Canadian Community Safety Information Management Strategy

February 25th, 2015

Acknowledgements

Acknowledgement

The Canadian Associations of Chiefs of Police (CACP) acknowledges the significant contributions of the Canadian Community Safety Information Management Strategy (CCSIMS) Working Group in the development of this document. The CACP also acknowledges the contributions of the following supporters in the development of the CCSIMS.

Our CCSIM Strategy Supporters

Gold Supporters

Silver Supporters

Record of Amendments

Version	Date	Pages	Amended By	Changes
Original	Jan 12/2015			
Ver2	Jan 31/2015	All	C. Davis	Based on CCSIMS Working Group feedback
Ver 3	Feb 13/2015	All	C. Davis	Based on CCSIMS Working Group feedback
Ver 4	Feb 25/2015	1-4	L. Valcour/C. Davis	Updated Background Section
V5	June 25th, 2015	iv	L. Valcour	Updated Executive Summary

Table of Contents

Executive Summary

The Canadian Community Safety Information Management Strategy (CCSIMS) is a strategic document that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises to promote information management in Canada. The CCSIMS, through its Action Plans, provides a series of action items, including milestones, to help emergency responders and relevant government officials make measurable improvements in day-to-day operations, as well as emergency communications, on an annual basis.

The CCSIM Strategy aligns with the Communications Interoperability Strategy for Canada and will be enabled by the following key elements:

- Effective Governance;
- A Responsible Sharing Culture;
- Supporting and Balanced Legislation;
- Established and Implemented National Data Standards and Supporting standards-based approaches, Procedures and Processes; and
- Technology Enablers for Responsible Information Management for Community Safety.

The CCSIMS therefore, promotes the vision for a comprehensive and integrated information sharing capability as part of a broader communications interoperability strategy for Canada and coordinated with United States (U.S.) partners as required. The overarching intention of this document is to assist key community safety stakeholders to work in a coordinated manner while respecting federal, provincial and territorial laws, regulations, and existing plans. The extent of participation by any jurisdiction is encouraged, but remains voluntary.

Canadian Community Safety Information Management Strategy

1. Background

Canada has a very long and proud history of law enforcement information sharing. In 1972, the Canadian Police Information Centre, or CPIC, began operating nationally. Managed on behalf of all Canadian law enforcement agencies by the Royal Canadian Mounted Police, at the time this system was state of the art. Allowing police officers from coast to coast access to a wide range of mission critical data in seconds, CPIC has been the lifeblood of operational policing in Canada for over 40 years.

In the years that followed a wide range of specialized computer systems, almost all proprietary and siloed in nature, emerged. As a result, the information management landscape in Canada became more complex and often less interoperable.

The CACP Informatics Committee (now ICT Committee) hosted its first ever national conference in 1998 in Cornwall. The focus of this event was police information sharing, interoperability and interconnectivity.

