



## ARCHIVED - Archiving Content

### Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

## ARCHIVÉE - Contenu archivé

### Contenu archivé

L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.



**Resolutions Adopted  
at the  
106th Annual Conference**

**August, 2011  
Windsor, Ontario**

**CANADIAN ASSOCIATION OF CHIEFS OF POLICE**

*Leading progressive change in policing*

Unit 100 – 300 Terry Fox Drive, Kanata Ontario K2K 0E3

p: 613-595-1101 f: 613-383-0372

e: [cacp@cacp.ca](mailto:cacp@cacp.ca) w: [www.cacp.ca](http://www.cacp.ca)

## Table of Contents

<b>2011-01</b>	
<b>Reintroduce Lawful Access Legislation to Reduce Lawful Access and Electronic Surveillance Deficiencies and Obsolescence.....</b>	<b>3</b>
<b>2011-02</b>	
<b>Introduce Electronic Countermeasures Legislation.....</b>	<b>6</b>
<b>2011-03</b>	
<b>Provide 9-1-1 Cell Phone Call Customer Name and Address.....</b>	<b>9</b>
<b>2011-04</b>	
<b>Amendment to the Criminal Code of Canada and the DNA Identification Act.....</b>	<b>12</b>
<b>2011-05</b>	
<b>Unexecuted DNA Orders.....</b>	<b>16</b>
<b>2011-06</b>	
<b>Building on Financial Intelligence in Organized Crime Investigations Through FINTRAC.....</b>	<b>20</b>
<b>2011-07</b>	
<b>National Police Services.....</b>	<b>24</b>
<b>2011-08</b>	
<b>Canadian Training Standard for Child Exploitation Investigators.....</b>	<b>25</b>
<b>2011-09</b>	
<b>Evolution of the Canadian Law Enforcement Strategy to Combat Organized Crime (CLES).....</b>	<b>29</b>
<i>Appendix 1 - Intelligence-Operations Functions Framework</i>	
<i>Appendix 2 - Canadian Law Enforcement Strategy (CLES) Vision Statement</i>	
<i>Appendix 3 - Canadian Law Enforcement Strategy (CLES) Statement of Commitment</i>	
<i>Appendix 4 – Intel-Ops Functions Framework – Stakeholder Roles and Responsibilities</i>	

**REINTRODUCE LAWFUL ACCESS LEGISLATION TO REDUCE  
LAWFUL ACCESS AND ELECTRONIC SURVEILLANCE  
DEFICIENCIES AND OBSOLESCENCE**

*Submitted by the Law Amendments Committee*

**WHEREAS** current *Criminal Code* provisions in respect to police powers to conduct judicially authorized electronic interceptions and seizures are outdated and not in touch with modern realities, and;

**WHEREAS** modernization of these legislative provisions is urgently required to reflect the significant advancements in communications technologies, and;

**WHEREAS** there are no requirements for new telecommunications technologies to be intercept capable, and;

**WHEREAS** the current legislative scheme has resulted in intercept safe havens.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police urge the Federal Government to pass legislation to amend the *Criminal Code* to require new telecommunications technologies to be intercept capable, to prevent intercept safe havens and to modernize electronic intercept provisions.

**REINTRODUCE LAWFUL ACCESS LEGISLATION TO REDUCE  
LAWFUL ACCESS AND ELECTRONIC SURVEILLANCE  
DEFICIENCIES AND OBSOLESCENCE**

*Submitted by the Law Amendments Committee*

**Commentary:**

Repeated attempts to introduce lawful access legislation have received government and all party support, however, the legislation has encountered the conclusion of parliamentary sessions prior to third reading.

Canada's obsolete legislative scheme was implemented during the days of the rotary dial telephone. Modernization of current legislative provisions is urgently required to reflect significant advancements in communications technologies – such as emails, encryption, and text based messaging. These new technologies allow for old crimes to be committed in new ways, as well as new crimes to develop, including viruses, trojans, worms, hacking, spyware, spam, phishing, identity theft, internet fraud and money laundering.

Unlike previous telephony data and technology, where a phone was hardwired into a specific location and communicated to another phone hardwired at the receiving end, new technologies operate much differently. Technology is mobile, operating on wireless frequencies routed through any number of internet service providers worldwide. Intercept is much more complex and requires advanced technologies and updated legislation to compete with criminals. Currently a number of new telecommunications technologies cannot be intercepted, allowing criminals a fail safe way to conduct business without the prying eyes of police. Other G-8 countries around the world require new telecommunications technologies to be 'intercept capable'.

Without modernization, the current legislation challenges police investigative techniques and compromises public safety. Urgent amendments are required to allow the police to lawfully and effectively investigate serious offences; particularly those committed by organized crime groups and gangs.

**REINTRODUCE LAWFUL ACCESS LEGISLATION TO REDUCE  
LAWFUL ACCESS AND ELECTRONIC SURVEILLANCE  
DEFICIENCIES AND OBSOLESCENCE**

*Submitted by the Law Amendments Committee*

**Media Lines:**

- The current legislation that is in effect relating to Lawful Access was implemented during the days of the rotary phone. With the continuing advances being made to electronic technology, this legislation is now obsolete and it compromises public safety by challenging police investigative techniques.
- Urgent amendments are required to allow the police to lawfully and effectively investigate serious offences that are being perpetrated using new and advanced communication technologies; particularly those offences committed by organized crime groups and gangs.
- Prior to parliament being prorogued, new Lawful Access legislation was introduced and it received all party support through its first and second readings. With parliament back in session, Bills C-46 and C-47 should be reintroduced in order to proceed to a third and final reading.
- These two Bills will provide the police with the tools that are necessary to deal with new and emerging crime trends associated with modern communication technology.

**INTRODUCE ELECTRONIC COUNTERMEASURES  
LEGISLATION**

*Submitted by the Law Amendments Committee*

- WHEREAS** Electronic Countermeasures (ECM) are available for purchase by the general public on the open market, and;
- WHEREAS** the Federal *Radiocommunication Act* does not provide clear guidelines for the possession and use (application) of Electronic Countermeasures, or clear prohibitions which will allow for an effective law enforcement response, and;
- WHEREAS** it has been proven that electronic countermeasures are effective tools, now being used by organized crime, to disrupt police communication systems including computer aided dispatch, police radios, and cell phones, and;
- WHEREAS** officer and public safety is compromised when law enforcement officials are left without communications when dealing with individuals possessing this technology.
- THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to introduce legislation pertaining to Electronic Countermeasures that will restrict the possession and use (or application) of this technology under the *Criminal Code* and the *Radiocommunication Act*. This legislation should give law enforcement officials the usual powers of arrest and detention, with the accompanying provisions for the search and seizure of this technology, when electronic devices are being used contrary to law.

**INTRODUCE ELECTRONIC COUNTERMEASURES  
LEGISLATION**

*Submitted by the Law Amendments Committee*

**Commentary:**

Electronic Countermeasure (ECM) devices, or jammers, have been in existence for a number of years. They were originally employed by the military to interfere with hostile communications and to mask their own activities from electronic surveillance. ECM devices have evolved from an unsophisticated “brute force” wide band application to either blocking discreet bands of the RF spectrum or blocking some of the spectrum while allowing certain frequencies to operate without interference. These devices are now available on the open market. Some are sophisticated in their design and come in a variety of shapes and sizes, from small units that are the size of a cigarette lighter inserts, to larger, more powerful vehicular mounted unites. They are advertised openly by companies inside Canada. These devices can prevent a police officer from communicating with their dispatch or other police officers.

