Resolutions Adopted at the 113th Annual Conference

August 2018

Halifax, Nova Scotia

CANADIAN ASSOCIATION OF CHIEFS OF POLICE

Safety and security for all Canadians through innovative police leadership

Unit 100 – 300 Terry Fox Drive, Kanata Ontario K2K 0E3
p: 613-595-1101 f: 613-383-0372
e: cacp@cacp.ca w: www.cacp.ca

Table of Contents

Resolution #01 - 2018

RESOLUTION FOR THE TIMELY DEVELOPMENT OF TECHNOLOGY POLICY FOR NATIONAL POLICE INFORMATION SERVICES (NPIS) SYSTEMS FOR LAW ENFORCEMENT IN CANADA

Submitted by the Information and Communications Technology Committee

WHEREAS the Canadian Association of Chiefs of Police (CACP) and its members require reliable, secure, and up-to-date technology to provide an efficient and effective level of service to the communities they serve, and;

WHEREAS the lack of supportive policy surrounding technological tools can cause delays for law enforcement organizations who are working to protect their communities, and;

WHEREAS new technological tools require a vetted policy framework to allow new technology to be implemented to ensure undue risk is not introduced, and;

WHEREAS the law enforcement community has been waiting a number of years for a number of vital technology policies, and;

WHEREAS the Canadian Association of Chiefs of Police Information and Communications Technology Committee, at their February 2018 workshop in Vancouver, BC, identified the "Shortest route to a cloud policy" and the "Shortest route to development of multi-factor authentication policy for mobile devices" as the highest technology priorities for law enforcement in Canada, and;

WHEREAS the National Police Information Services Advisory Board (NPIS AB) provides governance and oversight of all National Police Information Services (NPIS) which supports law enforcement agencies and enhances public safety by encouraging the sharing of electronic information through the National Police Services Network in a timely and cooperative manner, and;

WHEREAS the National Police Information Services Advisory Board (NPISAB) is further responsible for adopting and providing governance over technology policy developed by the Information Technology Sub-Committee of the NPISAB, and;

WHEREAS the Commissioner of the Royal Canadian Mounted Police (RCMP) is the steward of National Police Information Services (NPIS) systems and must comply with Treasury Board of Canada policy and standards relevant to Information Management and Information Technology Security, and;

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urges the NPISAB to update its technology policy development process to ensure that its policies remain current and relevant, and are disseminated in a timely manner, and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police urges the Federal, provincial and territorial (FPT) Ministers responsible for Justice and Public Safety to support law enforcement's desire to maintain reliable, secure, and up-to-date technology through investments in innovation and standard setting.

RESOLUTION FOR THE TIMELY DEVELOPMENT OF TECHNOLOGY POLICY FOR NATIONAL POLICE INFORMATION SERVICES (NPIS) SYSTEMS FOR LAW ENFORCEMENT IN CANADA

Resolution #01 - 2018

Background

The Canadian Law Enforcement community is not keeping up with technology changes and the resulting impacts on policy. At the biennial CACP ICT Committee Workshop in 2016, a policy for cloud computing was identified as a top priority. As of the 2018 ICT Workshop a cloud policy was still not available (federal guidelines are not yet available in relation to Protected B data in the Cloud), nor was a policy for multi-factor authentication for mobile devices, which is absolutely critical to the strategic efforts of many law enforcement agencies.

This may sound like a criticism of those involved, but it is not. Rather, it is an effort to better resource and update the policy development process used to create these technology policies. The goal is to keep up and exploit technology changes in the future. While an in-depth study was not completed, three suggestions were made that may help to produce technology policy in a timely matter. The following characteristics were discussed in the Vancouver ICT Workshop and may have merit in reducing elapsed time in policy development. This example is somewhat specific to Cloud Technology, but it works with many other standards as well.

External Involvement / Resourcing (Academia, Consulting Services, Industry)

We currently seem to take a somewhat insular approach to policy development. The Information Technology Sub-Committee (ITSC) of the NPISAB develops the actual policy with part time volunteer work, in the sense that members of committees, who have full time jobs with police agencies, are tasked with developing detailed technical policies. This results in a huge research workload for those involved, with little time to do the research. If the process was augmented by academia, consulting services and industry, we could work as a panel to craft the actual needs of the policy then work with these representatives to identify options that fit the requirements. We must view such representatives as experts in these emerging areas of technology. Technology companies are developing the technology and often have extensive experience in implementing it. Our concern should be on what we are trying to achieve. In many cases in the U.S., industry is actually a part of the approval process before any policy is released. This has value, both in saving work and time during development, and generally serves to increase policy longevity (some call this “future-proofing”).