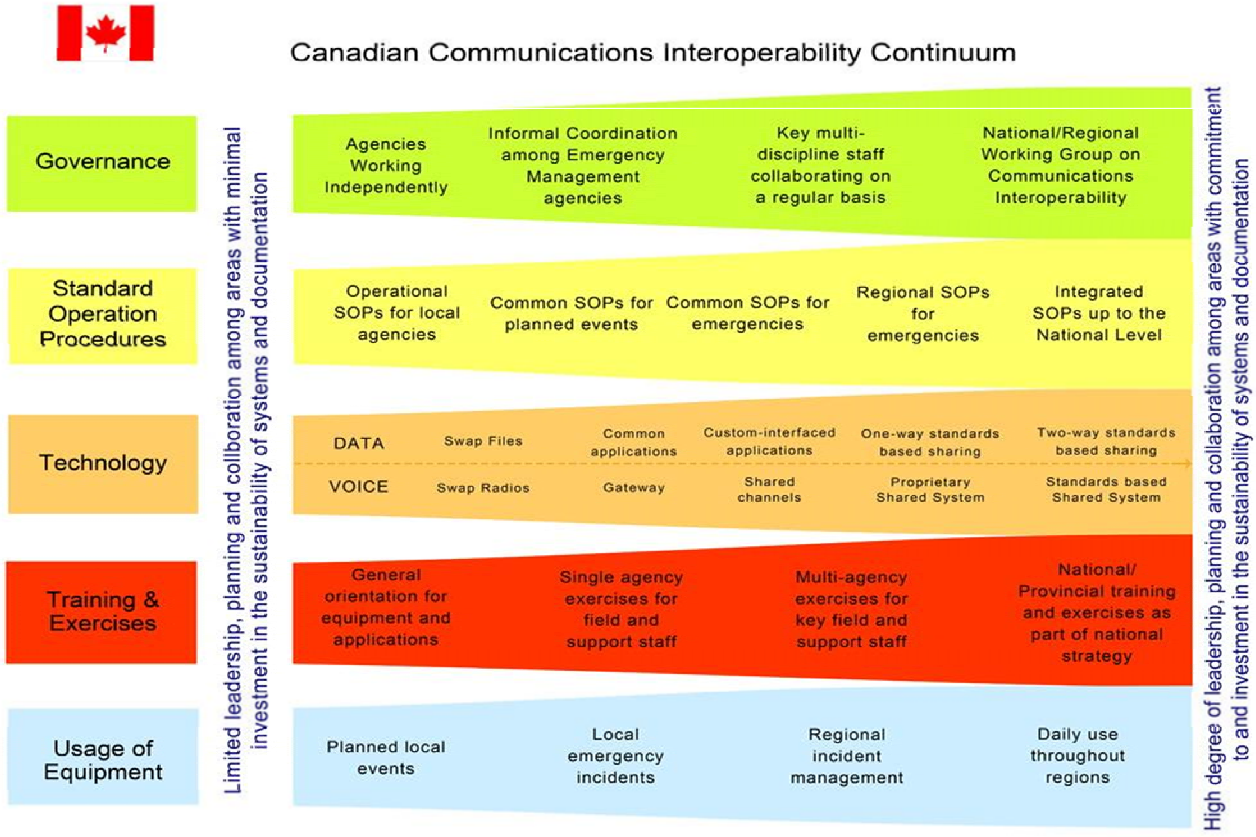
Police leaders from London, Windsor and Vancouver, commenced working on an information sharing initiative known as the Law Enforcement Information Management system, or LEIM. This tool initially allowed Ottawa, London, Windsor and Vancouver police to instantly share a wide range of data including occurrence reports and street checks.

The system, now known as the Police Information Portal, or PIP, is an integral component of law enforcement information management in Canada and is managed by the RCMP's National Police Services. While it served as a critical step in the evolution of information sharing, it too is limited in scope and is in the process of being reviewed with a view to enhancing its capabilities.

In 2007, the Canadian Association of Chiefs of Police (CACP), Canadian Association of Fire Chiefs (CAFC), and Emergency Medical Services Chiefs of Canada (EMSCC) joined forces with the Canadian Police Research Centre (CPRC) to create the Canadian Interoperability Technology Interest Group (CITIG). This initiative brought together representatives from public safety, industry, academia, government, and non-governmental organizations to work collectively on the future of Canadian public safety interoperability.

.

This initiative also led to the development of the Communications Interoperability Strategy for Canada (CISC), which set out a strategy to improve local and regional capacity to interoperate using the Interoperability Continuum as a means of pointing the way forward, suggested action items, and criteria for measuring success along the way. Emergency communications is defined as the ability of emergency responders to exchange information via data, voice, and video as authorized, to complete their missions. The Canadian version of the Interoperability Continuum is depicted below.



At its second annual national interoperability conference in December 2008, CITIG partnered with the Canadian Associations of Chiefs of Police, Fire and Paramedics and the Senior Officials Responsible for Emergency Management (SOREM is a Federal Provincial and Territorial partnership with Public Safety Canada (PS) acting as the secretariat).

A number of key “Action Plans” were developed on a wide range of interoperability issues that needed to be improved. One of the issues identified was that of a lack of data standards available to enhance information sharing. For example, a 2007 report on cross-border data exchange concluded that Canadian and U.S. law enforcement agencies would benefit from the adoption of a commonstandard of information

exchange. As a result, an action plan titled “Support the adoption of data exchange standards/ models” was developed and approved.

PS has worked with federal, provincial, territorial and municipal agencies to improve data interoperability as these agencies acknowledge that the lack of common standards for the exchange and use of data is a serious impediment to effective interoperability.

In 2009, the CACP Informatics Committee established a sub-Committee to deal specifically with information exchange and data standards. Subsequently, PS, in partnership with CACP, developed a draft *National Data Quality Standards Strategy* (NDQS). As part of its role in that Strategy, PS and the Centre for Security Science (CSS) jointly sponsored a study to establish a standards-based approach to exchanging information" for police agencies. The report, issued in August 2010, recommended the adoption of the National Information Exchange Model (NIEM).

Since this time, the CACP has created an operational committee “Law Enforcement Information Data Standards” (LEIDS) to drive data exchange interoperability based upon NIEM. This committee is responsible to establish standard data exchanges for law enforcement and partners across Canada.