These devices and the purpose for which they are created are inherently harmful and lend themselves to use by organized crime and other elements in furtherance of criminal activity. The danger they pose to the life and safety of all public safety officers is self evident. Absent an exemption or licensing scheme authorizing use by government agencies and public safety designates, the possession, importation, sale and manufacture of these devices must be made illegal in Canada. The regulation of these devices belongs in the *Criminal Code* and they should be dealt with in the same manner as other prohibited devices.

**INTRODUCE ELECTRONIC COUNTERMEASURES  
LEGISLATION**

*Submitted by the Law Amendments Committee*

**Media Lines:**

- Electronic Countermeasures (ECM) are devices that were originally designed and employed by the military to interfere with electronic communications.
- These devices are now available on the open market and they are being advertised by companies inside of Canada.
- It has been proven that these devices are now being used by organized crime groups to disrupt police communication systems.
- When law enforcement officials are left without communications, officer and public safety is compromised.
- The Canadian Association of Chiefs of Police strongly believe that these devices should be regulated by the *Criminal Code* in the same manner as other prohibited devices.

**PROVIDE 9-1-1 CELL PHONE CALL CUSTOMER NAME AND ADDRESS**

*Submitted by the Law Amendments Committee*

- WHEREAS** we live in a society that now relies heavily on mobile communication, and;
- WHEREAS** there should be no difference in the level of safety available pursuant to a 9-1-1 call that is made from a landline and a call that is made from a cell phone, and;
- WHEREAS** there is a gap in the Canadian Radio-Television and Telecommunication Commission's policy that only requires the release of the number and not the name and address associated with a cell phone that an emergency call is originating from, and;
- WHEREAS** there are unnecessary delays occurring before the police can be dispatched to an emergency call made from a cell phone because of the current back grounding and risk assessment steps that are required on 9-1-1 calls from cell phones prior to the identification of the associated address and public safety is compromised when these delays occur.
- THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to move forward with legislation that would require Wireless Service Providers to immediately provide Public Safety Answering Points with subscriber name and address on all 9-1-1 calls, and;
- BE IT FURTHER RESOLVED** that the Canadian Association of Chiefs of Police urge the Canadian Radio-television and Telecommunication Commission to take immediate steps to amend Telecom Decision 2009-40 by making it mandatory for Wireless Service Providers to provide subscriber name and address on all 9-1-1 calls from cell phones.

**PROVIDE 9-1-1 CELL PHONE CALL CUSTOMER NAME AND ADDRESS**

*Submitted by the Law Amendments Committee*

**Commentary:**

Currently there is a distinction made between the information that a Public Safety Answering Point (PSAP) receives on a 9-1-1 call that is made from a landline and a 9-1-1 call that is made from a cell phone. Canadian Radio-television and Telecommunication Commission's policy, under Telecom Decision 2009-40, mandates Wireless Service Providers to provide the phone number of a cell phone and, unlike a landline, not also provide the subscriber's name and address associated with the cell phone when an emergency call is placed.

This leads to unnecessary delays in police response. There have been recent incidents of domestic violence that have ended tragically after calls for help were made using cell phones where customer name and address were not readily available. This is unacceptable in a society where individuals calling 9-1-1 do so to receive immediate assistance.

**PROVIDE 9-1-1 CELL PHONE CALL CUSTOMER NAME AND ADDRESS**

*Submitted by the Law Amendments Committee*

**Media Lines:**

- In a society where more and more people are using wireless communications for all of their telephone needs, subscriber name and address information represents an initial 'building block', or starting point, from which the police can proceed with their variously required statutory and common law duties – crime prevention, investigation, maintenance of public safety, and others.
- The safety and security of our communities' demands that appropriate and reliable subscriber information be provided to Public Safety Answering Points in order that they may appropriately assess the risks to members of the public, and to locate them in situations of urgency, when seconds count. The current scheme of only providing the telephone number along with unreliable XY coordinates, thereby imposing additional time consuming steps for the assessment of risk and caller location during emergency 911 calls requires immediate changes to CRTC policy.
- It is with this in mind, that the Canadian Association of Chiefs of Police urges the Canadian Radio-television and Telecommunication Commission to take immediate steps to amend CRTC Telecom Decision 2009-40.

**AMENDMENT TO THE *CRIMINAL CODE OF CANADA* AND THE  
*DNA IDENTIFICATION ACT***

*Submitted by the Law Amendments Committee*

**WHEREAS** DNA Analysis is an invaluable tool in the investigation and prosecution of criminal offences, as well as the protection of society and the exoneration of the innocent, and it is in the public interest to have investigations proceed as expeditiously as possible, and;

**WHEREAS** the system established in the *Criminal Code* requiring a conviction for a primary designated offence and the issuance of a court order before a DNA sample can be collected is administratively cumbersome and results in considerable delay, and;

**WHEREAS** the court has limited jurisdiction to decline to order a DNA sample on a primary designated offence, and;

**WHEREAS** the delay between arrest and conviction can be lengthy and the consequent delay in the obtaining of a DNA sample can seriously compromise outstanding investigations.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to move forward with amendments to the *Criminal Code of Canada* and *DNA Identification Act* to allow for:

- The collection of DNA samples from any person lawfully charged for a primary designated offence, as defined in section 487.04 of the *Criminal Code*, by part (a) of the definition of “primary designated offences”; and,
- The removal of that sample from the DNA Databank should the accused not be convicted of the offence (post appeal periods).

**AMENDMENT TO THE *CRIMINAL CODE OF CANADA* AND THE  
*DNA IDENTIFICATION ACT***

*Submitted by the Law Amendments Committee*

**Commentary:**

There is no other forensic identification technique (fingerprints, ballistics, tire tracks and tool marks) that is as effective as DNA in identifying individuals who have committed a crime or in exonerating a person suspected of committing a crime. In section 4 of the *DNA Identification Act*, it is specifically stated that “the protection of society and the administration of justice are well served by the early detection, arrest and conviction of offenders, which can be facilitated by the use of DNA profiles”.

In Europe, where England is widely recognized as having one of the most successful approaches to the use of forensic DNA technology, statistics show that with over 2 million DNA profiles loaded into their system there is a 40 percent greater chance of obtaining a match between a crime scene profile and a “criminal justice” (arrestee or suspect) profile.<sup>1</sup>

Currently, an offender’s DNA is not checked against the Databank until a conviction is entered and an Order granted for collection of a sample, unlike with fingerprinting where fingerprints are taken at the time of arrest and compared to the fingerprint database. Unsolved cases in the Databank can remain on hold for a considerable amount of time waiting for an offender’s DNA to be submitted. In addition, there is often considerable delay between arrest and conviction, this results in an added delay of up to years before cases in the Databank can be properly investigated and the offenders either identified or exonerated. It is important to note that a hit on the Databank only allows the investigation to proceed to the obtaining of a warrant.

Delays in obtaining a sample for comparison to the Databank mean that previous offences committed by the offender remain unsolved until conviction for the new offence. This means that an accused who has committed other crimes will go undetected for years while awaiting trial for his current arrest, leaving victim’s without answers and allowing an accused on bail to continue to commit similar offences, undeterred. Should an accused not be convicted, that sample will be removed from the Databank and destroyed. Many accused fail to attend court and many individuals who are required to provide DNA do not do so. Collecting DNA at the time of arrest ensures that a sample is provided.<sup>2</sup>

---

<sup>1</sup> Asplen, Christopher. *The Application of DNA Technology in England and Wales*. Smith Alling Lane. Received by the US Department of Justice January 2004. p.1.