Work Within Existing Standards

If we build our own standard for Cloud technology it will:

- Take a long time to develop.
- It will require constant maintenance from the ITSC to keep it current with ever changing technology and standards, generally leading to more delays.

- It may lack future proofing" because of imminent technical change of which we are unaware.

We must, whenever possible, tie our standard to existing industry standards (we realize in the case of Cloud, that the Treasury Board of Canada has not released a cloud policy that covers Protected B data). For example, instead of writing a detailed cloud policy, we could tie our descriptions to a globally accepted standard such as the Cloud Security Alliance (CSA) or a federal standard. As an example, the Cloud Security Alliance has many cloud suppliers as members, as well as a broad spectrum of other security experts that participate. For example, instead of writing a policy that states "we need functions A, B, and C" in great detail, we may be able to tie those requirements to descriptions within the CSA, such as a "at least level 4 within the CSA rating for Geographic isolation". Therefore, as things change and are updated, we merely have to make minor adjustments, not rewrite large sections of descriptive text from scratch.

Create an Approved Working Environment (Cloud Specific)

The U.S. has the Criminal Justice Information Services (CJIS) Cloud Computing standard. It is a pre-approved structure of security that allows law enforcement organizations to take advantage of modern services without having to repeatedly define all the minutia that is involved in setting up a secure cloud implementation. This allows the nimbleness law enforcement needs and the economies of scale that may actually save costs in the long run. If a police agency encountered a major incident where thousands of hours of video needed to be stored and managed, there would be fast and efficient access to mass storage in a cloud environment. It is unknown if the Canadian Treasury Board is working toward such an accepted standard.

Police services in Canada are trying to supply our organizations with dynamic and functional technology, however, the lack of policy is causing them to fall farther and farther behind the technology curve. We must find ways to improve technology policy development process by making it more industry standard and less maintenance intensive.

Resolution #02 - 2018

REASONABLE LAW TO FACILITATE CROSS-BORDER ACCESS TO DATA RELATED TO CANADIAN CRIMINAL OFFENCES OR HELD BY CANADIAN SERVICE PROVIDERS

Jointly Submitted by the Law Amendments and Electronic Crime Committees

WHEREAS many criminal investigations require access to electronic evidence that is stored in other jurisdictions, including the "cloud", and;

WHEREAS cross-border access is one of the most pressing issues for law enforcement around the globe, particularly in the areas of sexual exploitation of children, fraud, cyber-terrorism and organized crime, and;

WHEREAS the current procedure presents challenges in terms of the voluntary collaboration of service providers, cooperation between police forces, the implementation of certain investigative techniques and the effective implementation of international mutual legal assistance in criminal matters, and;

WHEREAS the Parties to the Budapest Convention on Cybercrime agreed, on June 8, 2017, to launch the preparation of a protocol to this treaty to help law enforcement secure evidence on servers in foreign, multiple or unknown jurisdictions, and;

WHEREAS that Protocol could include provisions for elements such as: (i) more effective mutual legal assistance, (ii) enhanced cooperation with service providers in other jurisdictions, (iii) a clear framework and stronger safeguards related to cross-border access to data, and; (iv) safeguards, including data protection requirements, and;

WHEREAS Canada is a Party to that Convention and is participating in this work, and;

WHEREAS the United States of America have enacted, on March 23, 2018, the *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) (H.R. 4943), and;

WHEREAS this Act provides, inter alia, for an alternative and expedited MLAT procedure through bilateral executive agreements with foreign countries to provide data on United States citizens, permanent residents and corporations in a simplified manner to these countries, provided that the Attorney General, with the concurrence of the Secretary of State, is of the opinion that the foreign country has sufficient safeguards to restrict access to data concerning such persons.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police supports Canada's participation in the negotiations on the 2nd Additional Protocol to the Budapest Convention on Cybercrime to address the challenges of cross-border access to digital evidence in criminal matters, and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police urges the Government of Canada to negotiate a bilateral data-sharing agreement with the United States of America who are authorized to do so pursuant to the CLOUD Act, and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police seeks a commitment from the Government of Canada for meaningful consultation with the CACP during the development of these instruments.

