Public Safety Canada | Sécurité publique Canada


# Public Safety Canada

# Public Safety Interoperability Capability Roadmap ROADMAP

## Delivering Responsible Information Sharing through Open Standards and Technology

RDIMS #2621935

# 1 Contents



DRAFT

**Introduction**

This roadmap outlines a near and mid-term approach to develop and deploy information sharing and safeguarding (ISS) capability within and across the Public Safety Portfolio; a key activity for supporting activities that ensure the security of Canada and the safety of Canadians. The described approach is in conformance with the *Security of Canada Information Sharing Act* (SCISA) and related Canadian Legislation. The SCISA affirms the Government's commitment to respecting the rights and privacy of Canadians, and sets out the principles that guide the way the Government intends to facilitate information sharing. It highlights the key elements of a framework that the Government is putting in place to promote effective and responsible information sharing.

# Public Safety Information Sharing

Access to accurate, timely and reliable information is the foundation to any strategy to enhance and extend the governments' ability to deliver national security and public safety. Decision makers at all levels of government must have and maintain a shared situational awareness (hindsight, insight), and the ability to exploit shared Intelligence (foresight) in order to mitigate threats and risks, and the potential impact to Canada and Canadians. Both situational awareness and intelligence are needed to effectively:

- Design effective national security programs,
- Manage and mitigate risk,
- Make quick and sound operational decisions,
- Allocate limited resources, and
- Maintain a day-zero capability.

In today's interconnected and complex world, human and natural threats emerge and evolve rapidly and sometimes unpredictably. The response to any one of these threats often transcends the jurisdiction, capability, and capacity of any single organization, agency, or government. An effective response often requires the combined and coordinated efforts of public, intergovernmental, international, and private-sector partners. This level of collaboration and cooperation cannot be developed at the onset of an incident, it requires: significant planning, advance deployment of services and infrastructure, and training in the use of those services.

As illustrated in Figure 3, the development and maintenance of situational awareness and intelligence necessitates the continuous collection aggregation, analysis, and sharing of broad spectrum of data from multiple sources, e.g.:

- Social Media;
- Media reports;
- Situational Awareness and Intelligence from partners;
- Agency Information systems (e.g., Resource Management System and HR Systems);
- Real-time sensors and Internet of Things (IOT);
- Critical Infrastructure Protection services;
- Big data sources; and
- Other available sources.

The public safety community, as with most public and private organizations, is seeking to exploit Big-Data technologies to collect and process (e.g., aggregate, integrate, stage, mashup, reduce, tag & label, catalogue, cleanse, and enrich) data sets and enable the use advanced (e.g., descriptive, discovery, predictive and prescriptive) analytics that in turn provide situational awareness (hindsight and insight) and intelligence (foresight).

DRAFT

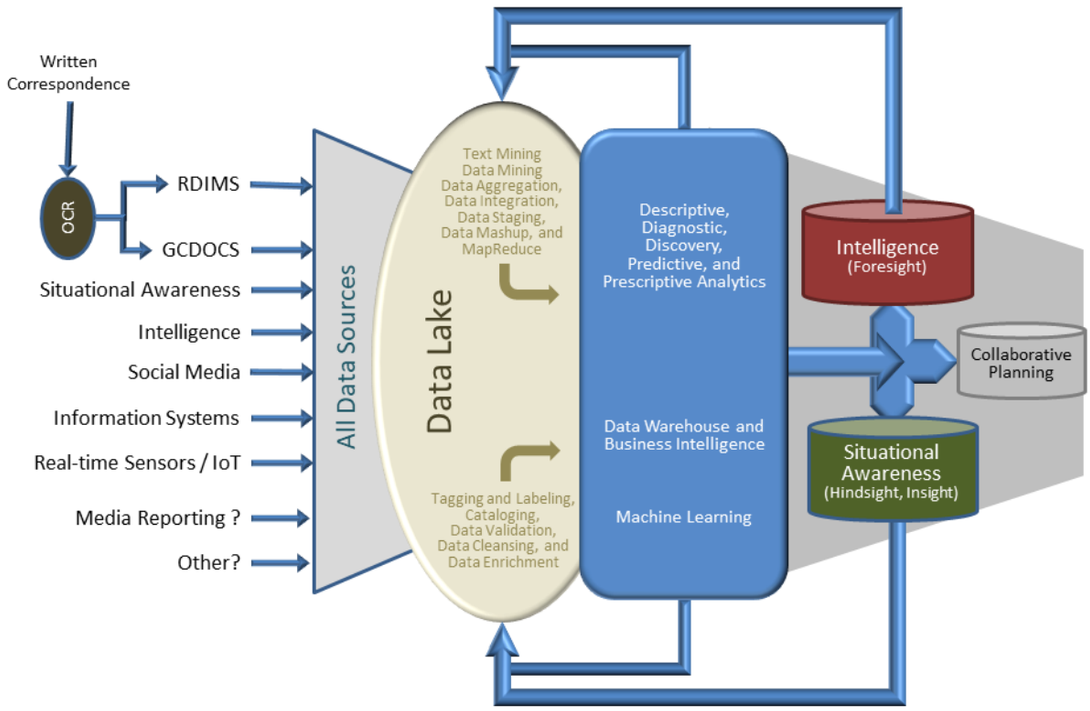


**Figure 1 - Data Gathering and Analysis**

As an agency develops situational awareness, intelligence, and/or a response plan, it is essential to decision makers that they are provisioned with the information they need in a form that enables them to quickly adapt to changes in the operational environment. As data is aggregated and processed, however, its sensitivity often increases; integrating private, confidential, legally-significant, and/or classified elements. This increasing sensitivity of information thwarts efforts to share information, as data stewards (*responsible and accountable for the protection of government*) lack the confidence that the information will not become accessible to unauthorized individuals, organizations or foreign entities.

To overcome this impediment to information sharing, services must be developed that can assess of the sensitivity of data and information elements, as they are aggregated and process and apply the appropriate sensitivity tags and labels. Sensitivity (security) tags and labels are used by traditional information security (access control) services to determine whether or not the requestor or recipient of the information is authorized to access, use, modify, or delete the specified asset. Alternately, the services may redact data from an information element (e.g. personal information) in order to desensitize the information and make it releasable at a lower authorization threshold.

The Treasury Board Secretariat's Digital Exchange Work Group (DXWG) is leading a government-wide push to advance responsible information sharing and maximize the availability of government information, while protecting information that is truly sensitive (if its release would harm an individual, a company, justice, or Canada). The public safety community is responsible for protecting Canada and Canadians. Each threat, risk, or incident to the security of Canada or the safety of Canadians demands a response from different permutations and combinations of partners and resources. This complexity of the public safety operational environment necessitates the development and deployment of an ISS capability that is flexible, adaptable and agile throughout is life-cycle; one that effectively, efficiently, responsibly, and dynamically adapts information-sharing patterns to changes in that environment.