<sup>2</sup> Victims of Violence. (2008). *Research – DNA Databanks*. Retrieved March 8, 2011 from [http://www.victimsofviolence.on.ca/rev2/index.php?option=com\\_content&task=view&id=341&Itemid=31](http://www.victimsofviolence.on.ca/rev2/index.php?option=com_content&task=view&id=341&Itemid=31)

The offences described in 487.04, “primary designated offences” (a), are the most serious offences in the *Criminal Code* (murder, aggravated sexual assault, kidnapping, robbery, etc.) and the Court “shall” order a DNA sample upon conviction. This is in contrast to other primary designated offences described in section 487.04 “primary designated offences” (a.1) – (d) and “secondary designated offences” described in section 487.04, where the Court has some discretion in ordering a sample upon conviction. The public has a special interest in ensuring swift investigations of these most serious offences.

If the *Criminal Code* is amended to allow for the taking of a sample at the time of arrest for a s.487.04 “primary designated offence”(a), hits on the Databank will be identified much earlier, and investigations will be able to proceed expeditiously. The elimination of delay benefits the administration of justice by ensuring that investigations are conducted when other evidence can still be obtained and witness memories are fresh. In addition, trials are conducted within a reasonable time which allows compliance with the accused’s constitutionally protected right.

**AMENDMENT TO THE *CRIMINAL CODE OF CANADA* AND THE  
*DNA IDENTIFICATION ACT***

*Submitted by the Law Amendments Committee*

**Media Lines:**

- The use of DNA to identify individuals who have committed a crime, or to exonerate a person suspected of committing a crime, is more effective than any other forensic technique.
- Unlike fingerprints which are taken at the time of arrest and compared to the fingerprint database, DNA is not checked against the national Databank until a conviction is entered and an Order granted for collection of a sample.
- Additionally, many accused fail to attend court and many individuals who are required to provide DNA do not do so. Collecting DNA at the time of arrest ensures that a sample is provided
- This current process causes timely delays in solving cases that are under investigation, as well as other crimes that the suspect may have committed previously. The Paul Bernardo and Russell William cases in Ontario are both perfect examples of this.
- If the *Criminal Code* is amended to allow for the taking of a sample at the time of arrest for a s.487.04 “primary designated offence”, hits on the Databank will be identified much earlier, and investigations will be able to proceed expeditiously.
- The public has a right to expect that these investigations will be carried out quickly and effectively, which will also serve to help prevent the commission of future offences by these offenders.
- Ultimately, the elimination of these delays will benefit the administration of justice in Canada.

**UNEXECUTED DNA ORDERS**

*Submitted by the Law Amendments Committee*

**WHEREAS** DNA Analysis is an invaluable tool in the investigation and prosecution of criminal offences, as well as the protection of society and the exoneration of the innocent, and;

**WHEREAS** the *DNA Identification Act* became law on June 30, 2000, and;

**WHEREAS** peace officers are responsible for executing DNA Orders issued by the courts “To Have Bodily Substances Taken”, and;

**WHEREAS** there continue to be a number of legislative gaps in the processes related to DNA Orders and there are hundreds of outstanding DNA Orders across the country that have not been executed, potentially posing a serious threat to public safety.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police urge the Federal Government of Canada to move forward with amendments to the *Criminal Code* to provide that:

- DNA Orders are valid until executed; and,
- Unexecuted DNA Orders may be executed anywhere in Canada.

**UNEXECUTED DNA ORDERS**  
*Submitted by the Law Amendments Committee*

**Commentary:**

The *DNA Identification Act*, S.C. 1998, as am. 2000, c. 10 ("*DNA Act*") provides a legal framework to regulate the storage and collection of DNA data and the biological samples from which they have been derived. The *DNA Act* provides for the structure and administration of a national DNA data bank. This database is maintained by the Royal Canadian Mounted Police ("RCMP") and is used to assist Canadian law enforcement agencies in the investigation of serious crimes.

The *DNA Act* must be read in conjunction with the *Criminal Code*, R.S.C. 1985, c. C-46 ("*Criminal Code*") provisions dealing with the collection and use of DNA samples. In January 2008, the *Criminal Code* was amended to expand on the criteria and procedure for collecting the DNA samples.

The *Criminal Code* provisions provide for a provincial court judge to grant an Order for the collection of DNA sample when he or she was satisfied that a designated offence had been committed.

Designated offences are generally serious personal injury offences. The judge has to be satisfied that the issuance of the Order is in the best interests of the administration of justice. Amendments made in January 2008 now provide that a judge may specify in the Order when and where the offender is to attend for the taking of their DNA samples (*Criminal Code*, section 487.051(4)).

Similarly, the amendments now include a provision that allows a warrant be issued for the arrest of any offender who fails to comply with such an Order.

Prior to these amendments, however, hundreds of DNA Orders from across the country had gone unexecuted.

Although not an exhaustive list, on review it would appear that most outstanding DNA Orders went unexecuted for one or more of the following reasons:

1. A non-custodial offender was never turned over to a police officer for DNA sampling;
2. Alternatively, a non-custodial offender was transported to a location to allow a police officer to take a DNA sample, but no officer was available to execute the order;

3. The offender was never served with an “Order to a Person to Have Bodily Substances Taken for Forensic DNA Analysis”; and as a result, the offender left the court without regard to the order;
4. After January 1, 2008, the court did not make an Order in Form 5.041 indicating a specific date, time and place for the offender to attend in order to have his/her DNA sample taken;
5. The custodial offender completed the sentence and was released without submitting a sample of their DNA.

While law enforcement agencies remain in possession of unexecuted Court Orders to obtain DNA samples from the offenders who have committed primary and secondary designated offences (as defined within s. 487.04 of the *Criminal Code*), they cannot execute the Orders without risking breaching section 487.056 of the *Criminal Code* which mandates that DNA samples should be obtained:

- (a) at the place, day and time set out in an order made under subsection 487.051(4) *or as soon as feasible afterwards* or;
- (b) in any other case, on the day on which the order authorizing the taking of the samples is made *or as soon as feasible afterwards*. [emphasis added]

**UNEXECUTED DNA ORDERS**  
*Submitted by the Law Amendments Committee*

**Media Lines:**

- The *DNA Identification Act* became law on June 30, 2000, and it provides a legal framework for the collection and storage of DNA data and the biological samples from which they have been derived.
- There were a number of legislative gaps in the original processes related to these DNA Orders that were not immediately identified (but have since been rectified).
- As a result of some of those previous legislative gaps, there are hundreds of outstanding DNA Orders across the country that have not been executed, which is a serious public safety concern.
- Delays in obtaining a sample for comparison to the Databank mean that previous offences that may have been committed by the offender will remain unsolved, and future offences may go undetected.
- Statistics in England show that with over 2 million DNA profiles loaded into their database there is a 40 percent greater chance of obtaining a match between a crime scene profile and a “criminal justice” (arrestee or suspect) profile.
- In order to deal with the issue of these outstanding DNA Orders, the Canadian Association of Chiefs of Police would like to urge the Federal Government of Canada to proceed with amendments to the *Criminal Code of Canada* and *DNA Identification Act* to allow the courts, on application, to reissue an outstanding DNA Order which compels an affected person to attend at a specific date, time and place to provide a sample as per their original Order; and, should it be demonstrated that the affected person cannot be located for service of such an Order, legislative amendments should also allow for an application to be made to issue a Canada-wide warrant to briefly detain and take a sample upon locating the affected person.