Resolution #02 - 2018

REASONABLE LAW TO FACILITATE CROSS-BORDER ACCESS TO DATA RELATED TO CANADIAN CRIMINAL OFFENCES OR HELD BY CANADIAN SERVICE PROVIDERS

Background

On March 23, 2018, the U.S. Congress enacted and the President signed into law the Clarifying Lawful Use of Overseas Data (CLOUD) Act. Intended to resolve problems related to cross-border data requests by law enforcement in the age of email and cloud computing, the CLOUD Act authorizes the U.S. to enter into bilateral data-sharing arrangements and clarifies that a warrant served on a service provider may reach data stored overseas if the data is in the provider's possession, custody, or control. Senator Orrin Hatch commented that, "…the US-UK bilateral agreement framework outlined in the CLOUD Act is intended as a model for future agreements between the United States and other countries…," and, "…implementing similar agreements with…allies is critical to protecting consumers around the world and facilitating legitimate law enforcement investigations." The U.K. government and leading U.S. technology companies support the CLOUD Act.

Canadian law enforcement faces the same investigative challenges and requires an analogous response. For example, a large number of investigations into the sexual exploitation of children on the Internet require access to electronic evidence that is stored in other jurisdictions, including in the cloud. The same is true of fraud, cyber-terrorism and organized crime. Law enforcement requires reasonable, constitutionally-compliant legislation that suits the Canadian context, respects international comity, and provides a framework for service providers to respond to judicially authorized information requests while protecting users' privacy.

Cloud computing, high speed internet, and 'always on' mobile devices impact law enforcement's ability to identify, gather and analyze digital evidence. Although such technology provides countless benefits to Canadians they also present challenges. For example, voice and SMS messaging services are being displaced by app-based communications tools such as WhatsApp and TextMe.[1] Unlike Canada-based telecommunication companies, most large app-based communication service providers store their data in many jurisdictions.

Canadians' increased used of on-line platforms was noted during Public Safety Canada's 2018 consultations with Canadians. Participants reported that timely access to digital evidence is a significant challenge, and called for legislation to clarify roles and responsibilities, support timely and effective investigations, and enable information sharing among Canadian and transnational law enforcement agencies.[2] Information provided during those consultations echoed the Government's acknowledgment that innovative approaches, new solutions, and collaboration with partners is necessary to combat domestic and international crimes such as human trafficking and child sexual exploitation.[3]

---

[1] E. Balkovich, et al, *Electronic Surveillance of Mobile Devices – Understanding the Mobile Ecosystem and Applicable Surveillance Law*, RAND Corporation (2015).

[2] Public Safety Canada, *Countering Online Child Sexual Exploitation: Sharing Knowledge, Enhancing Safety - Closed consultation* (2018). Located at: https://www.canada.ca/en/services/policing/police/consultation-countering-online-child-sexual-exploitation.html.

[3] Public Safety Canada 2017-18 Departmental Plan (2017).

Existing Laws and Procedures Cause Delay and Confusion

Canadian law enforcement often relies on the *Mutual Legal Assistance in Criminal Matters Act*, to access information stored outside Canada or held by service providers located outside Canada. In its 2013 report, *Liberty and Security in a Changing World*, the U.S. President's Review Group on Intelligence and Communications technologies reported that it took approximately 10 months to fulfill an MLAT request for email records. Recent Canadian examples highlight the inefficiencies and delay caused by the MLAT process:

- Google records related to a child pornography investigation were not received until 14 months after the MLAT request was submitted. During that time, the trial Crown was unable to take a position on a resolution and defence counsel was unable to properly assess her client's potential liability.

- During a large fraud investigation with multiple requests for Microsoft, Yahoo and Google records, it took 22 months to receive a portion of the records. The remaining records were provided 25 months after the MLAT request had been submitted.

As these examples demonstrate, the cumbersome and time-consuming nature of the MLAT procedure is incompatible with the operational requirements of investigations and ignores the reality that not all states have specialized liaison offices to support the work of foreign police agencies.