DRAFT

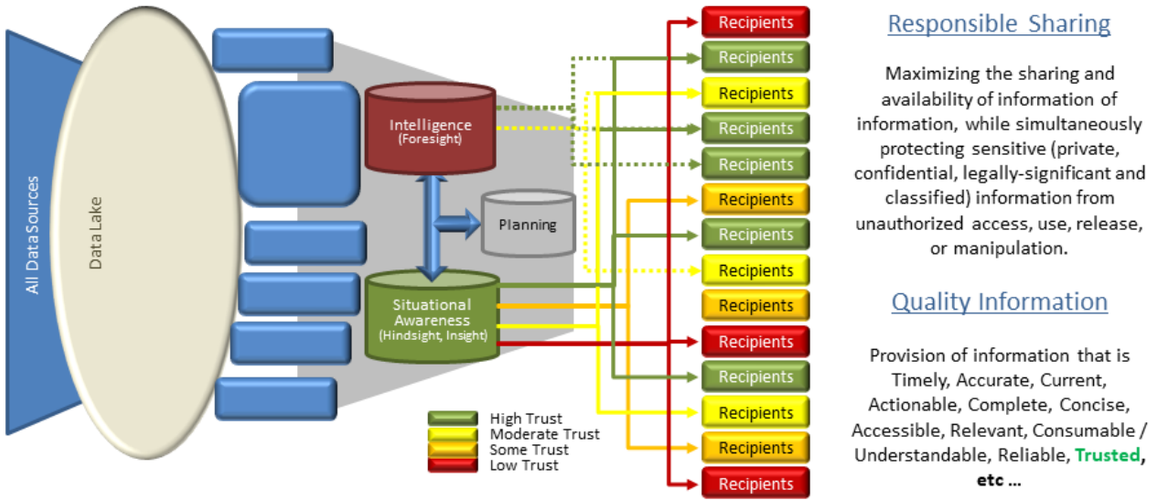


**Figure 2 - Data Sharing and Safeguarding**

This roadmap seeks the community development or adoption of an ISS capability (e.g., strategies, approaches, standards, tools, and technologies) that enable inter- agency ISS; without precluding the use of the same capability for internal agency use. A public safety capability that enables:

- Emergency Management,
- Public Safety,
- Border Security,
- Crisis Management,
- National Intelligence & Security,
- Humanitarian Assistance, and
- Civilian-Military operations.

Across all of these domains, information systems (e.g., data/information, applications, platforms and networks) are both logically and physically separated into security enclaves that isolate and protect sensitive information. This separation also isolates users from the information; making key information elements inaccessible, and ultimately of little or no value to organization and decision makers. There is a high cost to maintaining existing security enclaves and for that reason alone, a number of agencies are seeking to consolidate and integrate their systems and platforms on a single network. These integrated networks will require the ability *to store, process,* and exchange information at different levels of senility (i.e., at different security levels and caveats), and assure that policies are appropriately enforced within and between agencies. This will require greater transparency in the specification, design, implementation and operation of these networks, to assure stakeholders and data stewards that data and information is being handled appropriately. This expanding set of requirements is not unique to public safety (e.g. Privacy other data protection regulation) – but the dynamic nature of the public safety missions and operation and the potential involvement of all levels of government, international and private partners and the public exacerbates the challenge.

# Goals

Overall, this roadmap seeks to address the following public safety goals:

1. Minimize the redundant expenditures on information systems and technologies associated with the call for increased and responsible information sharing.
2. Improve the availability and quality (timeliness, accuracy, relevancy, usability, …, and trustworthiness)of information.
3. Maximize the availability of information to authorized recipients, while simultaneously protecting sensitive information from unauthorized access/release and tampering.
4. Enable the use of all source information to:
    a. Improve decision making,

b. Enable collaborative operational planning, coordination and execution,
c. Acts as a capability (or force) multiplier, and
d. Provides the ability to do more with fewer resources.

5. Provide a rapidly deployable day-zero capability; *"the ability to deploy a basic ISS capability to an unplanned threat, risk or incident at the onset of the event and rapidly adapt the capability to evolving environmental conditions".*

# Principles

The following principles will apply to all activities described in this roadmap, and information sharing for security of Canada and protection of Canadians:

- **Lawful**: All information sharing will be conducted in accordance with and traceable to Canadian law, regulation, and policy, including the Charter and the Privacy Act.
- **Agile**: Enable rapid adaptation throughout the capabilities life-cycle.
- **Effective**: Delivered solutions will enable the sharing of the right information, with the right people at the right time. Solutions will seek to assure the provision of quality information:
  - Timely: provided at a favorable or useful time,
  - Accurate: correct in all details,
  - Current: belonging to the present or relevant time period,
  - Actionable: able to be done or acted on,
  - Complete: having all the necessary or appropriate parts,
  - Concise: brief but comprehensive,
  - Relevant: closely connected or appropriate to what is being done, considered, or decided,
  - Consumable: information that can be used and understood relatively quickly;
  - Understandable: infer the intended meaning,
  - Reliable: consistently good in quality, and
  - Trusted: recipients believe in the reliability, truth, or strength of the information.
- **Defence in Depth**: Deliver security from the networks, to the platforms, to the systems and applications, to the individual information and data elements in the environment.
- **Secure**: Deliver solutions will enable the enforcement of security and privacy policy and the auditability of that enforcement.
- **Responsible**: Delivered solutions will provision of quality information to authorized recipients relative to the context of the operation (e.g., recipient role and responsibility, threat, risk, and severity) assuring that sensitive (private, confidential, legally-significant and classified) information is protected.
- **Accountable**: Delivered solutions will enable departments and agencies that are responsible and accountable for the sharing and safeguarding information to control access to, and release of information and data holdings.
- **Auditable**: Deliver solutions that enable both real-time monitoring and forensic auditing of information sharing and safeguarding transactions.
- **Transparent**: Provided solutions that enable traceability from legislative instruments (e.g., Canadian law, regulation, Policy, and international agreements), through design to operations.
- **Syndicate cost and risk**: A development environment that enables participating agencies to collaborate in the development of community capabilities, and share in advancements in practices, processes, standards, and tools.
- **Exercise and Experimentation**: Establish a program of ISS experimentation and exercises to validate and verify impact and value of capability developments and enhancements.
- **Share knowledge and understanding:** Establish a community based knowledge repository accessible to all community members.
- **Standards based**: Where available, adopt and implement open and international information and technical specifications and standards. Where requisite standards are

DRAFT

not available, work with recognized Standards Development Organizations to develop and issue those standards.

- **Share and Reuse**: Wherever possible, share capabilities with community members and other communities. Wherever possible, adopt and reuse the capabilities developed by other community members or communities – and augment, advance, or enhance those capabilities, then share the resulting capability.

## Keys to every effective solution

The following items identify key characteristics for Information Management and Technology (IM/IT) solutions for the delivery of Information Sharing and Safeguarding capability within the public safety community.