**BUILDING ON FINANCIAL INTELLIGENCE IN ORGANIZED  
CRIME INVESTIGATIONS THROUGH FINTRAC**

*Submitted by the Organized Crimes Committee*

**WHEREAS** there is an effort to support the collaborative nature of the Canadian Law enforcement community, and to enhance the coordination of investigations related to Organized Crime as no single agency can effectively combat organized crime independently, and;

**WHEREAS** the importance of active leadership to ensure effective and efficient integration of operations and intelligence has been identified, and;

**WHEREAS** it has been recognized that financial advantage is the key goal for all criminal organizations, and that consequently, financial intelligence must be an integral component of all organized crime investigations, and;

**WHEREAS** the mandate of FINTRAC is to facilitate the detection, prevention and deterrence of money laundering, terrorist activity financing and other threats to the security of Canada through the analysis of information and dissemination of financial intelligence relevant to such investigations, and;

**WHEREAS** it would be beneficial to Canadian Law Enforcement agencies to maximize the use of financial intelligence provided by FINTRAC in organized crime investigations to increase the cooperation in detecting and combating money laundering and organized crime.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police calls on all Canadian law enforcement agencies to include financial intelligence in their investigations, and share with FINTRAC their Provincial and National enforcement targets.

## **BUILDING ON FINANCIAL INTELLIGENCE IN ORGANIZED CRIME INVESTIGATIONS THROUGH FINTRAC**

*Submitted by the Organized Crimes Committee*

### **Commentary:**

The Financial Transactions and Reports Analysis Center of Canada (FINTRAC) was created in 2000 with the adoption of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), with a mandate to detect, deter and prevent money laundering and terrorist activity financing. Eleven years later, police and the security and intelligence community view the Centre's tactical and strategic financial intelligence products as integral to investigations, prosecutions, intelligence collection and decision-making.

The Centre fulfills its mandate through the following activities:

- gathering and analyzing information on suspect financial activities;
- ensuring those subject to the PCMLTFA comply with reporting, record keeping and other obligations;
- making case disclosures of financial intelligence to the appropriate law enforcement agency, CSIS or other agencies designated by legislation in support of investigations and prosecutions; and
- enhancing public awareness and understanding of matters related to money laundering.

Drawing on its database of millions of financial transaction records, FINTRAC analysts can trace the proceeds of crime money trail for law enforcement, identifying potential suspects and tracking proceeds of crime movements through money laundering activities. The bulk of the hundreds of cases FINTRAC discloses to law enforcement throughout Canada involve voluntary information requests from police for financial intelligence regarding criminal activities such as drug trafficking, fraud and organized crime. FINTRAC offers a unique resource for police because it can, through analysis of the reports submitted by financial institutions, follow the money trail across the country and in many cases offshore. Sophisticated organized crime rings will often use elaborate schemes and many different financial institutions to hide their profits, making it next to impossible for a single police force to track.

The OCC realizes the importance of financial intelligence in the fight against organized crime. In fact, money laundering is an integral process of criminal organizations' activities. Criminal organizations will use all techniques at their disposal, including key facilitators and the banking systems without limiting themselves to domestic transactions.

Realizing that all this financial information is being gathered through FINTRAC, the OCC acknowledged the benefits for FINTRAC to be kept apprised of the issues faced by Law Enforcement agencies and included FINTRAC in its membership.

The law enforcement community also realized that it has an important role to play in ensuring that intelligence agencies are provided with timely and accurate information. With this in mind, a resolution was introduced by the CISC National Executive Committee in 2009 (2009-05) to ensure that all approved operational plans targeting organized crime must be uploaded on ACIIS at the onset of the investigation. This provided the appropriate level of leadership, and ACIIS is now part of most police organization policies, and the necessary intelligence is therefore made available to the intelligence community.

This proposed resolution is intended to be in that same line. It seeks the CACP leadership and endorsement for financial intelligence to become a component of all organized crime investigations. It also seeks for FINTRAC to be recognized as a key partner and as such, informed of the law enforcement community's enforcement priorities across Canada. This will assist FINTRAC to align its priorities with law enforcement and improve the quality of the disclosure cases being produced.

## **BUILDING ON FINANCIAL INTELLIGENCE IN ORGANIZED CRIME INVESTIGATIONS THROUGH FINTRAC**

*Submitted by the Organized Crimes Committee*

### **Media Lines:**

- The CACP Organized Crime Committee (OCC) is focused on addressing the needs of the Canadian Law enforcement community in combating organized crime, promotes innovative law enforcement strategies and contributes to public policy and legislative change as a meaningful partner to the safety and security of Canadians and international partners.
- Following the money trail can shed light on criminal activity as money laundering has basically become standard practice among the criminal organizations.
- The OCC sees added-value to the fact that financial intelligence become a component of all organized crime investigations.
- To this end, FINTRAC has to be recognized as a key partner and is made aware of the enforcement priorities across Canada. This will in turn assist FINTRAC to align its priorities with law enforcement and improve the quality of the disclosure cases being produced.
- Created in 2000, FINTRAC is an independent agency with a mandate to assist the detection, deterrence and prevention of money laundering, terrorist financing and other threats to the security of Canada
- FINTRAC is an intelligence agency and our key product is financial intelligence.
- FINTRAC is one of the most automated financial intelligence units in the world, receiving and processing almost all of its financial transaction information electronically.
- FINTRAC has been able to make a contribution to hundreds of investigations each year of organized crime, smuggling, drug trafficking, and fraud.

**NATIONAL POLICE SERVICES**

*Submitted by the CACP Special Subcommittee on National Police Services*

- WHEREAS** the Canadian Association of Chiefs of Police (CACP) remain committed to support of policing in the Federal, provincial, municipal and First Nations realms, and;
- WHEREAS** the impact of service delivery of National Police Services is essential to the delivery of police services across Canada, and;
- WHEREAS** the delivery of said service requires an effective and efficient provision of National Police Services, and;
- WHEREAS** the effective delivery of consistent service and national standards can only be accomplished through a adequately resourced and funded National Police Services, and;
- WHEREAS** the CACP Special Purpose Subcommittee on National Police Services is mandated to make recommendations regarding service delivery in relation to those services as defined as "National Police Services".
- THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police recommend that the Federal Government of Canada - represented by Public Safety Canada, adequately resource and appropriately fund the National Police Services, and;
- BE IT FURTHER RESOLVED** that an NPS Advisory Committee, representing the regions of Canada, be formed to assist with the governance and future direction of NPS.

## **CANADIAN TRAINING STANDARD FOR CHILD EXPLOITATION INVESTIGATORS**

*Submitted by the E-Crime Committee*

- WHEREAS** Canadians have connected to the Internet and embraced computer related technologies at one of the highest rates in the world, and;
- WHEREAS** child exploitation has become an issue of national and international significance that demands the attention of law enforcement agencies and the criminal justice system, and;
- WHEREAS** to address these demands the Canadian Association of Chiefs of Police created the e-Crime Committee in 2002 with the mandate of this Committee to establish a CACP leadership role in the development of administrative policy and standards for technology-based investigations, the promotion of inter-agency cooperation in the detection and investigation of child exploitation and exploited children abuses, the establishment of training standards and the identification of effective cooperative strategies to combat e-Crime at a local, Provincial, Canadian and International level, and;
- WHEREAS** the committee has addressed in its Strategic Plan the establishment of a leadership role in the development of administrative policy and standards for technology based investigations, the promotion of inter-agency cooperation in the detection and investigation of computer based crime, and the establishment of training standards, and;
- WHEREAS** the training for Canadian law enforcement agencies by the e-Crime Committee has revealed that while specific standardized training programs exist, disparities exist amongst Canadian law enforcement agencies in the application and enforcement of standardized training for child exploitation investigators, and;
- WHEREAS** the investigation of child exploitation by untrained, partially trained or self-trained investigators who do not follow training standards and methodologies creates huge risk for the Canadian law enforcement community which may reduce public confidence in the investigative capability of police agencies, undermine procedural fairness and may serve to bring the administration on justice into disrepute, and;
- WHEREAS** the Canadian Police College has developed and validated specialized child exploitation training courses that are delivered by the Canadian Police College and available to all accredited law enforcement agencies, and;