The British Columbia Court of Appeal in *Brecknell* recently highlighted the unacceptable result of strict adherence to territoriality at a time when criminals and communication technologies do not respect national borders:

> *The reality is that criminal activity involving such matters as human trafficking, child pornography, money laundering, commercial fraud and international terrorism conducted by means of electronic communication can be insulated from investigation if a production order is viewed as being implemented where the data is stored and its issuance is, therefore, impermissibly extraterritorial. Such a result is an open invitation to criminals to hide their activity targeting this jurisdiction by ensuring that information about their communications is stored in another.*
>
> *It is notorious that service providers move customer information around the world frequently, no doubt for entirely legitimate commercial reasons, and it seems frequently break up data storing it in a variety of different places. The result may be the effective, if unintended, frustration of investigation into serious criminal conduct.*

Some courts have allowed access to data stored abroad when it is "available" to a person in Canada (e.g. a branch or subsidiary): *eBay Canada Limited v. MNR*, [2010] 1 R.C.F. 145, pars. 48-52. In other cases, local corporations were required to disclose in a jurisdiction even if the data was not stored or available to them. Gorman J.'s ruling in *In the Matter of an application to obtain a Production Order pursuant to section 487.014 of the Criminal Code of Canada*, highlights the unsettled state of the law:

> *I do not disagree with the Court of Appeal's sentiments. International crime causes difficulties for investigators, though international agreements help to remedy these problems (see the*

Mutual Legal Assistance in Criminal Matters Act, R.S.C., 1985). The difficulty with the Court of Appeal's reasoning, however, is that it put its desired result ahead of the proper interpretation of the provision.

Other problems related to territoriality were also noted, such as the legal recognition abroad of certain surreptitious investigation techniques, the notification of the persons whose information was required, the absence of regulations requiring that broadcasters maintain a service bureau in the countries where they broadcast, or that IT or telecommunication service providers confirm the identity of their customers and retain this information for a specified period.

A Potential Solution - Bilateral and Multilateral Agreements

The above-summarized CLOUD Act is an example of legislation that respects international comity, provides a framework for law enforcement and service providers, and protects users' privacy. For example, it authorizes the U.S. to enter into reciprocal bilateral data-sharing agreements with qualifying foreign governments. The reciprocal agreements remove disclosure barriers to law enforcement agencies in both countries. The CLOUD Act also clarifies that a warrant served on a U.S. communication service provider may reach all data in the provider's possession or control, wherever it may be.

The CLOUD Act established a streamlined process to access data and promotes transparency by authorizing service providers to disclose to a foreign government the fact that the provider received a warrant for information stored in that country. The CLOUD Act also gives service providers the ability to challenge a warrant issued for data stored overseas if complying with the warrant would cause the provider to violate the laws of a foreign government.

The CLOUD Act provides a framework for an effective bilateral agreement that is consistent with Canadian constitutional guarantees. It would be a major step forward in the effective fight against crime. Thus, Canada should negotiate a bilateral agreement with the United States of America under the CLOUD Act.

Several international initiatives have also been undertaken to address the issue of cross-border access to data, including the *Council of Europe Convention on Cybercrime* (The Budapest Convention). The Budapest Convention serves as a guideline for countries developing Cybercrime-related legislation and a framework for cooperation between the 57 State Parties.

The proposed Second Additional Protocol to the Budapest Convention is intended to address challenges related to obtaining cross-border access to digital evidence for criminal justice purposes. It is under discussion among States Parties what it will include, however it might include provisions aimed at providing for: (i) more effective mutual legal assistance, (ii) enhanced or more direct cooperation with service providers in other jurisdictions, (iii) a clear framework and stronger safeguards related to cross-border access to data, and; (iv) safeguards, including data protection requirements. Canada is party to the Convention and participates in the work of the Committee. Continuing discussions with member States on mechanisms for efficient trans-border access to data that respect sovereignty and human rights are key to ensuring law enforcement has the tools required to investigate transnational crime.

Microsoft Corp. v. United States demonstrates why legislation and international agreements are preferable to uncertainty and litigation. In that matter, Microsoft refused to provide email stored in Ireland even though a U.S. Magistrate Judge issued a warrant. It was Microsoft's contention that the enabling legislation did not have jurisdiction in Ireland. The matter was rendered moot with the passage of the CLOUD Act.

