devices (.i.e dedicated CPIC terminals in agencies)	Critical	High

User Community	Availability	Performance
RO - (Ontario, Québec, Saskatchewan, Alberta, British Columbia) NCIC/ACUPIES Vehicle Index Gateway CFRO	High	Normal
External Agencies - (Canada Customs and Revenue Agency, Corrections Canada, Department of National Defense, Firearms - CFO, GoNet, and others to be defined)	High	Normal
Single Terminal	Normal	Normal

Table 1: Relative Availability and Performance Requirements by User Type

2.2 CPIC Program Availability Objectives

Each subsystem strives for 100% availability during peak hours of operation. For reporting purposes, an overall target availability of 99% averaged over a calender month and 24 hours per day has been established for the CPIC Program. Current service availability objectives are included in Table 2.

Availability Objectives - CPIC Program	
CPIC 06:00 - 22:00 (peak hours) - Excludes Times for Major Releases which are usually implemented on Saturday/Sunday time frames.	100 %
CPIC 7 x 24 / Month	99 %

Table 2: Peak Hours Availability Objectives

Peak hours are defined as Monday to Friday, 6:00 a.m. to 10:00 p.m. Eastern Standard Time.

2.3 CPIC Program Performance Objectives

Unlike the availability objectives for this SLA, performance objectives will only be assigned to CPIC Transactions. The CPIC Messaging Performance Objectives are not included. They will be added once a historical base has been established.

These performance objectives only apply to the demarcation point between the CPIC Program and the CPIC Agency.

CPIC Transaction Performance Objectives are expressed as the following:

- Average CPIC Transaction Response Objective, and
- CPIC Response Objective by Transaction Type.

Both of these transaction performance objectives are obtained by combining CPIC Host and NPSNet metrics. Host metrics account for all of the transaction that pass through the system. NPSNet performance metrics are obtained by sampling response times for CPIC transactions. Average CPIC transaction sizes (in and out bytes) are periodically sent to a sample of edge routers providing a metric on network performance.

Table 3 defines the average transaction response objective for the CPIC Program peak hours. This objective is used primarily for external reporting outside of the RCMP.

Average CPIC End-to-End Transaction Response < 6 seconds.

Table 3 expresses the performance objectives by transaction type to be achieved 75%, 90%, 95% and 99% of the time (at the CPIC Host and End-to-End the demarcation point to an Agency). In the event that performance problems are encountered, the ability to break down performance objectives by transaction type helps to identify where problems exist.

Transaction Type		**End-to-End Response (sec) Host to Demarcation**			
			75%	90%	95%
Maintenance	Simple	2.5	5	7	13
		Complex	5	10	17
Query	Simple	2	5	7.3	12
		Complex	3	5	26

Table 3: Performance Objective (Peak Hours)

2.4 Service Level Reporting

Service level reporting against performance and availability will be provided by the CIO Sector on a scheduled basis. These reports will be made available to the CIO Sector and CPI Center. The CIO Sector will continue to investigate and/or produce additional reports.

2.4.1 Availability Reports

Availability reports consists of the following:

- CPI Centre Communications Network Availability Report (Monthly)

2.4.2 Performance Reports

Performance reports consist of the following:

- CPIC Daily/Weekly/Monthly Performance Reports

3. Change Management

3.1 Change Management Documentation

Accompanying all system changes will be Change Requests (CR) and the appropriate and detailed technical documentation. Documentation will include a description of the proposed CR, Impact Assessment (IA) for the proposed change, implementation date, approvals and when appropriate, test results.

3.1.1 Notification of Changes

Depending on the complexity, for system changes that require an outage, the CIO Sector will provide 1-5 working days notice via general broadcasts. Outages will also be posted on the CHD Web page as soon as the information is available and the outage is confirmed.

3.2 Change Management Constraints

3.2 Change Management Constraints

3.2.1 CPIC Program

Notwithstanding an emergency or an exceptional circumstance, scheduled system changes may be implemented to the CPIC Program and related systems with an approved CR on specified days during non peak hours / low traffic periods, or on a suitable day and time period as agreed to by CPI Center and the CIO Sector.

For changes that impact external interfaces, where feasible, CIO Sector will provide 100 calendar days notice to CPI Center. As required and, as feasible, CPI Center will provide external agencies with 90 days notice of changes.

The CIO Sector will require lead time for system changes requested by CPI Center. This lead time will be negotiated for acceptability on a case by case basis.

3.2.2 Mainframe

Notwithstanding emergency or exceptional circumstances, mainframe changes and updates are currently performed during non peak hours / daily low traffic periods.

3.2.3 Network

Except for an emergency or an exceptional circumstance, network changes will be scheduled to minimize negative impact on CPIC Program performance and availability.

3.2.4 Safe File Management

Overall policy and management of the CPIC Safe File are the responsibility of the CPI Center. The DB2 Safe File permits both real-time and scheduled changes. In support of Safe File management, CPI Center requires the CIO Sector to support and assist as required. This support and assistance include the following:

- Maintaining programs on the mainframe to manage the Safe File
- Providing Safe File updates and appropriate Safe File reports.

4. Technical Support

The CIO Sector, as the responsible area for maintenance and support of the CPIC Program, will maintain technical and support staff to ensure the consistent availability, performance, and maintainability.

5. Problem Management and Classification

5.1 Central Help Desk of the CIO Sector

CPIC Program problems must be reported through the defined problem management procedures. The CPIC user community problem management is achieved through the Central Help Desk (CHD). In some instances, the initial CPIC user may be required to first report a problem to the user's local help desk, which in turn, reports to the CHD.