**WHEREAS** the Canadian law enforcement community has accepted the Canadian Police College Technological Crime Learning Institute training courses as the “standard” for child exploitation investigators, and;

**WHEREAS** the CACP e-Crime Committee has endorsed the Canadian Police College Technological Crime Learning Institute Training Program as the basis for all Canadian law enforcement personnel undertaking child exploitation investigations, and further that the CACP e-Crime Committee recommends that such training be delivered in such a manner as to facilitate learning and qualification in both official languages.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police recognizes the current training at the Canadian Police College for child exploitation investigators, as being an approved agency to provide training in Canadian law enforcement agencies, which recognition does not restrict Canadian Association of Chief of Police member law enforcement agencies from acquiring additional forensic computer training, as would support the investigative function in the furtherance of the common goal, of thorough, comprehensive and impartial e-Crime investigations in the best interests of the Canadian administration of justice, and;

**BE IT FURTHER RESOLVED** that the Canadian Association of Chiefs of Police urges that all member agencies undertaking child exploitation investigations computer undertake these functions only with personnel who have met, at a minimum, the recommended training standards of the Canadian Police College, Technological Crime Learning Institute or other validated training as it pertains to child exploitation investigations.

## **CANADIAN TRAINING STANDARD FOR CHILD EXPLOITATION INVESTIGATORS**

*Submitted by the E-Crime Committee*

### **Commentary:**

Since the creation of information technology, digital information or data is used in the everyday lives of all Canadian citizens and businesses. The range of electronic criminal opportunities is extensive and will continue to expand in tandem with technological advances in online communications and access.

The investigation of child exploitation cases by untrained, partially trained or self-trained investigators who do not follow training standards and methodologies can potentially be a huge risk for the Canadian law enforcement community which may reduce public confidence in the investigative capability of police agencies, undermine procedural fairness and may serve to bring the administration on justice into disrepute. In some provincial jurisdictions it is the responsibility of the police organizations to provide services according to their level of classification therefore mandating more duty and accountability. The Canadian Police College provides training courses which are necessary to enable all police organizations to provide such services and therefore must be properly funded and equipped to provide specialized training for child exploitation investigations in both official languages as required.

## **CANADIAN TRAINING STANDARD FOR CHILD EXPLOITATION INVESTIGATORS**

*Submitted by the E-Crime Committee*

### **Media Lines:**

- Child exploitation crimes have become an issue of national and international significance that demands the attention of law enforcement agencies and the criminal justice system.
- Child exploitation investigations by untrained, partially trained or self-trained investigators who do not follow approved methodologies may potentially create a huge risk for the Canadian law enforcement community.
- Although standardized training programs exist, disparities exist amongst Canadian law enforcement agencies in the application and enforcement of standardized training for child exploitation investigators and covert online investigations.
- It is the recommendation of the CACP that all member agencies undertaking child exploitation investigations, and online covert investigations, undertake these functions only with personnel who have met, at a minimum, the recommended training standards of the Canadian Police College Technological Crime Learning Institute or other validated training.
- The Canadian Police College provides training courses, which are necessary to enable all police organizations that provide such services and therefore must be properly funded and equipped to provide specialized child exploitation training in both official languages as required.

**EVOLUTION OF THE CANADIAN LAW ENFORCEMENT  
STRATEGY TO COMBAT ORGANIZED CRIME (CLES)**

*Submitted by Director General, Criminal Intelligence Service Canada (CISC) on behalf of the  
National Executive Committee (NEC)*

- WHEREAS** the Canadian Association of Chiefs of Police (CACP) fully endorse the principles and values of integration and intelligence-led policing, and;
- WHEREAS** the CACP unanimously provided its support in August 2007 to earlier efforts to develop and implement an integrated, intelligence-led Canadian Law Enforcement Strategy (CLES) to combat organized crime , in which a key component was the use of integrated provincial and national threat assessments for enforcement priority setting at the municipal, provincial and national levels, and resulted in the creation of the Council on Public Safety and its subsequent evolution into the Canadian Integrated Response to Organized Crime (CIROC), and;
- WHEREAS** the CACP acknowledges there is value in formally recognizing the partnership between the functions of intelligence and operations – currently represented by the existing entities of Criminal Intelligence Service Canada (CISC) and the Canadian Integrated Response to Organized Crime (CIROC) – as a means to further the original spirit of CLES in 2007, and that this partnership should be accountable to a common governance framework to achieve consistent, efficient and effective results, and;
- WHEREAS** the CACP concurs that the existing CISC governance structure should be leveraged by expanding its current mandate to encompass the governance of the CISC/CIROC partnership, at the national and provincial levels, under the banner of the Canadian Law Enforcement Strategy (CLES) to combat organized crime:
- THEREFORE BE IT RESOLVED** by the Canadian Association of Chiefs of Police that it fully endorses the modernized CLES, under the governance of the National and Provincial Executive Committees, and demonstrates its support by endorsing the CLES Statement of Commitment, which outlines the expectations of the CLES partnership and the roles and responsibilities of CLES stakeholders.
- BE IT FURTHER RESOLVED** that the Canadian Association of Chiefs of Police recommends that all CACP members in Canada support the modernized CLES and adopt the roles and responsibilities outlined in the CLES Statement of Commitment, as applicable.

**EVOLUTION OF THE CANADIAN LAW ENFORCEMENT  
STRATEGY TO COMBAT ORGANIZED CRIME (CLES)**

*Submitted by Director General, Criminal Intelligence Service Canada (CISC) on behalf of the  
National Executive Committee (NEC)*

**Commentary:**

The Canadian law enforcement community has demonstrated its commitment to combating organized crime through a number of initiatives over the years that are based on integration and collaboration across all jurisdictions to create a safer Canada. Furthermore, organizations such as Criminal Intelligence Service Canada (CISC) and its partnership with the ten provincial criminal intelligence bureaus exist to ensure the production and exchange of information and intelligence and to promote an integrated, intelligence-led approach to law enforcement. This approach emphasizes the importance of collecting and sharing information in order to develop timely intelligence products, which ultimately serve to guide tactical, operational and strategic decisions.

Several years ago, the Canadian law enforcement community committed to an initiative to produce integrated threat assessments intended to inform law enforcement decision-makers. In 2007, the Organized Crime Committee (OCC) of the Canadian Association of Chiefs of Police (CACP) brought forward a resolution to both CISC's National Executive Committee (NEC) and the CACP that introduced the Canadian Law Enforcement Strategy (CLES) to combat organized crime.

The strategy was the first step in establishing a link between intelligence and operations. While it was recognized that the full strategy would develop over time, the initial component was based upon the use of integrated provincial and national threat assessments for enforcement priority setting. The unanimous endorsement to proceed with the strategy's development led to the creation of the Council on Public Safety (CoPS) and subsequently evolved into the Canadian Integrated Response to Organized Crime (CIROC). This national committee is comprised of provincial representatives that exchange information on ongoing investigations and best practices on the enforcement efforts in their respective provinces. At the outset of CLES it was envisioned that in addition to a national committee there would be provincial enforcement steering committees that make enforcement decisions based on integrated threat assessments. The provinces that have established such a committee have recognized the benefits of working collaboratively with their intelligence counterparts. A number of other provinces are at varying stages of implementation.

As CIROC has evolved, so too has its relationship with CACP and CISC. In 2009, the CIROC National Committee sought to realign with CISC's NEC rather than remain with the CACP OCC in recognition that its purpose needs to have a link with the intelligence function. While the relationship and accountability measures were not clearly defined, it was understood that a partnership between CIROC and CISC is critical.