The Canadian Association of Chiefs of Police requests meaningful consultation with the Government of Canada in relation to the work on the 2nd Protocol to the Budapest Convention on Cybercrime, as well as the conclusion of a bilateral agreement with United States of America under the CLOUD Act.

Resolution #03 - 2018

RESOLUTION FOR THE SUPPORT OF CYBER-CRIME EDUCATION AND TRAINING FOR CANADIAN LAW ENFORCEMENT

Submitted by the Human Resources and Learning Committee
in consultation with the E-Crimes Committee

WHEREAS Cyber-crime is a significant public safety and law enforcement issue that threatens Canadians and businesses, including Canada's societal and economic well-being; in spite of issues with public under-reporting, cyber-crime in Canada appears to be increasing, with nearly 24,000 cyber-crimes reported to Canadian police services in 2016, a 58% increase compared to 2014, and;

WHEREAS the CACP and its members through adoption of prior resolutions have acknowledged that all "cyber-crime", regardless of its underlying motivations, sources or forms, is in fact a crime; and, like all crime, it creates victims who merit our support, and;

WHEREAS in August 2014, the CACP Board of Directors recognized cyber-crime as an emerging concern stating, it is "a topic that challenges the traditional skills, capacities, roles and response patterns of policing", and;

WHEREAS as Canadian law enforcement is adapting to this paradigm of policing, cutting-edge training must be at the forefront to provide law enforcement with the skill-sets required to successfully detect, investigate and prevent cyber-crimes; effective training underpins all law enforcement efforts to combat cyber-crime, including the National Cybercrime Coordination Unit and cybercrime investigative teams announced by the Government of Canada in Budget 2018, and;

WHEREAS Canadian law enforcement generally lack adequate cyber-crime education and training, which inhibits their ability to effectively address cyber-crime and support Canadian victims, and;

WHEREAS the extent to which Canadian law enforcement agencies deliver cyber-crime training to their personnel varies, yet numerous rely predominantly, if not exclusively, on the Canadian Police College, which offers standardized and consistent training in this field to law enforcement agencies across Canada,[4] and;

WHEREAS the Canadian Police College's capacity to provide the most up to date cyber-crime training and deliver courses has been significantly limited, and it is currently not meeting the demand from police services across Canada, as courses are generally full and there are significant waitlists, and;

WHEREAS There is a clear and compelling requirement to increase the capacity of the Canadian Police College as it relates to cyber-crime education and training.

[4] The Canadian Police College delivers approximately 15 different courses and workshops related to cyber-crime or digital forensics to approximately 820 students annually

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls on the Government of Canada to nationally harmonize cybercrime training across the Canadian law enforcement community, and to increase the focus on cyber-crime training and education at the Canadian Police College to ensure Canadian law enforcement have the required skills and capability to combat cybercrime in the 21st century.

Resolution #03 - 2018

RESOLUTION FOR THE SUPPORT OF CYBER-CRIME EDUCATION AND TRAINING FOR CANADIAN LAW ENFORCEMENT

Background

Cybercrime significantly impacts the safety and economic well-being of Canadians and businesses, and regularly victimizes vulnerable members of our society. No single organization can resolve cybercrime alone. Even though cybercrime appears to be significantly under-reported, in 2016, nearly 24,000 cybercrimes were reported to Canadian police services, which is a 58% increase compared to 2014.

Cybercrime requires new ways of policing and training approaches. Law enforcement across Canada and around the world are increasingly faced with cybercrime, and are recognizing a need to shift the paradigm of policing to address cybercrime. However, significant gaps exist with respect to the knowledge and skills required to effectively combat cybercrime. Canadian law enforcement lacks adequate training for cybercrime and frontline units to detect and pursue cybercriminals.

In Budget 2018, the Government of Canada announced $201.3 million over five years and $43 million per year ongoing devoted to the creation of the RCMP National Cybercrime Coordination Unit and to increase the number of RCMP cybercrime investigative teams dedicated to conducting federal cybercrime investigations. This increased Government of Canada focus on combating cybercrime has resulted in a pressing requirement to improve and expand cybercrime law enforcement training.