- **Open**: public safety ISS architectures, solutions and supporting artifacts are available to all community members.
- **Open Standards (Community Accepted Specifications)**: Exploit the knowledge of international SMEs not typically available to project developing requirements. Using the standards reduces cost and risk, while increasing innovation and availability. Conforming products and services are available from multiple sources. Standards define open public Interfaces and specifications that are available to integrators and users.
- **Separate Concerns**: Separate the business (/ISS Policies) rules and constraints from the technical services charged to enforce them enables the implementation of infrastructure that can be tailor to operate as needed – policies can be activated, deactivated, augmented, or removed as needed - the services and more portable, scalable, flexible, adaptive and agile.
- **Responsible, Trusted and Auditable**: Fully transparent from design through operations – All elements are modeled and traceable to business requirements (e.g., legislation, regulation, Information Assurance Policy). In order for stakeholders to certify and accredit the solutions for operation they need to trust that information is only access and shared in accordance with their legislative and policy mandates. Solutions must demonstrate that they conformation through real-time monitoring and support for forensic auditing.
- These same capabilities can also be used to assure citizens and Parliament that information is being handled appropriately, by enabling audits by independent officers of Parliament including the Office of the Privacy Commissioner and the Office of the Auditor General. The auditing capabilities can also be extended to independent, external review of the activities of the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and the Communications Security Establishment.
- **Policy Driven**: Operations are traceable to policy instruments, including:
    - Legislation,
    - International Agreements,
    - Regulation,
    - Government directives,
    - Operational Policy (e.g., Information Management, Information Sharing Agreements, Memorandum of Understanding, Security, Privacy, etc.),
    - Memorandum of Understanding, and
    - Service Level Agreements.
- **Architecture Enabled**: Institutional memory captured as part of standard architectures and sharable amongst community members. Architecture metadata can be used for specification, design, implementation and operational analysis to mitigate risk and generate specifications for enhance governance and capability.
- **Augment – do not Replace**: Solution does not require the replacement of a users' installed capability and infrastructure. Components work as plugins or independent add-ons to an existing element in the users' environment. Few organizations have resource to replace existing operational systems in order to augment ISS capability.

- **Agile Specification, Design and Development**: Enable the evolution of ISS ability – Iterative, evolutionary, agile development of policy models that can be exercised as built - mitigates the risks associated with complex, poorly defined and dynamic information sharing and safeguarding requirements. Experiment and test early and often to assure faults are identified early and corrected at the lowest possible cost: discard strategies, approaches, and technologies that do not serve the community's requirements.
- **Data-centric**: Rules and constraints directly to the data content – machine speed enforcement of rules as data and information elements are aggregated, transformed, marked and redacted. Tailor dataset to elements that are authorised for release and conform to recipient authorizations. This focusses the develop of sharing and safeguarding development on the asset, versus the infrastructure needed to share and safeguard that asset.
- **Adaptive Operations:** Systems that that rapidly modify operation to accommodate changes in the operational environment, e.g.:
    - Threat Level,
    - Risk Level,
    - Impact Level,
    - Participant roles & responsibilities,
    - Participant location,
    - Community of Interest membership,
    - Incident, scale, scope and severity,
    - Available Communications, and
    - Quality of Service.

# 2 Overview of the roadmap

## Public Safety (PS) Role and Responsibilities

Public Safety is committed to the development of broad-based interoperability (information sharing and safeguarding capabilities), and the promotion of effective and responsible information sharing within Public Safety and throughout the public safety community. Public Safety's role in this effort is to work with central agencies (e.g., TBS, and PCO), intergovernmental and international partners, and the private sector to develop and sustain broad-based ISS capability. The PS role and responsibilities include:

- **Clear and Balanced Policies**: Work with TBS and the PCO to develop a policy framework that enables effective and responsible information sharing that balances the requirement for government agencies to protect Canadians with that of respecting individual rights and freedoms.
- **Open Standards**: Work with the community and TBS to identify and adopt open practice, process and technical standards that will guide the development and deployment of ISS capability. (e.g., National Information Exchange Model [NIEM]); PS will also engage with Standard development organizations to assure the appropriate levels of governance are applied and that all willing parties have the opportunity to contribute to the development of the standards.
- **Syndicating Cost and Risk**: Work with public safety community, the GC, and intergovernmental and international partners to identify open development and deployment opportunities for ISS solutions that can be adopted and sustained by all community members.
- **Coordination and leadership**: Promote effective and responsible information sharing within the public safety community and Government of Canada. This will include, for example, Public Safety Canada leading the development guidance, and information session that will aid officials understand and administer the SCISA.
- **Shared capabilities**: Promote the community ecosystem that that enables collaborative development, deployment, and sustainment of ISS practices, processes, standards, capabilities and technologies.

DRAFT

- **Training and Support**: Promote continuous training and education (e.g., workshops and information sessions) to increase community awareness and understanding of evolving legal/regulatory frameworks, operational needs, standards, and capabilities that enable responsible information sharing.

# Roadmap Elements

As a starting point, Public Safety is offering the following as core element in the development of a broad based ISS capability for the community.

## Identifying Communities of Practice

Public safety and security covers a wide range of activities that if address as a single domain world prove to be insurmountable. It is recommended that the community self-divide into communities to identify the ISS needs, challenges and solutions. As many of the members span multiple communities, we would look these organizations to seek common strategies, approaches, standards and solutions to the broader public safety community. Communities may include:

1. Emergency Management and Response,
2. Crisis Response Management,
3. National Security,
4. Border Security,
5. Maritime Security,
6. Cyber Security,
7. Critical Infrastructure Protection,
8. Other

Activities for each of the communities may include:

1. **Describe Public Safety Community of Interest/Practice**: Prepare a brief description of the roles, responsibilities and ISS needs for the COP.
2. **Describe Community Use Cases**: Develop use cases for the sharing of information between community-partners, and identify gaps in the community's ability to exercise each use case.
3. **Set Community Requirements**: Capture the business/operational information sharing and safeguarding requirements derived from the described use cases.
4. **Identify common gaps and overlaps with other COPs:** Review the information being developed by other COPs and uncover common requirements or areas where the COPs may collaborate in the development of the underlying capability.
5. **Identify intergovernmental and international partners**: identify and engage non-GC partners in the identification and development of ISS strategies, frameworks, standards and solutions. This further syndicates effort; reducing individual agency risk and cost.
6. **Identify Safeguarding Constraints:** Review legislative, regulatory and policy requirements to safeguard sensitive (private, confidential, legally-significant and classified) information. Also identify the requirements for monitoring and auditing that sensitive information is being managed, handled, stored and shared in accordance with defined authorities and responsibilities.
7. **Identify common/share requirements**: Identify common or shared requirements within the COP of with other COPs, and determine whether or not the requirements might be satisfied through the development of another community member or community. Seek opportunities to test existing capabilities and a method to reduce risk and cost.
8. **Set Community Priorities**: Set the priority for the development of individual capabilities.

## Develop COP Capabilities / Solutions

DRAFT

Engage with community members in an open development and testing of potential strategies, frameworks, standards and solutions. Use an adaptive and agile approach the developing, testing and deploying ISS capability.