In 2010, an external review of CISC's governance identified a number of recommendations focused on the need to modernize practices, renew partnerships and clarify roles and responsibilities. One recommendation in particular spoke of the need to formalize the relationship between CIROC and the NEC and CISC.

To fully consider the review's recommendations, the CISC NEC established a provisional working group on governance consisting of five regional NEC members (dubbed the "Group of Five"), the DG, CISC and a provincial bureau director. During initial deliberations, the group met with the Co-Chair of the CIROC National Committee to examine the origins of CISC, CIROC and the original intent of CLES. It became clear that there was an opportunity to build upon the progress to date and further CLES by bringing together the two existing entities – CISC (representing the intelligence function) and CIROC (representing the operations function) – under a common governance framework (Appendix 1). Given the existing infrastructure of the CISC NEC and Provincial Executive Committees (PECs) it was further felt that the current governance mandate of the NEC and PECs should be expanded to encompass the CISC/CIROC partnership under the banner of CLES.

It was through this lens that the group developed a new vision statement (Appendix 2) for CLES based on the following key concepts: 1) partnership between the functions of intelligence and operations across all jurisdictions; 2) active and meaningful participation; and, 3) unity of effort through an integrated approach. It was then agreed that a statement of commitment (Appendix 3) was required to complement the CLES vision, clarify the expectations of the CLES partnership and outline the roles and responsibilities of CLES stakeholders (Appendix 4).

It is important to note that the CLES roles and responsibilities are not intended to be prescriptive; rather, they are designed to achieve a balance between the need for consistency to achieve the CLES vision while recognizing that there are regional differences in its application. The common denominator to achieving CLES will be the collective leadership through the governance framework of the NEC, at the national level, and the PECs, at the provincial level. These bodies will provide the necessary leadership in developing and adjusting CLES's vision and strategic direction. Furthermore, they will provide the required leadership to monitor and ensure implementation of resolutions from the NEC. Having senior leaders of the Canadian law enforcement community sign the CLES statement of commitment will bring a new level of clarity to the strategy and affirm a broad base of support for the continued efforts towards achieving the CLES vision.

The group made a presentation to the CISC NEC on May 11, 2011 about the proposed CLES vision, statement of commitment and roles and responsibilities. The outcome was support in principle for the proposal and a motion to commence additional consultation with the PECs and CIROC in advance of resolutions to NEC and CACP to adopt the CLES proposal in August 2011. A number of provinces have already implemented an intelligence and operations partnership under the governance of its PEC, while others are in varying stages of implementation. Given all law enforcement agencies in Canada are stakeholders in CLES, it is essential to inform the CACP membership of the CLES proposal as well as to obtain the membership's endorsement and support to proceed with implementation and execution of CLES across all jurisdictions.

**EVOLUTION OF THE CANADIAN LAW ENFORCEMENT  
STRATEGY TO COMBAT ORGANIZED CRIME (CLES)**

*Submitted by Director General, Criminal Intelligence Service Canada (CISC) on behalf of the  
National Executive Committee (NEC)*

**Media Lines:**

- The Canadian law enforcement community has made significant progress since the Canadian Law Enforcement Strategy (CLES) to combat organized crime was introduced by the CACP Organized Crime Committee in 2007.
- As a leader of progressive change in law enforcement, the CACP supports the continuous evolution of the Canadian Law Enforcement Strategy to combat organized crime.
- Two existing law enforcement entities – Criminal Intelligence Service Canada (CISC) and the Canadian Integrated Response to Organized Crime (CIROC) – currently represent the functions of intelligence and operations respectively.
- A common governance framework for the collaborative effort of intelligence and operations has been proposed that would see CISC and CIROC under one banner – the Canadian Enforcement Strategy to combat organized crime.
- A common governance framework would be created by expanding the current mandate of the National Executive Committee of CISC, as well as those of CISC's Provincial Executive Committees, to include linking together the collaborative effort of CIROC and CISC under these governing bodies to achieve consistent, efficient and effective results.
- The proposed governance framework includes:
  - A vision statement;
  - A statement of commitment to adopting the vision and framework to be signed off by members of the law enforcement community;
  - Roles and responsibilities of all stakeholders in the Canadian Law Enforcement Strategy.
- The proposed strategy enhancements aim to strengthen unity of effort across all law enforcement agencies in Canada to achieve an effective and proactive response to organized crime and to threats to public safety in Canada.

*For reference only:*

*Resolution #09-2007*

*Canadian Law Enforcement Strategy to Combat Organized Crime  
Submitted by the Organized Crime Committee*

**WHEREAS** the Canadian Association of Chiefs of Police (CACP) fully endorse the principles and values of integration and intelligence-led policing, and;

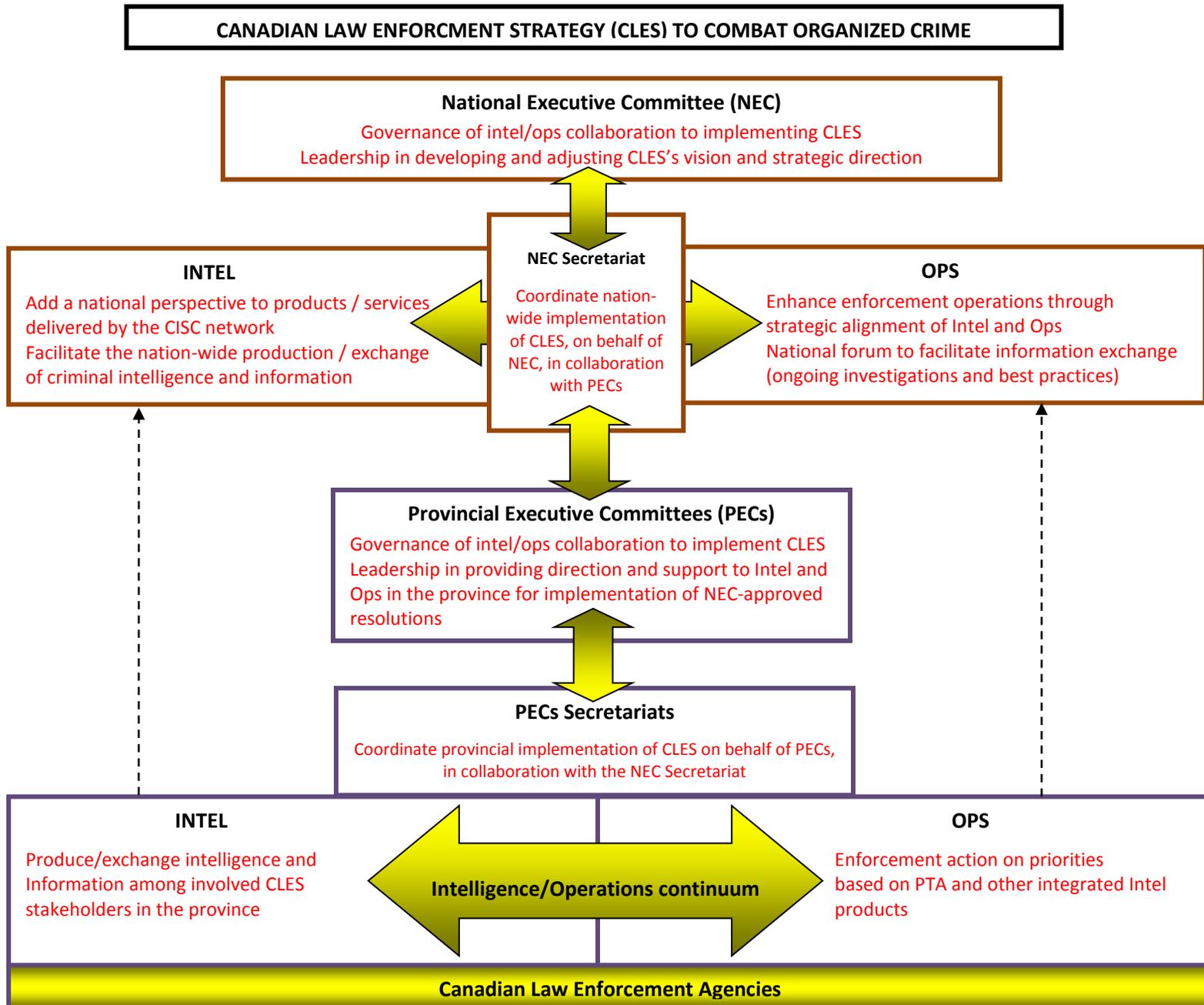
**WHEREAS** Canadians are concerned about the growing and pervasive threat of organized crime in their communities, and;