As a National Police Service that serves the broader Canadian law enforcement community, the Canadian Police College (CPC) is uniquely positioned to deliver cybercrime training to all Canadian law enforcement. In 2015, the Government of Canada invested in law enforcement cybercrime training by funding four new full-time positions at the CPC's Technological Crime Learning Institute (TCLI). Despite these enhancements, the CPC's capacity to provide the most up to date training and run a significant number of cybercrime courses has been limited. It is currently not meeting the demand from police services across Canada. Increasing the focus on cybercrime training and education at the CPC, in partnership with other police academies, is necessary to ensure Canadian law enforcement is equipped to combat cybercrime and meeting policing requirements of the 21st century.

The CACP has passed prior resolutions in regard to cybercrime and related issues. This resolution aligns with these, as having the necessary knowledge and skills must underpin all law enforcement efforts to combat cybercrime. Without addressing law enforcement's cybercrime training gaps and challenges, Canadian law enforcement's ability to combat cybercrime will be hampered.

Resolution #04 - 2018

RESOLUTION FOR THE REGULATION OF PILL PRESSES

Submitted by the Drug Advisory Committee

WHEREAS the illicit use of pill presses has increased the availability of street drugs containing synthetic opioids such as fentanyl, and;

WHEREAS the result is causing a public health crisis in communities across Canada, and;

WHEREAS amendments to the Controlled Drugs and Substances Act Canada in 2017 (Bill C-37) does not provide effective measures to restrict the importation and domestic supply of pill presses for illicit purposes.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urge Public Safety Canada to protect Canadians by further amending the Controlled Drugs and Substances Act to comprehensively vet persons importing pill presses, have them specify the intended use and to regulate their domestic sale.

Resolution #04 - 2018

RESOLUTION FOR THE REGULATION OF PILL PRESSES

Background

In 2015, Western Canada observed a startling increase in overdose deaths. This increase can in part be traced back to the reformulation of the opioid Oxycontin. In 2012, Oxycontin was replaced with the tamper resistant product OxyNEO. The impetus for this was to reduce the illegal diversion of Oxycontin for non-medical use. The unfortunate unintended consequence was that these diverted opioid pills were more difficult to source on the street which opened up the illicit opioid drug market to counterfeit Oxycontin pills – fentanyl.

Organized crime and street level drug dealers started to purchase fentanyl and its analogs and began counterfeiting "Oxy 80" pill for street sale. Industrial pill press machines, dyes, stamps, encapsulators and pill sorters were legally purchased and imported for this purpose. In our efforts to disrupt this illegal market we were frustrated with the ease at which these devices could be purchased and imported. Several investigations have revealed the significant amount of pills that could be produced for street distribution with these industrial pill presses.

Unfortunately, today the opioid crisis continues to have a devastating impact on communities across Canada. In 2016, British Columbia had 982 overdose deaths and in 2017 to August 31 there have been 1,013. In approximately ninety percent of these deaths fentanyl was detected. In 2017, provinces across Canada experienced increases in overdose deaths related to opioids.

In 2017, Bill C-37 received Royal Assent to amend the *Controlled Drugs and Substances Act*. This Bill provided valuable tools to better equip law enforcement to disrupt opioid importation and production. One tool critical in disrupting the opioid crisis was regulating pill presses and encapsulators, thereby making it more difficult for drug dealers to mass produce counterfeit pills. Unfortunately, Bill C-37 did not go far enough to deter the importation of pill presses for illicit purposes. Specifically:

- Lack of comprehensive vetting of persons and businesses importing pill presses and encapsulators
- No requirement for importers to articulate intended use
- No controls over domestic sales or resale of imported pill presses
- CBSA not provided with full range of powers under s.46 of the CDSA to arrest and charge for illegal importation of pill presses

Counterfeit pills containing fentanyl and its analogs continue to make their way to the illicit drug markets across Canada. Enforcement action on drug labs demonstrate that pill presses, encapsulators, stamps and dyes are widely used in the production of these counterfeit pills. Tightening up the regulations will assist law enforcement with disrupting the distribution of illicit counterfeit fentanyl pills.