1. **Manage Business/Operational Backlogs**: Actively manage and publish a prioritized backlog of capabilities and capability enhancements needed by the COP.
2. **Investigate current capabilities**: Seek opportunities to adopt and enhance existing community capabilities, services and systems.
3. **Develop Capability**: Develop, test and deploy each of the capabilities in the backlog.
4. **Manage Experimentation and Exercises**: Actively manage and publish a prioritized list of exercises and experiments to validate and verify the developed capabilities or enhancements. Negotiate participation of COP and other partners.
5. **Test (Experiment / Exercise)**: Execute the planned tests, experiments and exercise with participating members to validate and verify that capability development and enhancements are contributing to community information haring and safeguarding capability.
6. **Integrate Capability**: Integrate the developed capabilities into community members' operational environments.
7. **Share Capabilities and Knowledge**: Publish the results of the capability development, experiments and exercises to the GC or public domain, as appropriate and authorized.
8. **Govern the Solutions**: As the delivered solution will be open to a broad-based set of users, changes to the solution must be managed effectively to assure quality, reliability, and security are maintained through its life-cycle.

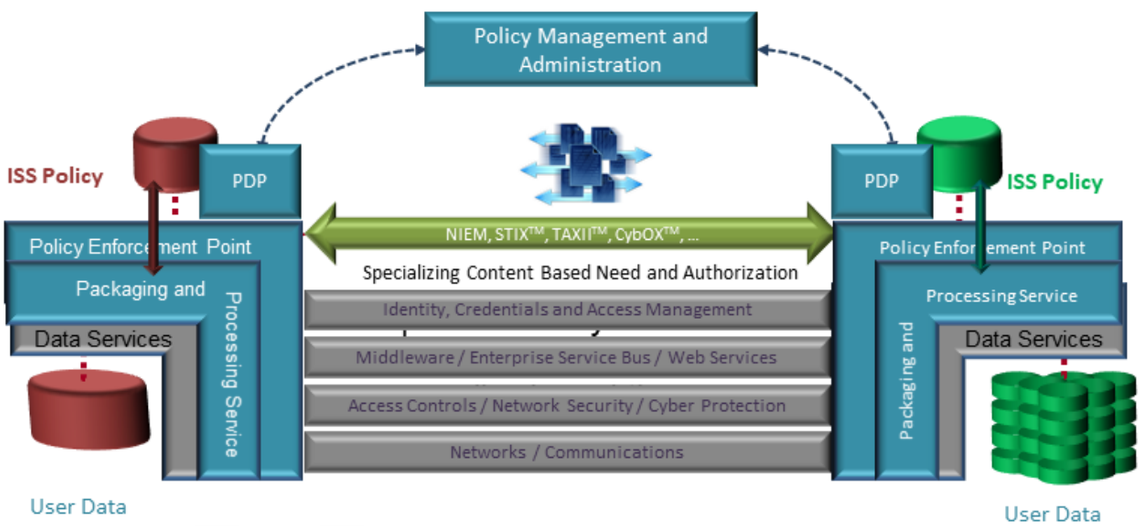


**Figure 3 - ISS Infrastructure**

## Share Capabilities

Work with TBS and the PCO to establish the legislative and policy framework needed to enable responsible information sharing

a) **Shared Support Ecosystem**: In order to promote collaborative and shared development of capability the community will need a common strategy, practices, standards and tools to enable the communities sharing of ideas and capabilities. PS will lead and coordinate efforts to evolve and promote common strategies, frameworks, practices, standards, and tools.

b) **Information Sharing and safeguarding Framework**: PS will work with community members to identify the best practices, standards, and tools that will enable and enable and agile development of capabilities and promote the sharing and reuse of those developments.

c) **Governance**: PS work with TBS to lead efforts to integrate information sharing and safeguarding governance into existing GC governance practices and structures.

d) **ISS Capability Continuum**: PS will revive efforts to develop the Information Interoperability (Information Sharing and Safeguarding) continuum and capability maturity model for the community. These elements will enable community members assess their ability to interoperate with public safety partners. Figure 6 represents the 2010 PS effort to extent the DHS SafeCom Continuum for the communications into the ISS domain.

e) **Data Classification (Metadata Standards)**: A common classification scheme (metadata semantics) is an essential component of ICM and trust frameworks. PS will lead a community effort to develop a classifications scheme and, if practical, promote the scheme to an open standard that could be specified in systems specifications and open RFPs. As a standard, the classification scheme could be adopted by intergovernmental, international and private sector partners, further extending and improving information sharing and safeguarding capabilities.

f) **Federated ICAM and Trust Framework**: Effective ICAM and Trust components underpin all ISS services. PS work with the central agencies (TBS, PSC and SSC) to develop community ICAM and Trust framework capabilities. PS will lead community effort to establish ICAM and Trust capabilities for PS operations.

g) **Common ISS Infrastructure and Service**: PS will work with the central agencies and community members to implement ad deploy the interagency infrastructures and services (Figure 5) needed establish to deploy and sustain operational ISS capabilities. This includes working with community members to identify the standards and technologies enable flexible, adaptable and agile ISS capabilities, and enable the integration of members' existing capabilities.

h) **Common Test and Experimentation Services**: The ability of member organizations to test, experiment and exercise ISS new capabilities is essential to ensuring that they will be effective under mission or operational conditions. PS will work with community members to develop and deploy ISS testbeds and core infrastructure that enable community members to test new capabilities and local implementations. These services will also enable desktop and other exercises planned by PS or the community.

### Sustain Capabilities

Public Safety will work with community members to develop a strategy for sustaining developed capability over its life-cycle and assuring that these capabilities are available to community members.

### Govern Capabilities

Public Safety will work with community members to develop a strategy for maintaining the quality of shared capabilities, and that changes do not have a detrimental impact to operational capability.

## The Roadmap Developments Process

Although Public Safety is publishing a draft roadmap to the community, is con considering it a definitive document. The document is being published as a sample of things that may be required by the community in it journey to develop a broad-based, community wide Information Sharing and Safeguarding Capability. It is intended to engage the community in discussions that will:

1. Define tasks and activities that need to be completed;
2. Define the needs//requirements to be addressed;
3. Prioritizes the tasks and activities;
4. Identify community members willing to invest in the completion of the tasks; and
5. Schedule the completion of the desired outcome / output.