**WHEREAS** in response to their concerns, and in cooperation with the Law Enforcement Community, the CACP Organized Crime Committee is currently implementing a governance model for which the setting of enforcement priorities at the municipal, provincial, regional and national levels based on the intelligence contained in the National Threat Assessment will be a key component.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police supports the efforts in the development and implementation of the integrated intelligence-led Canadian Law Enforcement Strategy to Combat Organized Crime; whereby enforcement priorities are recognized, based on the Provincial and National Threat Assessments, and acted upon at the municipal, provincial and federal level.

# INTELLIGENCE-OPERATIONS FUNCTIONS FRAMEWORK (2011-07-21)

## High-level Role Descriptions – Appendix 1



## **Canadian Law Enforcement Strategy (CLES) Vision Statement**

The Canadian Law Enforcement Strategy [CLES] embodies the partnership between the functions of intelligence and operations across all jurisdictions of law enforcement. Being committed to a common goal of creating a safer society, Canadian law enforcement agencies are dedicated to active and meaningful participation in CLES to protect Canadians from organized crime. Unity of effort through this integrated approach of intelligence and operations achieves an effective and proactive response to organized crime and to threats to public safety in Canada.

## **Canadian Law Enforcement Strategy (CLES) Statement of Commitment**

Agreement by stakeholders involved in the Canadian Law Enforcement Strategy (CLES):

- National Executive Committee (NEC);
- Provincial Executive Committees (PEC);
- Canadian Integrated Response to Organized Crime (CIROC);
- Central and Provincial Bureaus (CISC);
- Canadian Association of Chiefs of Police (CACP);

hereafter collectively referred to as the senior leaders of the Canadian Law Enforcement Community:

### ***Recognizing:***

- the value in having both the intelligence and operations functions report through the same governing body, both at the provincial level (PEC) and at the national level (NEC);
- the functions of intelligence and operations are distinct yet interdependent;
- the importance of active leadership to ensure effective, efficient integration of intelligence and operations;
- the need for consistency while respecting regional differences;
- the collaborative nature of the Canadian law enforcement community and that no single agency can effectively combat organized crime independently;

### ***Building upon:***

- the essence of CACP Resolution #09-2007 - the origin of CLES
- the legacy of past NEC and CACP resolutions, including the resolve to:
  - contribute to one criminal intelligence database;
  - produce integrated provincial and national threat assessments;

- develop and implement CLES; whereby enforcement priorities are recognized, based on the provincial and national threat assessments and acted upon across all jurisdictions;
- the existence of a national criminal intelligence network since 1970 (i.e., CISC’s network of member law enforcement agencies and the infrastructure and technology provided by CISC’s provincial and central bureaus);
- the commitment of a National Executive Committee that has a concentration of senior law enforcement executives from across Canada who provide leadership, influence and advocacy across all jurisdictions on issues relating to organized crime;
- the commitment of ten Provincial Executive Committees, comprised of senior law enforcement leaders who will provide leadership, influence and advocacy within their province on issues relating to organized crime;
- the commitment of a National Enforcement Committee since 2007 known as the Canadian Integrated Response to Organized Crime (CIROC) that has sought out NEC to be its governing body;
- the establishment and implementation of provincial enforcement priority-setting mechanisms in a growing number of provinces;
- agreement by these provincial priority-setting mechanisms to utilize the integrated provincial threat assessment as part of operational priority-setting;
- the need for a degree of standardized practice;
- the opportunity to advance CLES by forging a partnership between CISC (intelligence) and CIROC (operations);

We, the senior leaders of the Canadian Law Enforcement Community, commit to advancing the Canadian Law Enforcement Strategy to combat organized crime in Canada.

***We specifically commit to:***

- making our common vision a reality by building upon our collective progress to date and work towards a unity of effort;
- enabling the integration and cooperation of intelligence and operations across all jurisdictions through two existing entities – CISC and CIROC (each with its own constitution) – under the governance of the National Executive Committee and each Provincial Executive Committee;

- implementing CACP and NEC resolutions within our provinces and agencies (e.g., contribute information to a common, national intelligence database; collect and share information for the production of an annual, integrated threat assessment; and use the resulting threat assessments for enforcement priority setting);
- supporting the CLES framework and the roles, responsibilities and accountabilities of each involved CLES stakeholder as defined in the attached appendices;
- leading the change required to achieve the collective responsibility to share both information and intelligence within the law enforcement community, while respecting applicable policies and legislation;
- actioning the CLES across all jurisdictions.

### **Signatures**

## INTEL-OPS FUNCTIONS FRAMEWORK STAKEHOLDERS' ROLES and RESPONSIBILITIES

Function/Stakeholder	Roles	Responsibilities
<b>National Executive Committee (NEC)</b>	<ul style="list-style-type: none"> <li>• Governance of CISC/CIROC for the purpose of implementing CLES</li> <li>• Leadership in developing and adjusting CLES's vision and strategic direction</li> </ul>	<p><b>CLES NEC:</b></p> <ul style="list-style-type: none"> <li>• Promote CLES and the collaboration required for its implementation as a viable law enforcement strategy for dealing with organized crime in Canada</li> <li>• Provide leadership to ensure the success of CLES</li> <li>• Monitor progress of implementation of NEC resolutions</li> <li>• Discuss/resolve issues brought forward for NEC resolution by PECs, Permanent Working Group (PWG), CIROC or CISC Supervisory Committee</li> <li>• Evaluate the performance of CISC and CIROC relative to CLES (ensure there is a definition of what constitutes success and that there are evaluation criteria)</li> <li>• Select DG, CISC and assess his/her performance</li> <li>• Identify issues that are beyond reach of Intel/Ops community (leverage other committees such as NCC, CACP-OC or CACP-Law Amendments Committee)</li> <li>• NEC members are responsible for their attendance, discipline, governance methods, development, agendas and ability to envision the future</li> </ul> <p><b>Co-Chairs:</b></p> <ul style="list-style-type: none"> <li>• In addition to traditional duties as Chair, ensure the agenda for NEC meetings identifies successes and challenges, so that learning and improving can take place</li> </ul>
<b>NEC Secretary (DG, CISC)</b>	<ul style="list-style-type: none"> <li>• Coordination of nation-wide implementation of CLES on behalf of NEC, in collaboration with PECs</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain the process for bringing issues forward to NEC from PECs, PWG, CIROC and CISC Supervisory Committee</li> <li>• Coordinate and facilitate NEC meetings</li> <li>• Be the point of contact for all members, NEC and PECs on CLES issues at the national level</li> <li>• Act as Chair of the Supervisory Committee</li> <li>• Develop strategies for communicating NEC resolutions</li> <li>• Develop strategies for monitoring implementation of NEC resolutions</li> <li>• Maintain a process for orientation, development and ongoing progression of NEC members</li> <li>• Represent CISC network when attending PEC meetings</li> <li>• Oversee effective operation of CISC Central Bureau</li> </ul>