Resolution #05- 2018

DEVELOPMENT OF THE SEXUAL VIOLENCE RESPONSE MODEL

Submitted by The Crime Prevention, Community Safety and Wellbeing Committee and Victims of Crime Committee

WHEREAS the Crime Prevention, Community Safety and Wellbeing Committee's (CPCSW) strategic objectives include identifying new models of collaborative and integrated approaches for community safety, health and wellbeing, and;

WHEREAS the Victims of Crime Committee's strategic objectives include promoting effective practices and enabling innovation when dealing with victims of crime, and;

WHEREAS it is estimated that sexual violence occurs more than 600,000 times per year in Canadian Communities and remains one of the most underreported crimes in Canada, impacting victims by causing psychological dysfunction, post-traumatic stress and suicidality, and;

WHEREAS sexual violence can be more effectively and efficiently addressed through the fundamental principles of contemporary community policing; and collaboration among police and non-police sectors, (education, prevention, intervention, response, support, evaluation), and;

WHEREAS the CACP Board of Directors encouraged all police services to review practices around Sexual Violence investigations and that the CACP Victims of Crime Committee and CPCSW Committee provide recommendations on best practices and to share them throughout the policing community, and;

WHEREAS the Sexual Violence Response working group is comprised of leaders from police services and community organizations who possess expertise in the area, and;

WHEREAS the Sexual Violence Response Model is a collaborative advocate review program committed to providing a victim-centered response to crimes of sexual violence. The model endorses best practices, evidence-based, trauma-informed investigations, and;

WHEREAS the CACP has previously endorsed national standards as a means of promoting common principles.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police requests that the Government of Canada endorses and supports the development of a Sexual Violence Response Model.

Resolution #05- 2018

DEVELOPMENT OF THE SEXUAL VIOLENCE RESPONSE MODEL

Background

In February 2017, The Globe and Mail released an article outlining how police handle sexual assault allegations. Data gathered from more than 870 police services indicated deficiencies during the investigative process contributing to the discouraging statistic that one in every five sexual assault allegations in Canada is classified as unfounded.

The Globe and Mail reported that, on average; Canadian Police Services are dismissing 19 percent of all sexual assault allegations as unfounded (during the reporting years of 2010-2014).

As a result of the unfounded series, law enforcement agencies across the country have reviewed more than 37,000 files. UCR coding was obvious as a significant contributor of the unfounded investigations, as a result 6,348 files, once cleared as unfounded were found to be misclassified.

The Globe and Mail reports 402 unfounded files were reopened as a result of the reviews with half a dozen being recognized as "should have resulted in criminal charges". This finding raised valid concerns and police services dug deeper to identify the root cause throughout the investigative process. Issues have been recognized such as inadequate training in trauma informed practices, dated interviewing techniques and the persistence of "rape myths" among justice partners.

In October of 2017 a working group of police leaders was developed in order to create a framework to ensure that the police response to complaints of sexual violence is coordinated, effective, and victim-centered. The goal is to develop a consistent, comprehensive provincial framework on a standardized sexual assault review model; a Canadian Model. The working group is currently developing a framework for a model that will include quarterly reviews of all unfounded cases, a review of all or a sample of uncharged cases that are not open (no further action) and fulfill the Privacy Commission criteria for review, include all Domestic Violence cases with a sexual assault component and is considering review of all human trafficking investigations.

It is anticipated that the working group will continue to develop best practices for evidence based trauma informed investigations while improving on our support for victims of sex related crimes. Included in the framework will be shared language and understanding of sexual violence that can be used among police agencies and with our community partners. This framework will be the product of collective efforts involving subject matter experts from policing, academia, and community organizations. Rooted in leading evidence-based research and practices, the goal is for the framework to serve as a foundational guide on which municipal, regional, provincial and national police organizations can build their own policies.

Outreach and research (through surveys) has been conducted by the Sexual Violence Review Model working group in order to evaluate the need for a consistent framework. The following responses have been documented;

- Sixty eight (68) percent of services are engaged or are considering a review process similar to the one proposed by this working group
- Seventy two (72) percent of those canvassed are planning to complete ongoing reviews yearly with advocate agencies but have to address barriers such as; financial, a need for unified best practices, and creating a Memorandum of Understanding.
- Sixty two (62) percent responded that officers required more training around "trauma informed" practices during their investigations.
- Fifty two (52) percent of those polled had not created a memorandum of understanding while seventy nine (79) percent were aware of the guidelines of the Privacy Commissioner.

It is evident that a best practice guideline, outlining the most efficient and prudent course of action in regards to sexual violence is necessary not only provincially but across the Country. This group, representative of eighteen (18) police services has the capability of delivering a product that can be seamlessly adopted by police services.