DRAFT

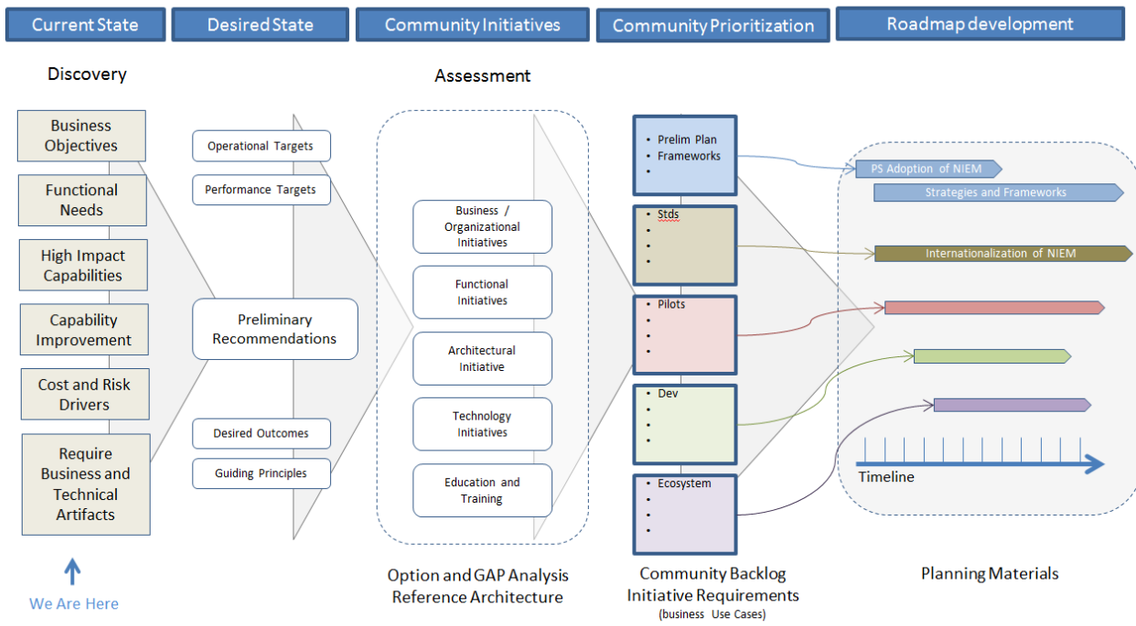


**Figure 4 - Road Map Development Process**

Beyond Public Safety's desire to standardize on NIEM and the foundation for public safety information sharing and efforts around enabling this adoption, and effort that has been on the books since 2012, there rest of the roadmap material is for discussion only.

# 3 ISS Strategies, Frameworks and Continuum

The following identify potential strategies and frameworks that may be used to architect, design and implement a cost effective and sustainable ISS capability for the community. It is anticipated that these and other suggested elements will be combined to define a strategy, framework and continuum that the community can endorse and use.

## Strategies

Public Safety is seeking community strategies (e.g., CBSA, RCMP, PS and intergovernmental and international partners) to deliver interoperability or information sharing and safeguarding in the public safety or public safety domains – as the foundation for an overarching ISS strategy. PS will work with willing partners to blend the best ideas and practices and issue a strategy document.

## Frameworks

Public Safety is aware of a number of frameworks that combine to define a rich and mature approach to the specification, design and

- ESMIF: The EMSIF was a Public Safety / Centre for Security Sciences effort to develop and framework under which the Public Safety and Emergency Management communities could develop, deploy and sustain information sharing and safeguarding capabilities. The framework was intended to assist the community:
    - Improving information quality during the planning, response and recovery from an emergency or public security incident; and enhance decision making.
    - Enhancing Government(s) of Canada's ability to effectively plan, execute and monitor the operational situation and coordinate support for the accomplishment of operational objectives while adapting to changing situations.
    - Leverage community developed capabilities:
        - Incident management,
        - Resource Management,
        - Off-the-shelf and open-source solutions (e.g., Multi-Agency Situational Awareness System (MASAS)),
        - Open-standards and publically accepted specifications (e.g., IEF, CAP, and NIEM),

    - Allow agencies to evolve capability based on mandates and priorities; aligned to a shared vision of interoperability, and
    - Integrate lessons-learned into the EMSI development portfolios of the participating agencies.
- I2F: The Information Interoperability Framework ($I_2F$) is used to guide the implementation of the ISE information sharing capabilities. The ISE approach links information across jurisdictional boundaries and creates a distributed, protected, trusted environment for sharing information. It provides mechanisms to permit partner agencies at the Federal, state, local, tribal, and territorial levels (e.g., fusion centers) to share similar data based on common standards and practices. The ISE $I_2F$ exploits existing information architectures, suggesting standards, tools and methodologies to link existing systems as well as specifying the development of common artifacts that will enable disparate departments and agencies' architectures to make the full framework operational.
- The ISE $I_2F$ was developed so that ISE participants could better respond to complex policy challenges and improve the delivery of services and information to protect our citizens. To achieve a connected government, ISE participants require guidance to confidently manage, transfer, and exchange information by:
    - identifying key decision points for interoperability between disparate systems,
    - providing a comprehensive, high-level description of each interoperability domain, and
    - establishing the framework for implementing ISE information sharing capabilities.
- IEF: Defines an integration pattern (reference Architecture) for delivering Policy-driven Data-centric Information sharing and safeguarding. The IEF focusses on providing defence-in-depth based on data content rather than the tradition application, platform and network forms of information security.
- NIEM: Defines a process and tools for developing and documenting community information sharing agreements.
- TOGAF: An Open Group Standard that provides:
    - A proven enterprise architecture methodology and framework used by the world's leading organizations to improve business efficiency.
    - A prominent (adopted by the GC) enterprise architecture standard, ensuring consistent standards, methods, and communication among enterprise architecture professionals
    - The ability to avoid being locked into proprietary methods, utilize resources more efficiently and effectively, and realize a greater return on investment
- UAF: A generic and commercially orientated architecture framework (ontology and domain model) that defines ways of representing an enterprise architecture and enable stakeholders to focus on specific areas of interest in the enterprise while retaining sight of the big picture. UAF addresses specific business, operational and systems-of-systems integration needs of private, public, and military, sector enterprises. The UAF standard is based on the Object Management Group® (OMG®) Unified Modeling Language™ (UML®) 2.0 and the Systems Modeling Language™ (SysML®) standards but also aligns to a wide array of UML profiles (extensions) including BPMN, IEPPV, NIEM, TOGAF/Archimate. UAF architecture models provide a means to develop an understanding of the complex relationships that exist between organizations, systems, and systems-of-systems and enable the analysis of these systems to ensure that they meet the expectations of the stakeholder community.

These frameworks serve different functions, but complement each other well. Public Safety is seeking to adopt these and other framework elements (proposed by the community) to guide for the development of ISS capability.

# Proposed ISS Continuum

The public Safety Information Interoperability (or Information Sharing and Safeguarding) continuum, Figure 9, was developed under the Public Security Technical Program in 2009-2010; Emergency Management System Interoperability Framework. It sought to extend the Homeland Security SAFCOM continuum into the ISS domain. Public Safety recommends that the community

use this effort as the starting point for the development a continuum that could be used by an individual agency to assess is ISS capabilities in a clear and consistent manner.