In 2011, the Canadian Interoperability Technology Interest Group, or CITIG (www.citig.ca), submitted a proposal to the ICT Committee. This proposal recommended, as a first step in a multi-year, multi-phase approach, the commencement of a “National Law Enforcement Information Management Strategy Study.”

The study was designed to provide a detailed analysis of the current major investigative and operational databases in the policing community across Canada at the local, regional, provincial and federal levels. It was based on a series of in person interviews and a structured questionnaire to be developed by CACP ICT professionals, led by the CACP Informatics Committee.

The study was completed by IDC Canada and funded by the Canadian government’s Centre for Security Science. It clearly outlines the lack of interoperability between information management systems, sometimes because the “systems” are actually paper based.

The study provides, in a quantitative, qualitative and evidence-based fashion, an outstanding analysis of exactly what operational systems are in place and any interoperability between them. It also outlines why the systems are not interoperable bases on criteria such as policy, privacy, technology, etc. (add link to study here)

The next phase of the development of a national strategy was for the CACP ICT Committee to host, as part of the series of events going back to Cornwall in 1998, a

National ICT Workshop in February 2014 in Vancouver. The number one recommendation flowing from the workshop, accepted unanimously by delegates, was:

That the Board of the CACP be asked to assign the ICT Committee to develop a National Law Enforcement Information Management (NLEIM) Strategic Plan for consideration and possible adoption by the CACP.

This recommendation was subsequently approved by the CACP Board of Directors.

The third phase of the ICT Committee's effort was to plan a three day workshop in Ottawa in November. About 30 of Canada's leading law enforcement and justice information management experts attended, with facilitation being provided by Lansdowne Technologies Inc. and a member of the Ontario Provincial Police.

The Workshop was based on a similar event led by CITIG in 2008 where the Communications Interoperability Strategy for Canada (CISC: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-eng.aspx) was first drafted.

Attendees, from key stakeholder groups such as the CACP ICT Committee, National Police Information Services Advisory Board (the NPISAB is a "Commissioner's Advisory Board," reporting to the Commissioner of the RCMP), Provinces, Territories (via RCMP) and Public Safety Canada attended the workshop.

The CACP enlisted the support of CITIG and the Canadian Advanced Technology Alliance (www.cata.ca) to help plan the Workshop and to develop funding support via their networks.

During the workshop, a number of delegates pointed out the linkages between this process and other important community motivation movements in Canada as well as the Economics of Policing / Community Safety efforts led by Public Safety Canada. As a result, the name of the draft strategy was changed from the National Law Enforcement Information Management Strategy to what is now known as the Canadian Community Safety Information Management Strategy.