Problems are identified in one of these three ways.

- The agency or user calls the CHD and reports a problem.
- A monitoring tool detects a fault, and a problem ticket is opened manually.
- Another team recognizes a problem and notifies the CHD.

In all cases the CHD is notified and a problem ticket is opened and remains open until resolution.

5.2 Severity

A severity level of a problem is a measure of its impact on the organization and how quickly the problem must be resolved. Information such as life threatening, operational system failures, communications failures or the number of users affected are factors in determining the severity level.

5.2.1 Security Level

- A measurement of how seriously a user is impacted by a problem.
- It is assigned when the problem is initially recorded - 1 for most serious to 5 for least serious.
- Support groups will use the severity to organize their workload priorities.
- Severity should be assigned according to the overall impact on the operational system.
- The severity level may be adjusted up or down from its original assigned level as the operational impact evolves.

5.2.2 Defined Severity Response Times

CHD Standards are as shown in the Table 4. These response times apply 7 days per week and on a 24 hours per day basis. Operations staff will apply "best effort" to meet these standards. Technical personnel are not always "on call" and it is possible that a problem situation may not be addressed immediately pending contact with appropriate resources to resolve the problem.

Severity Level	Definition	Notify CPIC Policy Centre	Response Times	Resolution Target[1]
1: Critical Impact	CPIC system functionality is critically affected; critical system or data is unavailable. All or a majority of	After System Has Been Down for 2 Hours	Immediate	4 Hours

Severity Level	Definition	Notify CPIC Policy Centre	Response Times	Resolution Target[1]
	users are affected.			
2: Serious Impact	CPIC system functionality is seriously affected. A large segment of user are affected.	Next Business Day / CPIC Availability Report	2 Hours	8 Hours
3: Moderate Impact	CPIC system functionality is moderately affected. A smaller segment of users are affected.	Next Business Day / CPIC Availability Report	24 Hours	72 Hours
4: Low Impact	CPIC system functionality is marginally affected and monitoring and follow-up is required.	Next Business Day / CPIC Availability Report	3 Days	When a Fix Becomes Available
5: No Impact	CPIC system functionality is not affected but a modified / new functionality has been developed for implementation in a future CPIC Program release.	As soon as possible with no urgency	At next CPIC Program Release	At next CPIC Program Release

[1] Resolution involving resources not readily available may well exceed these time frames depending on the site location and severity.

Table 4: Severity Response Times

Note: The CIO Sector will make reasonable efforts to respond as quickly as possible to all Severity Levels; however, it is common sense that responses to CPIC system failures during core business hours, Monday to Friday, are likely to be quicker than after normal business hours. Call back of key personnel after normal business hours may increase the time to respond and time to resolve a CPIC system malfunction.

5.3 Problem Escalation

Within the Central Help Desk, the proper procedures exist for problem escalation and are referenced in the RCMP Central Help Desk Protocol manual. These procedures are amended from time to time to take into account changing trends. Escalation procedures deal with both Technical staff call out for CPIC Program fix and hierarchical management notification in more serious situations.

6. Reports and Manuals

6.1 CPIC Reference Manual and Other Publications

From time to time, amendments are necessary to the ***CPIC Reference Manual***. Between the CPI Center, Program Policy, and the CIO Sector, Technical Documentation and Graphics Section (TDGS), such amendments will be written by CPI Center and published by TDGS.

Similarly, other Publications concerning the CPIC Program which are of a National Police Service interest, will be published by TDGS where there is a joint consensus.

7. Backup and Recovery

7.1 Storage of CPIC Data

CPIC data will be stored as prescribed by the governing legislation and the RCMP's retention and disposal schedules in effect at the time of signing the SLA. Currently, CPIC data is governed by the federal Privacy Act and the National Archives of Canada Act. The RCMP regulations and policy also bear on the matter.

7.2 CIO Sector Disaster Recovery Plan

The CIO Sector's Disaster Recovery Plan (DRP) will be activated in accordance with RCMP policy of the RCMP Operations Manual. As appropriate, at the National Operations Center (NOC), the Deputy Commissioner will appoint a Special Operations Crisis Management Commander (SOCMC). The SOCMC is responsible for the decision to invoke the CIO Sector's DRP. The Business Resumption Plan will be activated in concert with the Disaster Recovery Plan.

Within the CIO Sector, the sequence procedures for the CPIC Program Disaster Recovery will be tested from time to time and revised as needed.

8. Audit Requirements

In support of the mandatory audit of agency records function, CPI Center requires the CIO Sector to support and assist as required. This support and assistance includes the items listed below.

- Maintaining audit programs on the mainframe
- Retrieving archived data to perform audit activity
- Providing required audit reports

Audit Logs

The Offline Search of the audit logs supports criminal and non-criminal investigations involving the use of the CPIC Program. The CIO Sector will, on behalf of the CPIC Program, maintain audit logs indefinitely or as technology will permit. Where it becomes necessary to purge any segment of the audit logs, the CIO Sector and the CPI Centre will jointly complete an impact assessment prior to any action to purge any segment of the audit logs.

9. Document Sign-Off/Approval Record

Approvals	Name & Position	Signature	Date
Acceptor	Director General CPI Center		2004 Nov. 15
Acceptor	Director General Systems Operations, CIO Sector		2004 Nov. 15
Acceptor	Director General Infrastructure Engineering and Development CIO Sector		2004 Nov. 15
Acceptor	Director General IM/IT Business Solutions CIO Sector		2004 Nov. 15