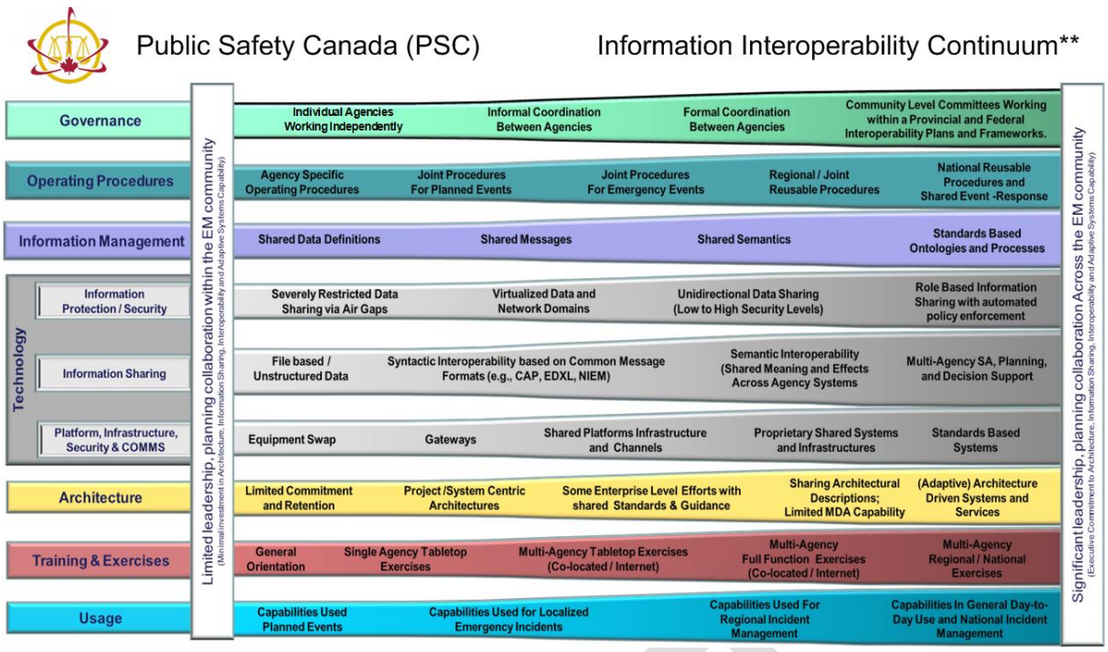


**Figure 5 - Information Sharing and Safeguarding Continuum**

Community members will be able to use the continuum to monitor and track the progress toward an ISS capability.

# Open Standards

The standards used by the public safety community will be identified and adopted by the community and if applicable, promoted to the GC for adoption. Public Safety will establish and standards management capability with full participation of community members.

DRAFT

# 4 Annex 1 – Preliminary Roadmap Tasks

This Annex proposes an initial set of tasks and activities for the public safety ISS effort. Beyond the championing the adoption of NIEM as a public safety standard and the Internationalization of NIEM (Public Safety initiated and led), the rest of the potential tasks and activities are offered as suggestions to initiate discussion and identify lead agencies).

## TASK 0: Planning

- Roadmap
- Strategy
- Frameworks
- ISS Continuum

## Task 1: Collaboration and Shared Capability

As part of this effort Public Safety will lead efforts to establish the following elements community efforts:

- **Support Ecosystems**: Collaborative, sharing and open development by their very nature require information sharing and safeguarding (interoperability) and collaboration to operate effectively. As part of this effort PS will work with community members to:
    - Develop strategies, practices and technology recommendations to community members that will enable collective/community action.
    - Identify and adopt information and technology standards that will underpin the development of community ISS services.
    - Identify and develop open products and services that will be freely available to all community members;
    - Identify how support services will be made available for community members.
    - To identify a lead agency to develop and maintain key community capabilities.
    - Work with Standards Development Organisations (SDO) to ensure GC PS requirements are in the ISS standards.
    - Work with inter-governmental, international and private sector partners to evolve an ecosystem that provides ISS capability that can be scaled to each member's needs and requirements.
- **Governance**: Work with community members to safeguard changes in standards and infrastructure do not detrimentally impact on PS community capability, and these changes progress through GC governance as necessary.
- **Testbeds**:

DRAFT

- **Experimentation and Exercises**:
- **Collaboration and Information Sharing sites**: See Knowledge Sharing.

## Activity 1-1: Roadmap Planning (July 2017 – March 2018)

PS will prepare and deliver a short and mid-term roadmap (this document) of activities for the development and deployment of community ISS Capabilities.

## Activity 1-2: Capability Development

## Activity 1-2-1: Open Development Sites

Develop and maintain open community pages development sites on technologies such as PS GitHub, GC Github, Public GitHub. Appropriate Quality, Security and governance controls over changes to the applications under development must be maintained by the community.

## Activity 1-2-2: Basic Situational Awareness Open Source Service

It has been suggested that the TIES capability be extended and provisioned as an open-source Situational Awareness application that can be downloaded and used by all governments (federal, provincial and municipal) departments and agencies. This service will gradually add services, as developed by the community to a common infrastructure based on the OMG[1] Information Exchange Framework (IEF) open standards and Reference Architecture[2].

## Activity 1-2-3: Public Safety Application Store

## Activity 1-2-4: Open Policy Store

IEPD, XSD, Policy Model, Data Model for data standards adopted by a community.

## Activity 1-3- : PS Community ISS Ecosystem

## Activity 1-3-1 - PS Information ISS Framework and Continuum

[1] Object Management Group (www.omg.org)
[2] IEF Reference Architecture

DRAFT

PS will revive effort to define its Information Sharing and Safeguarding Continuum and capability maturity model for the community. The original continuum was developed as part of a 2009 as part of a Canadian Safety and Security Program (CSSP). It was derived from the SAFECOM Interoperability Continuum[3], and added the elements needed to develop, execute and sustain information sharing and safeguarding capabilities:

- Information Management;
- Information Safeguarding; and
- Architecture.

The proposed update will add enhancement for:

- Trust Framework;
- Policy management and automation;
- Enhanced traceability, monitoring and auditing;
- Enhancement to capability and maturity definitions; and
- Integration of strategy, architecture and technology advancement sing 2009.

These elements will enable community members assess their ability to interoperate with public safety partners.

### Activity 1-3-2 : Community Test, Experimentation and Exercises

### Activity 1-4- : Science and Technology

- GC S&T Community
- Academia

## Task 2: Knowledge Sharing

[3] https://www.dhs.gov/sites/default/files/publications/Operational%20Guide%20for%20the%20Interoperability%20Continuum_0.pdf

DRAFT

As part of this effort Public Safety will lead community efforts to establish ISS information sharing for elements such as:

- Practices, processes, and tools;
- Specifications and standards;
- Architecture models and information;
- Profiles and guidance documents on the application of standards legislation, policy, and regulations;
- Open-source and open-use software; and
- Training and Exercise Materials.

Public Safety Seeks to maximize the discovery and availability of this information while protecting those elements that if disclosed would detrimentally impact on public safety and security. PS with community members to selects the forum and technologies used to share information with community members (e.g.: GC, intergovernmental, international and private secure). The following table identifies and briefly describes the core elements of the PS Knowledge base.