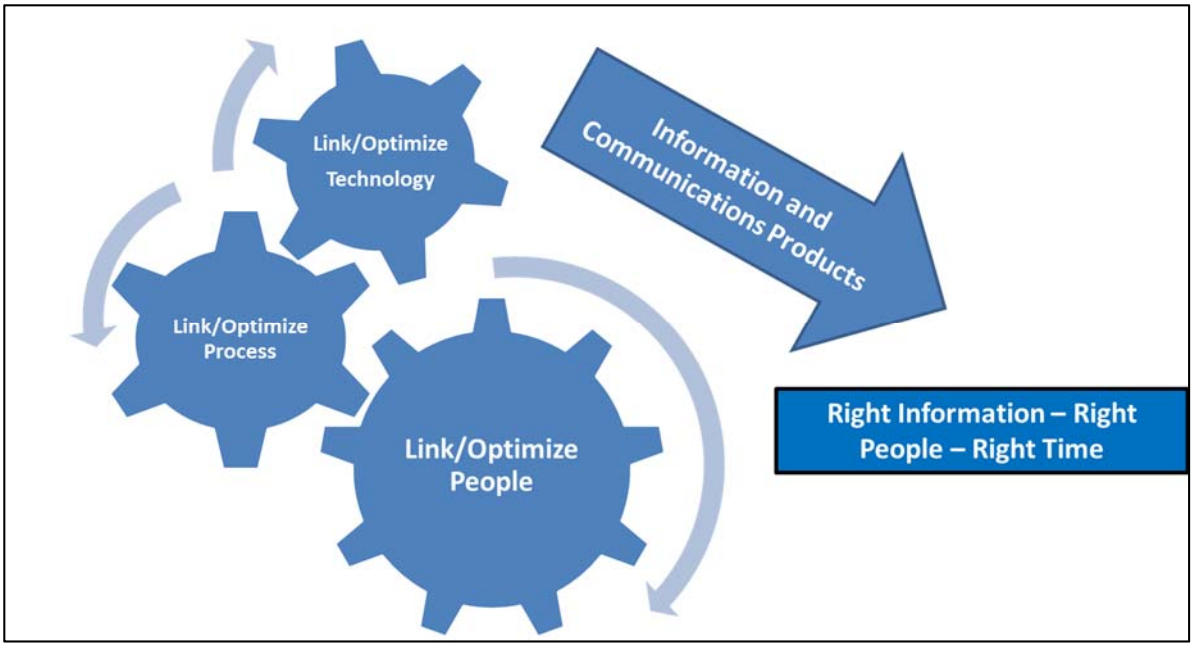
2. Purpose

The purpose of the CCSIMS is to establish the framework and supporting Action Plan required to achieve the CCSIM Vision**: "Responsible Information Management for Community Safety"**.

3. Scope/Strategic Context

Police and other community safety services across Canada are constantly attempting to improve their effectiveness and efficiency. This means looking at what they need to do differently and what they need to do better. This is about turning challenges into opportunities while the sustainability of the cost of policing is being debated and crime continues to evolve. In the evolution of policing and community safety strategies, information management is a key component. An enhanced Canadian Community Safety Information Management Strategy will allow all key community safety partners and services to work smarter and safer.

In simple terms the CCSIM Strategy is designed to leverage people, processes and technology to get the right information to the right people at the right time in support of a broad community safety information sharing environment.

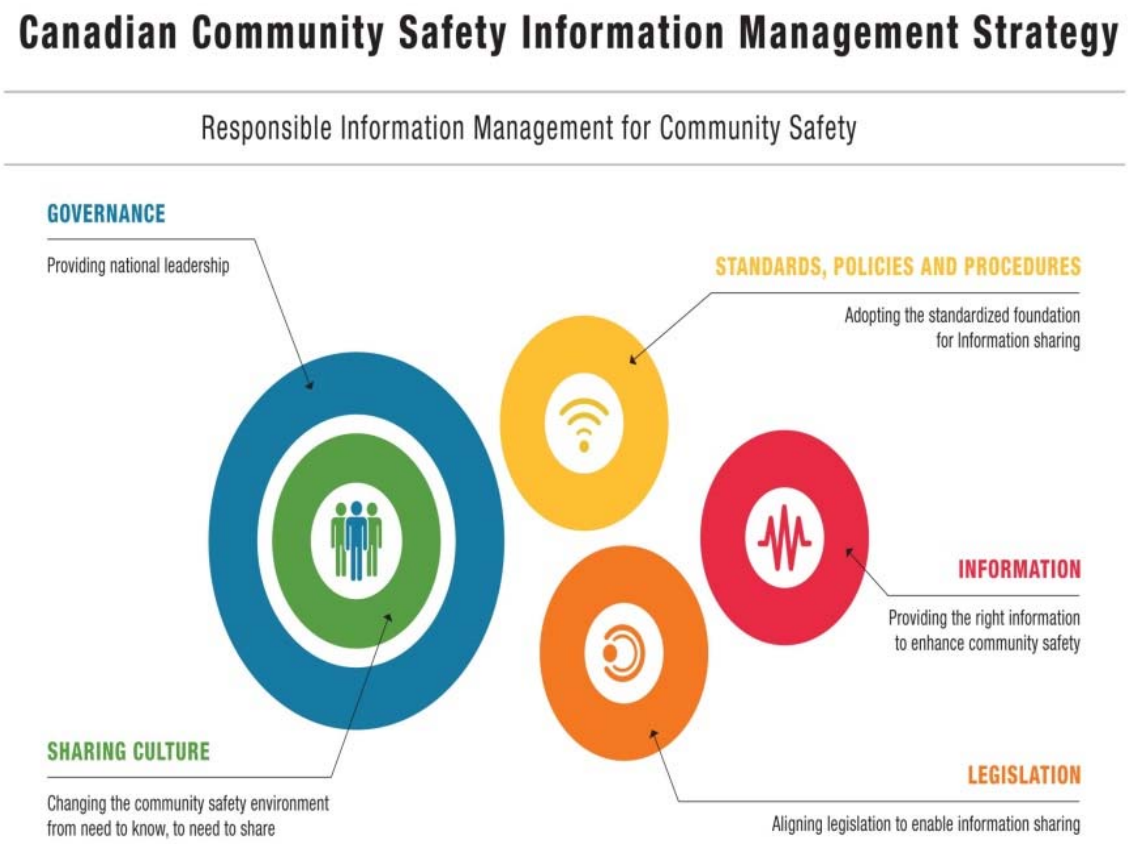


Demands on already finite resources are significantly impacted by: requests for a police response to non-criminal issues; cutbacks and changes in government and social services and programs; requirements of legislation, case law and the judiciary; borderless criminal activities; along with emergent events requiring law enforcement intervention or support. If police services do not manage their information effectively at a national level, individual organizational resources and information are limited.