Function/Stakeholder	Roles	Responsibilities
<b>INTEL – CISC Central Bureau</b>	<ul style="list-style-type: none"> <li>• Bring a national perspective to the products and services delivered by the CISC network, for CLES partners and beyond</li> <li>• Facilitate / coordinate the nation-wide production and exchange of criminal intelligence and information</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain and enhance the CISC network</li> <li>• Produce an integrated NTA</li> <li>• Produce other integrated intelligence products</li> <li>• Coordinate the ITA process</li> <li>• Assess client needs and evaluate products and services delivered</li> <li>• Maintain and enhance ACIIS</li> <li>• Coordinate, research and develop IT, IM, analytical and other tools</li> </ul>
<b>OPS – CIROC</b>	<ul style="list-style-type: none"> <li>• National forum to facilitate information exchange (ongoing investigations and best practices)</li> <li>• Enhance enforcement operations through strategic alignment of Intel and Ops</li> </ul>	<ul style="list-style-type: none"> <li>• Demonstrate leadership by promoting and influencing integrated priority setting (based on threat assessments)</li> <li>• Ensure NTA is considered when priority setting is done at the provincial level</li> <li>• Promote the sharing of information and intelligence among all law enforcement agencies</li> <li>• Provide operational updates on organized crime within each province</li> <li>• Direct the CIROC Secretariat to undertake special projects</li> <li>• Report successes and challenges in operationalizing intelligence and law enforcement issues</li> <li>• Comparative reporting, i.e. progress over time, on NTA and PTAs</li> <li>• Provide leadership in addressing provincial, inter-provincial and national operational issues on behalf of the enforcement community</li> <li>• Advisory role, i.e. provincial legislation, further intelligence requirements, other operations</li> </ul>
<b>CISC Supervisory Committee<sup>1</sup></b>	<ul style="list-style-type: none"> <li>• Coordination of the criminal intelligence process</li> <li>• Assist the DG, CISC in carrying out nation-wide CLES implementation</li> </ul>	<ul style="list-style-type: none"> <li>• Recommend, through the Chair, CISC Supervisory Committee, resolutions for decision by NEC on changes in policy, strategic direction, CISC Constitution and CISC Regulations</li> <li>• Bring forward factors that may hinder nation-wide implementation of NEC resolutions due to provincial legislation or other restrictions, offer suggestions for alternative solutions, and share best practices for consideration</li> <li>• Advise the Chair, CISC Supervisory Committee of significant issues that may have an impact on CISC</li> </ul>

<sup>1</sup> The Intel-Ops Functions Framework diagram does not show the Supervisory Committee, as the Framework depicts governance of the collaborative effort of Intel and Ops as functions. The Framework is not an org chart. However, the Supervisory Committee’s role in coordinating the criminal intelligence process across Canada is essential and is therefore included in this Roles and Responsibilities table.

Function/Stakeholder	Roles	Responsibilities
<b>Provincial Executive Committee (PEC) <sup>2</sup></b>	<ul style="list-style-type: none"> <li>• Governance of Provincial Bureau/Provincial CIROC for the purpose of implementing CLES</li> <li>• Leadership in providing direction and support to Intel and Ops in the province for implementation of NEC-approved resolutions</li> </ul>	<ul style="list-style-type: none"> <li>• Promote CLES and the collaboration required for its implementation as a viable law enforcement strategy for dealing with organized crime in Canada</li> <li>• Provide leadership to ensure the success of CLES</li> <li>• Monitor progress of implementation of NEC resolutions</li> <li>• Report to NEC on progress of implementation of NEC resolutions</li> <li>• Oversee Provincial Bureau</li> <li>• Create/oversee provincial priority-setting mechanisms (e.g., Provincial Enforcement Steering Committee)</li> <li>• Ensure the Provincial priority-setting mechanism/Provincial Bureau partnership functions as required</li> <li>• Monitor the utilization of PTAs</li> <li>• Monitor the use of ACIS and the participation in the PTA process</li> <li>• PEC members are responsible for their attendance, discipline, governance methods, development, agendas and ability to envision the future</li> </ul> <p>Chair: In addition to traditional duties as Chair, ensure the agenda for PEC meetings identifies successes and challenges, so that learning and improving can take place</p>
<b>PEC Secretary (Provincial Bureau Director)</b>	<ul style="list-style-type: none"> <li>• Coordinates provincial implementation of CLES on behalf of PEC, in collaboration with the DG, CISC</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain the process for bringing issues forward to PEC from provincial priority-setting mechanism and CIS Provincial Bureau member agencies</li> <li>• Be the point of contact on CLES issues at the provincial level</li> <li>• Coordinate and facilitate PEC meetings</li> </ul>

<sup>2</sup> In Québec, the PEC will ensure that the functions of intelligence and operations work together according to relevant Québec legislation and the Projet MINERVE Protocol.

Function/Stakeholder	Roles	Responsibilities
<b>INTEL – Provincial Bureaus</b>	<ul style="list-style-type: none"> <li>Production and exchange of intelligence and information among involved CLES stakeholders in the province</li> </ul>	<p><b>CIS Provincial Bureau:</b></p> <ul style="list-style-type: none"> <li>Ensure integrated PTA is produced and meets the needs of provincial CLES stakeholders (with copy to Central Bureau for NTA development)</li> <li>Guided by agreed-upon national standards</li> <li>Be accountable to PEC</li> <li>Manage provincial component of shared database</li> <li>Provide training at the request of member agencies</li> </ul> <p><b>CIS Bureau Director:</b></p> <ul style="list-style-type: none"> <li>Oversee effective operation of provincial bureau</li> <li>Manage partnership between member agencies</li> <li>Coordinate provincial criminal intelligence effort in alignment with PEC direction</li> <li>Coordinate collaborative effort between Provincial Bureau and provincial priority setting mechanism<sup>3</sup></li> <li>Member of Supervisory (report provincial progress)</li> <li>Maintain contact with Central Bureau</li> <li>Promote the maximum exchange of criminal information and intelligence (in accordance with Privacy and Access to Information legislation)</li> </ul>
<b>OPS – Provincial Priority-Setting Mechanisms</b>	<ul style="list-style-type: none"> <li>Enforcement action on priorities based on PTA and other integrated intelligence products – linking Intel to Ops</li> </ul>	<ul style="list-style-type: none"> <li>Establish provincial enforcement priorities based on integrated PTAs</li> <li>Align enforcement efforts with the PTA and propose an integrated provincial enforcement strategy to PEC</li> <li>Promote the use of ACIS</li> <li>Represent provincial enforcement community</li> <li>Report progress to PEC</li> <li>Bring forward issues to PEC</li> </ul>
<b>Canadian Law Enforcement Agencies</b>	<ul style="list-style-type: none"> <li>Carry out law enforcement function relative to CLES</li> </ul>	<ul style="list-style-type: none"> <li>Ensure meaningful participation to CLES</li> <li>Contribute to CIS Provincial Bureau-led initiatives</li> <li>Contribute to collection effort for annual integrated PTA</li> <li>Ensure adherence to ACIS policy, as applicable</li> <li>Ensure that information/intelligence is shared with agency’s Criminal Intelligence Unit and CIS Provincial Bureau</li> <li>Utilize PTA when establishing local enforcement priorities</li> <li>Report updates on enforcement priorities to provincial priority-setting mechanism</li> <li>Bring forward issues to provincial priority-setting mechanism and CIS Provincial Bureau</li> </ul>

<sup>3</sup> This may require additional resources, which the Provincial Bureaus do not have