DRAFT

| Knowledge base Element | | Description |
|---|---|---|
| **Governance** | | Community defined practices, procedures, technologies used to assess and certify proposed standards and technologies. |
| **Guidance Materials** | Best Practices, Processes and Tools | Community adopted practices, processes and tools that support the specification, development/acquisition, deployment and operation of interoperable PS capabilities, systems and services. |
| | Standards | A catalogue / repository of standards, specifications, best practices, etc… that have been adopted by the community. The repository will also contain profiles, developed by community members, identifying how various standards a tailored, or integrated to deliver a capability. |
| | Profiles and Guidance | A catalogue / repository of community adopted profiles and guidance documents that describe how to apply elements of legislation, policy and standards in the specification, development, deployment and operation of interoperable PS capabilities, systems and services. |
| | Architecture Models | Community and stakeholder developed and published architecture models and supporting information describing ISS capabilities, deployments and configurations. These model would be made availability for analysis and use by targeted groups to guide the development of interoperability capability.<br>Models may include: capability models, deployment models, ISS policy models, information models etc … |
| | Training and Exercise Materials | Community adopted practices, processes, guidance and datasets that enable the community to evolve its capacity to train and exercise at the local, regional and national levels. |
| | ISS Continuum | Community dashboard that illustrates progress along a continuum of capability. The continuum seeks to present capability in a manner that:<br>• Illustrates the state of ISS capability to stakeholder, decision makers and planners.<br>• Fosters a common understanding and collaboration across disciplines.<br>• Fosters commitment to resource allocations from policy |

DRAFT

| Knowledge base Element | | Description |
|---|---|---|
| | | makers, stakeholders, planners.<br>• Promotes the regular use ISS solutions and capabilities.<br>• Enables planning and budgeting for ongoing enhancements to systems, procedures, and documentation.<br>• Aligns elements across Interoperability Continuum elements. |
| | ISS Framework | • <br>• <br>• <br>• <br>• |
| Support Services | | • |
| | | |
| | Support Infrastructure | Community supported capabilities that bridge the member processes, systems and services to common or shared infrastructure and data.<br>Architectures, designs, technologies and configurations that will enable a community member to interoperate with PS ISS capabilities |
| | Capability Metrics | A set of self-performance assessment metrics (against architectural elements) that enables an assessment of progress along the elements of the interoperability continuum. |
| | | |

DRAFT

| Knowledge base Element | Description |
|---|---|
| Testbeds | |
| Shared Software | |

### 1.1.1 Information Sessions and Workshops

Develop and deliver a series of information sessions and workshops to engage the community in developing and delivering the vision, strategy, standards and capabilities needed to deliver responsible information sharing within and between public safety community members.

## Activity 2-2 Web-site and Wiki

Develop and Maintain community pages on websites open to all PS community members such as GCconnex, GCpedia and GCcollab.

## Activity 2-3 – GIT site

## Activity 2-4: ISS Information Session and Workshops

As part of the roadmap PS will identify a series of information sessions and work shop that target community building and the sharing of strategies, architectures, designs and implementations of ISS capabilities by each of community members. PS will develop and deliver session that focus on exposing GC information and capabilities, as well as bringing in international and intergovernmental organizations and Subject matter experts to bring the latest innovations to local resources. For interoperability to evolve, all the partners must mature their abilities to consume partner messages and appropriately handle, store and share that information. These sessions include:

1. January 30-31, 2018 – PS Information Sharing and Safeguarding Symposium
2. September 24-28, 2018 – Object Management Group Technical Meeting.
3. Other …

DRAFT

# Task 3: Adopt and Deploy Community Standards

## Activity 3-1: Standards management

## Activity 3-2: Inter-agency Data Exchange Standards

The National Information Exchange Model (NIEM) has been identified as one of the candidate ISS models that could be adopted and rapidly advance ISS within the PS community. NIEM provides a collection of message specifications and tools that could be adopted and used by the community. NIEM provide data exchange specifications (IEPDs). NIEM enables information sharing across a growing number of domains, including:

1. Agriculture;
2. Maritime;
3. Human Services;
4. Immigration;
5. Personal Screening;
6. Infrastructure Protection;
7. Chemical, Biological, Radiological, and Nuclear (CBRN);
8. Emergency Management;
9. Intelligence;
10. Justice;
11. Biometrics;
12. International Trade;
13. Surface Transpiration;
14. Military;
15. Evolving; and
16. Cyber.

Because of this coverage, NIEM become a prime candidate for adoption. Adoption of NIEM will follow the following stages:

DRAFT

- Stage 1 – Have TBS declare NIEM as an Information Sharing Standard for the PS community. This will require the submission of NIEM to the TBS governance bodies for endorsement and adoption. PS to work with TBS to develop guidance and support for agencies seeking to adopt and use NIEM IEPDs.
- Stage 2 - Multilingual Version of NIEM. NIEM is a unilingual implementation – this is a known GAP. As a minimum the GC requires a bilingual capability. The selected approach should be capable of supporting multiple languages to promote international adoption and address the needs of a broader range of PS international partners. PS has initiate discussions with the NIEM governance bodies to undertake this internationalization effort.
- Stage 3 - Develop open GC NIEM infrastructure: in order for broad based adoption of NIEM within the public safety community there need to be a GC open source solution to the sharing and safeguarding of information using community selected Information Exchange Package Documentation (IEPD[4]) sets. This development should provide the core for a universal sharing capability for NIEM (/XML / JSON) message types.
    - Stage 3a - XML Support: XML is the standards exchange protocol for NIEM – Initial development will focus on a XML based capability.
    - Stage 3b - JSON Support: NIEM is seeking to provide JSON support – Extend the XML capability to JSON.
- Stage 4 - Operationalizing NIEM
    - Stage 4a - Moving from TDP:
    - Stage 4b – Operational Pilots:
    - Stage 4c – Production:
    - Stage 4d – Sustainment and Enhancement:
    - Stage 4e - TBS Messaging Fabric:
- Stage 5: Support Infrastructure

## Activity 3-2.1: PS Adoption of NIEM

## Activity 3-2-1: Internationalization of NIEM

PS plans to lead efforts to Internationalized the National Information Exchange Model (NIEM) and facilitate its adoption across the public safety community. This effort includes:

1. Enable real-time exchange and translation of French and English messages;

[4] IEPD includes a NIEM Message design materials.

DRAFT

2. Translation of normative NIEM documentation into French;
3. Develop the infrastructure needed for the real-time and translation of message;
4. Demonstrate the capability;
5. Provide a community sharable service.