All modern policing organizations collect a vast amount of data at an increasing velocity. This presents both a challenge to manage, but an opportunity to transform this data into a valuable asset. Compound this ability to share information between services, and the

opportunities are exponential. Benefiting from information requires creating governance, processes, enabling legislation while creating a working environment with the willingness to understand the importance of information management and sharing for a public safety advantage.

By connecting the dots, as illustrated in the graphic, the CCSIMS will lead to the development of the required components to support greater collaboration between services which contribute to community safety. Together the components will allow for greater information management and sharing which in turn will enhance police service delivery in Canada. The result will be greater localized public safety knowledge and broader community partnerships.



Managing and maximizing our information and the resulting actionable intelligence can assist in advancing prioritization and the deployment of resources. By working more efficiently we will be able to redirect resources to address new and emerging threats to community safety. Together, these five areas which support information management will propel police services, working alongside their partners, into the next era of community safety.

4. Strategic Objectives

The CCSIMS will be guided by the following strategic objectives:

- **Governance.** CCSIMS governance will be representative and reflect a national approach with appropriate Federal, Provincial, Territorial and Municipal membership within a formal national governance model. The CCSIMS governance model will enjoy a high degree of leadership and buy-in. Establishing and maintaining a sustainable funding model for CCSIM Strategy related efforts is also central to the success of the CCSIM Strategy.
- **Sharing Culture**. Community Safety stakeholders and partners will work collaboratively and practices will reflect Responsible Information Management for Community Safety. The sharing culture will be evident in practice and balance the need to share with due regard for operational and legislative constraints.
- **Legislation**. Privacy and related Community Safety related legislation (development, implementation, application and interpretation) supports secure and responsible Information Management for Community Safety.
- **Standards, Policies and Processes.** Data and information related open standards and supporting policies, standards-based approaches (e.g. NIEM) and processes contribute to collecting, receiving, sharing, using and archiving data. Training and exercises reinforce established standards, policies and processes.
- **Information and Technology Enablers**. All source information (text, audio, video, GIS, etc.) and the supporting technology enablers (software, applications, systems, networks) are guided by a formal Technology Roadmap that aligns future investments.

A “Game Plan” providing an overview of the CCSIMS is provided at Annex A.

5. Case for Change

Police and Law Enforcement, Emergency Services, and other Community Safety partners face an increasingly complex and ever-changing information management environment compounded by increased information requirements and sources to manage. Notwithstanding lessons learned from past investigations and reports, the development and implementation of the CCSIM is driven by a critical operational requirement to develop the tools and processes to facilitate information sharing to fight crime more effectively and to meet the demands and expectations of the public we collectively serve. This is an operational requirement and the status quo is not a viable option as the current approach to Community Safety Information Management is not sustainable and is further complicated by a lack of aligned open standards, funding challenges and staff demands.

Implementation of the CCSIM Strategy will ultimately lead to operational, economic, and technical efficiencies that will contribute directly to enhanced community safety.

6. Guiding Principles

The development and Implementation of the CCSIMS and associated action plans will be reflected by the following guiding principles:

- The strategy and Action Plans will be national in Scope (FPT Supported and engagement with Municipalities).
- Aligns with the CISC and the Canadian Interoperability Continuum.
- The strategy and action plans will be needs and operationally driven.
- Citizen/Community Safety Centric
- Resonates with operational leaders, stakeholders and community members
- Reflects and Respects Legislation, Jurisdictions, Privacy, Security, etc.
- Standards Based
- Creates end to end efficiencies
- Reuse existing investments and governance bodies where possible (e.g. LEIDS)
- Sustainable

7. Implementation

The CCSIMS is designed to provide a framework for the use by all jurisdictions within Canada at any level and all key stakeholders to assist in identifying and strengthening information management and sharing capabilities. The implementation of the CCSIMS is achieved through the attached Action Plan (Annex B) that documents specific responsibilities and the basis for resource allocation by respective organizations. The Action Plan is based on the strategic objectives identified in the CCSIMS which are core to developing action items and timelines for CCSIMS activities over the next three to five-year period.