## Activity 3-2: Inter-agency Technology Standards

DRAFT

# 5 Annex 2 - Glossary

## TERMS

This glossary is provided for reference purposes and is not intended to modify existing definitions

| | |
|---|---|
| **All-Hazards** | Emergency management adopts an all-hazards approach in every jurisdiction in Canada by addressing vulnerabilities exposed by both natural and human-induced hazards and disasters. The all-hazards approach increases efficiency by recognizing and integrating common emergency management elements across all hazard types, and then supplementing these common elements with hazard specific sub-components to fill gaps only as required. As such, “All-Hazards” does not literally mean preparing to address any and all potential hazards in existence. Rather, it emphasizes the leveraging of synergies common across hazards and maintaining a streamlined and robust emergency management system. The “All-Hazards” approach also improves the ability of emergency management activities to address unknown hazards or risks. |
| **Critical Infrastructure** | Refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. |
| **Disaster** | Essentially a social phenomenon that results when a hazard intersects with a vulnerable community in a way that exceeds or overwhelms the community's ability to cope and may cause serious harm to the safety, health, welfare, property or environment of people; may be triggered by a naturally occurring phenomenon which has its origins within the geophysical or biological environment or by human action or error, whether malicious or unintentional, including technological failures, accidents and terrorist acts. |
| **Disaster Risk Reduction** | The concept and practice of reducing disaster risks through systematic efforts to analyze and manage the causal factors of disasters, including through the mitigation and prevention of exposure to hazards, decreasing vulnerability of individuals and society, strategic management of land and the environment, improved preparedness for disaster risks, coordinated response and planning and forward looking recovery measures. |
| **Emergency** | A present or imminent event that requires prompt coordination of actions concerning persons or property to protect the health, safety or welfare of people, or to limit damage to property or the environment. |

DRAFT

| | |
|---|---|
| **Emergency Management** | The management of emergencies concerning all-hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery. |
| **Environmental Change** | A disaster risk reduction concept that includes consideration for both the hazard of global climate change, as well as community vulnerabilities and resilient capacities. Unsustainable alterations to the physical environment and human interactions with it, may create or exacerbate risks that exist with or without climate change. As such, sustainable adaptation must be considered both within context of climate change and the broader hazardscape. |
| **Hazard** | A potentially damaging physical event, phenomenon or human activity that may cause the loss of life or injury, property damage, social and economic disruption or environmental degradation. |
| **Hazardscape** | The cumulative emergency management environment, composed of all hazards, risks, vulnerabilities and capacities present in a given area. |
| **Mutual Assistance Agreement** | A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement. |
| **Partner** | Any individual, group, or organization that might be affected by, or perceive itself to be affected by an emergency. |
| **Prevention** | Actions taken to avoid the occurrence of negative consequences associated with a given threat; prevention activities may be included as part of mitigation. |
| **Prevention/Mitigation** | Actions taken to eliminate or reduce the impact of disasters in order to protect lives, property, the environment, and reduce economic disruption. Prevention/mitigation includes structural mitigative measures (e.g. construction of floodways and dykes) and non-structural mitigation measures (e.g. building codes, land-use planning, and insurance incentives). Prevention and mitigation may be considered independently or one may include the other. |
| **Resilience** | Resilience is the capacity of a system, community or society exposed to hazards to adapt to disturbances resulting from hazards by persevering, recuperating or changing to reach and maintain an acceptable level of functioning. Resilient capacity is built through a process of empowering citizens, responders, organizations, communities, governments, systems and society to share the responsibility to keep hazards from becoming disasters. |
| **Resistance** | The ability to resist or withstand impacts so that inevitable damage from an extreme event does not reach 'disastrous' proportions. |

DRAFT

| | |
|---|---|
| **Risk** | The combination of the likelihood and the consequence of a specified hazard being realized; refers to the vulnerability, proximity or exposure to hazards, which affects the likelihood of adverse impact. |
| **Risk-based** | The concept that sound emergency management decision-making will be based on an understanding and evaluation of hazards, risks and vulnerabilities. |
| **Risk Management** | The use of policies, practices and resources to analyze, assess and control risks to health, safety, environment and the economy. |
| **Sustainable** | A sustainable approach is one that meets the needs of the present without compromising the ability of future generations to meet their own needs. |
| **Threat** | The presence of a hazard and an exposure pathway; threats may be natural or human-induced, either accidental or intentional. |
| **Vulnerability** | The conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards. It is a measure of how well prepared and equipped a community is to minimize the impact of or cope with hazards. |

## Acronyms

| | |
|---|---|
| EM | Emergency Management |
| EMSIF | Emergency Management System Interoperability Framework |
| IEF | Information Exchange Framework |
| I2F | Information Interoperability Framework |

DRAFT

| | |
|---|---|
| ISE | Information Sharing Environment |
| ISS | Information Sharing and Safeguarding |
| NIEM | National Information Exchange Model |
| PS | Public Safety Canada (the department) |

# 6 Annex 3: Data Standards

The following table identifies public safety developed/adopted open data, metadata and messaging standards.

Table *1* – Communities of Practice

| Community of Interest/practice | Brief Description | Applicable Data Standards | Agencies Using this Standard |
|---|---|---|---|
| **Emergency Management** | | NIEM IEPD-x | |
| | | EDXL | |
| | | HL7 | |
| **Crisis Response Management** | | NIEM | |
| **National Security** | | NIEM | |
| **Border Security** | | NIEM | |
| **Maritime Security** | | MIEM | |
| **Port Security** | | NIEM | |
| **Critical Infrastructure** | | NIEM | |

DRAFT

| | |
|---|---|
| **Protection** | |
| **Cyber Data Exchange** | NIEM<br>STYX<br>TAXII<br>CyBOX |
| **Geospatial Data** | |
| **Sensor Data** | |
| | |

# 7 Annex 4: Infrastructure and Technology Standards

The following table identifies public safety developed/adopted open technology standards.

Table *2* – Infrastructure and Technology Standards

| Applicable Technology Standards | **Brief Description** | **Lead Agency** | **Agencies Supporting this Standard** |
|---|---|---|---|
| | | | |
| | | | |

DRAFT

# 8 Annex 5 – PS Open Source

The following table identifies completed public safety developed/adopted open source solutions.

Table *3* – Infrastructure and Technology Standards

| Open Source Application | **Brief Description** | **Develop and Contributing (Agency)** | **Location** |
|---|---|---|---|
| | | | |
| | | | |

DRAFT

DRAFT

# 9 Annex 5 - Reference Documents

The following document were used in the preparation of this roadmap.


1. Operation Guide for the Interoperability Continuum, Homeland Security, SAFECOM, https://www.dhs.gov/sites/default/files/publications/Operational%20Guide%20for%20the%20Interoperability%20Continuum_0.pdf
2. Public Safety Canada National Information Exchange Model (NIEM), Galdos Systems Inc., http://www.galdosinc.com/solutions/case-studies/public-safety-canada
3. Emergency Management Systems Interoperability Framework Vision, 2010, Advanced Systems Management Group Ltd.,
4. Emergency Management Systems Interoperability Framework Overview, 2010, Advanced Systems Management Group Ltd.,
5. Public Safety Canada (PSC)- Interoperability – Data Exchange Standards, Recommendation Report, Version: Draft 0.94, Date: September 15th, 2010
6. I2F
7. GDPR
8. Harbour Siren a630942.pdf
9. IEF