To be effective, the CCSIMS must be backed by appropriate commitment and adequate plans and developed in collaboration with all jurisdictions and key stakeholders. The success of the CCSIMS will be measured by the deliverables and timelines described in the Action Plan. An ongoing and coordinated communications plan will convey achievement on the CCSIMS.

In addition to the action items associated with the CCSIMS, jurisdictions and key stakeholders are encouraged to initiate CCSIMS guided plans that support their specific or unique needs, in a manner consistent with the CCSIMS.

8. Review and Capability Improvement Process

Community Safety Stakeholders will work together to monitor the implementation of the CCSIMS and support the assessment of programs and activities against the Interoperability Continuum. It is expected that the collaborative approach established in the CCSIMS and the associated CISC will remain current and strengthen coherency of action among all levels of government and contributors.

The success of the CCIMS will be measured by deliverables and timelines provided in the CCSIMS Action Plan and will be considered successful when the performance indicators set out in the Action Plan are met.

The CCSIMS will be reviewed and revised, in consultation with key stakeholders, every three years, or more frequently, if necessary. Pending the creation of a formal CCSIM Governance model, the Action Plan will be reviewed and updated at least annually and approved by the CACP.

Annex A – Canadian Community Safety Information Management Strategic Framework

Background Information / Influences

- Communications Interoperability Strategy for Canada and Action Plan
- Increased reliance on rich real-time data for operations and community safety initiatives
- Emerging y technology and data opportunities
- Campbell, Pickering Reports
- Bernardo, Pickton, Highway of Tears investigations

Current State Assessment

Governance
- No current national governance or coordination body with federal, provincial and territorial representation focused on information management requirements and opportunities
- CACP is the primary champion for this issue with support from various entities
- Funding for information management initiatives is fragmented. No sustainable funding model is in place (compounded by current procurement practices)

Sharing Culture
- Limited sharing between police agencies and other community safety partners
- The Hub Model in Saskatchewan is a good practice with potential to be a national model
- The true value and benefit of information sharing is not fully recognized

Legislation
- Current legislation varies across jurisdictions and hamper efforts to improve information sharing
- Limited legislation in place that reflects a multijurisdictional approach to information sharing in support of community safety programs

Standards, Policies and Procedures
- Current data systems do not shared information
- Information retention and archiving practices vary across Canada

Information and Data
- Major systems in place but not being optimized (CPIC, PIP, RTID, PRIME, OPTIC etc)
- Limited/no common standards for information and data formats (less than 5% of current data is based on a common standard)
- The full impacts of 700 MHz Broadband/LTE and NG911 are not clear
- There is a risk of information overload for community safety partners (overwhelmed with volume of data and unable to meet public expectations)
- NLEIMS exists but has not been widely adopted or implemented

Technology
- Law enforcement has access to many systems/data sources but still struggles to access and share information
- Vendor solutions are not interoperable (lack of accepted standards)
- Lack of standards compounds procurement of interoperable data systems

January 2015

Canadian Community Safety Information Management Strategy

Strategic Framework

Case for Change

- This an operational requirement that directly impacts our ability to fight crime and contribute to community safety
- Current approach not sustainable (lack of standards, insufficient funding, HR impacts)
- Increased information requirements and sources to manage
- Technology/solution changes pending (Getting NG911 ready)
- Commitment to be more proactive - not waiting for public inquiries to occur
- Growing frustration in sharing information with partners and stakeholders - no standards
- Opportunities with changes anticipated to National Systems over the next few years
- To avoid embarrassment and damaged reputations, police services must adapt to changing information needs
- Span of intelligence information – international and transnational – criminal element is more mobile, no boundaries
- Not able to support organizational goals/Inquiries have supported the need for this information management solution e.g. Campbell report, Pickton, Bernardo.

Strategy – How will we get there?

Governance
- National Entity
- Leadership and Buy-In
- Funding Models

Sharing Culture
- Need and want to share (for the right reasons)
- Collaboration

Legislation
- Multjurisdictional
- Privacy and Security Focuse

Standards, Policies and Procedures
- NIEM
- Quality Assurance

Processes
- Collecting/Receiving
- Sharing/Using
- Archiving
- Training and Exercises

Technology
- Standards based
- Technology Roadmap

Challenges (What will make this difficult?)

- Identifying who or what agency is going to lead the CCSIMS effort
- Approval process for establishing and adoption standards
- Time constraints and the pace of change
- Pace of legislative change

Barriers (What can get in our way?)

- Deeply entrenched legacy of governance and funding models
- Public expectations – perception of our abilities
- Overly narrow interpretation of privacy legislation
- Overcoming ourselves – figuring out solutions to get it done – changing the mindset and culture for information shareing across the public safety community

Future State Vision

Responsible Information Management for Community Safety

Right Information – to the Right People – at the Right Time

Getting the right information to make the right decisions for community safety

Elements of the CCSIM Strategy Vision: Relevant, dynamic, accurate, consumable, complete, unified view, policy supported, legislatively supported, national end to end data flow, single point of governance, standards-based

Future State Outcomes/Capabilities

Governance
- Seamless and effective collaboration with all key partners in the Public Safety/Community Safety portfolio
- National governance model with federal, provincial/territorial and municipal contribution and influence to enable nimble, risk-based decision making
- Value of information/"infonomics" recognized
- CCSIM Strategy is supported by sustainable funding model and viewed as a priority an area for targeted investment
- National stewardship for a standards based and legislation enabled program

Sharing Culture
- Responsible information sharing is enabled by a culture of sharing
- Information is shared in a secure manner and secured appropriately in a seamless environment (system of systems/centres of centres)
- All key stakeholders can access appropriate information from anywhere across the nation

Legislation
- A key element of an overarhcing information management/sharing framework
- Reflects and enables a whole of government and multi-jurisdictional approach
- Community Safety partners recognize sharing ability in privacy legislation

Standards, Policies and Procedures
-Information sharing is guided by common standards, policies and procedures that reflect best practices for information management/use of data, security, privacy and accountability
- Common tools and analytics to optimize available data
- Supports collecting, receiving, sharing, using and archiving data

Information and Data
- Seamless and secure storage of mass data (e.g. NG911, Social Media)
- Adoption of Records Management best practices
- Integrated evidence and records management
- Enhanced operational and situational awareness (smart data)
- Standard BI packages for Law Enforcement

Technology
- Key enabler to the CCSIM strategy (secure, upgradeable, mobile, supported, system of systems)
- Universally accepted standards based
- Supports multiple data formats (text, video, audio, GIS)
- Accessible and useful for all key stakeholders
- Supported, accountable, secure, able to access all the databases
- Able to used multiple formats i.e. video, audio etc. (NG911 ready)

Annex B – Canadian Community Safety Information Management Strategy – Action Plan

Canadian Community Safety Information Management Strategy Action Plan

February 2015

Canadian Community Safety Information Management Strategy
Action Plan
Tasks, Sub-Tasks and Deliverables 2015/2016

The purpose of this Action Plan is to articulate the specific tasks assigned to each action item derived from the Canadian Community Safety Information Management Strategy (CCSIMS) developed during the CCSIMS Working Group held in Ottawa in November 2014. The Action Plan reflects key interoperability initiatives within the public safety community used in the compendium of day-to-day to extreme operations, thereby enhancing the safety of emergency personnel and improved efficacy for the emergency management community.

Each designated task is assigned a coordinator, deliverable(s) and a prospective timeline. Action Items have been developed and designed to support the CCSIMS vision in alignment with the Strategic Objectives laid out in the CCSIMS:

- **Governance.** CCSIMS governance will be representative and reflect a national approach with appropriate Federal, provincial, Territorial and Municipal membership within a "national entity". The CCSIMS governance model will enjoy a high degree of leadership and buy-in. Establishing and maintaining a sustainable funding model for CCSIM Strategy related efforts is also central to the success of the CCSIM Strategy.
- **Sharing Culture**. Community Safety stakeholders and partners will work collaboratively and practices will reflect Responsible Information Management for Community Safety. The sharing culture will be evident in practice and balance the need to share with due regard for operational and legislative constraints.
- **Legislation**. Privacy and related Community Safety related legislation (development, implementation, application and interpretation) supports secure and responsible Information Management for Community Safety.
- **Standards, Policies and Processes.** Data and information related standards, standards-based approaches (e.g. NEIM), and supporting policies and processes contribute to collecting, receiving, sharing, using and archiving data. Training and exercises reinforce established standards, policies and processes.
- **Information and Technology Enablers**. All source information (text, audio, video, GIS, etc.) and the supporting technology enablers (software, applications, systems, networks) are guided by a formal Technology Roadmap that aligns future investments.

This document guides the development of complimentary and supportive action plans for each of the identified action items. This concurrent planning activity will facilitate the coherency of multi-stakeholder efforts in the move the CCSIMS towards the desired interoperability end state. These action items (complete with tasks, deliverables and timelines) will be prioritized/reprioritized annually.

Canadian Community Safety Information Management Strategy - Action Plan 2015/2016

Action Items	Task	Sub-Task	Coordinators	Deliverable	Timeline
Governance					
1.	**G1. Seek FPT approval of the CCSIM Strategy**	**Consult with key stakeholders to include FPT and Municipalities, CACP, CPS, and Unions.**			
2.	**G2. Establish or link into a National Governance Entity with P/T representation**	**Conduct further study on potential models** **Consider a broader/better NPIS and usage of all systems**			
3.	**G3. Engage and inform Privacy Commissioners**	**Engage Privacy Commissioners and key stakeholder at annual conferences and other high profile forums**			
Policies, Procedures and Legislative Framework					
4.	**Pol/Leg1. Leverage previous and planned initiatives to update and expand the current state assessment of legislative capability to share and develop recommendations to enhance IM while respective privacy, etc.**				

Action Items	Task	Sub-Task	Coordinators	Deliverable	Timeline
5.	**Pro1. Identify process to receive* information from the community (Real time and All media)**				
6.	**Pro2. Identify process to provide* information to the community (Real time and All media)**				
7.	**Pro3. Identify standards (FPTM) to exchange information**	**Consider standards for data….** o **Categorization** o **Classification** o **Valuation** o **Storage (physical and life cycle)** o **Access**			
Sharing Environment					
8.	**Share1. Funding e.g. PIP 2.0 or new model**	**Explore funding from PS**			
9.	**Share2. Issue an RFI for a "public safety" cloud**				
10.	**Share3. Conduct and leverage a privacy legislation review to enable sharing (map the "can do" space)**				
11.	**Share4. Define "community/ LE" information sharing requirements. Create the Culture to Share (exception not to)**				

Action Items	Task	Sub-Task	Coordinators	Deliverable	Timeline
Data					
12.	**Data1. Engage and establish leadership from PSC and CACP on the selection and adoption of existing standards**				
13.	**Data2. Adoption of cloud based services that are cost effective and secure**				
14.	**Data3. Acquisition and consumption of data sharing/storage within multi-domains e.g. mental health**				
15.	**Data4. Culture shift from developing solutions to cooperative resource sharing (cherry picking apps that can be easily shared)**				
16.	**Data5. Identify and implement best practices and guidelines for data retention.**				
Technology					
17.	**Tech 1. National Agreement on a set of standardized Data exchanges (also see Task Tech 4)**				

Action Items	Task	Sub-Task	Coordinators	Deliverable	Timeline
18.	**Tech 2. National Agreement for Security and Identity Management (ICAM (Identity Credentials and Access Management) framework**	- **Review status of "Pan Canadian" provincial ICAM framework and progress with Treasury Board's "Canadian Digital Interchange" and "Pan-Canadian Trust-Management Framework" to identify impact on CCSIMS.** - **Review ICAM framework being pursued by U.S. public safety agencies (including for Firstnet).**		**Summary report to advise on strategy for incorporating/applying ICAM standards suitable to CCSIMS requirements.**	
19.	**Tech 3. Explore the consolidation of National Systems – e.g. modernize CPIC, PIP, ACIIS**				
20.	**Tech 4. Review architecture models – NLETS/Message broker/Hub Spoke, and Data-centric NIEM-enabled information exchange framework (IEF OMG open standard)**	- **CSS tech demo on Datacentric, NIEM-enabled Info Exchange Framework Architecture for multi-agency shared information networks.** - **Analysis of datacentric IEF for fit with CCSIMS requirements (provide CCSIMS observer to existing pilots in progress with CBSA and DND)** - **Test plan to pilot and transition IEF solution for a first instance of a national network.**	- **CSS Portfolio Manager (Dr. Dan Charlebois)**	- **Tech Demo** - **Pilot Project Proposal**	**FY 2015/16**
21.	**Tech 5. Develop National Data Warehouse – review models e.g. PIP/ Stats Can/ ICURS/BI**				
22.	**Tech 6. Technology solutions for data input and output – single time data entry as close to source**				

Action Items	Task	Sub-Task	Coordinators	Deliverable	Timeline
23.	**Tech 7. Develop new Public/Private collaboration/partnerships**				
24.	**Tech 8. Explore shared services model in policing (including procurement)**				

Annex C – Canadian Community Safety Information Management Strategy – Key References

- Communications Interoperability Strategy for Canada/ https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-eng.aspx
- Communications Interoperability Action Plan/ https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-ctn-pln/index-eng.aspx
- National Data Quality Standards Strategy (NDQS).
- Law Enforcement Information Data Standards (LEIDS)
- Campbell Report
- Pickering Report