Developing the CSSP Planning Process

Brian W. Greene
DRDC – Centre for Security Science

Defence Research and Development Canada

Reference Document
DRDC-RDDC-2017-D018
March 2017

Abstract

This Reference Document describes and captures work carried out between 2012 and 2015 in support of the effort to establish a strategic policy planning framework for the Canadian Safety and Security Program (CSSP), including the first group of Portfolio Narratives written in support of the initiative. It also includes a diagrammatic representation of the overall process.

Résumé

Le présent document de référence énonce et décrit les travaux effectués entre 2012 et 2015 à l'appui de l'établissement d'un cadre de planification d'une politique stratégique pour le Programme canadien pour la sûreté et la sécurité (PCSS), ce qui comprend le premier groupe de descriptions de portefeuilles rédigées pour les besoins de cette initiative. Il comporte par ailleurs un diagramme représentant l'ensemble du processus.

Table of Contents

List of Figures

List of Tables

Acknowledgements

I would like to thank my colleagues at DRDC CSS for their contributions to the development of the CSSP planning process. In particular, I want to thank the following individuals for their efforts in writing the CSSP Portfolio Narratives: Daniel Charlebois, Philip Dawe, Sheldon Dickie, Lynne Genik, Rodney Howes, Paul Hubbard, Guy Jonkmans, Carey Larsson, Stéphane Lefebvre, Dave Matschke, Pierre Meunier, Jack Pagotto, Marc Roy, Doug Socha, Simona Verga, and Norm Yanofsky.

1 Introduction

This Reference Document describes and captures work carried out between 2012 and 2015 in support of the effort to establish a strategic policy planning framework for the Canadian Safety and Security Program (CSSP).

The first stage in this initiative was the development of an environmental scan to provide an overview of the key drivers and emerging trends defining the context in which the CSSP operates. This document was released as CSSP Environmental Scan 2013 (also catalogued under the author's name as DRDC-RDDC-2014-R83). An update to that document—Strategic Assessment 2015[1]—followed two years later. Although never released as an official CSSP planning document, Strategic Assessment 2015 was subsequently published under the author's name as a DRDC Scientific Letter (DRDC-RDDC-2017-L006).

The next phase in building the planning process commenced in late 2013 and focused on the development of narrative documents to describe the program of work in each of the CSSP's domains of activity, also known as portfolios. These Portfolio Narratives were written by the responsible DRDC Centre for Security Science (DRDC CSS) Portfolio Manager in accordance with the requirements set out in a template drafted by the author (reproduced in Chapter 2). A second version of the template (also reproduced below) was circulated in August 2014, with the narratives revised accordingly.

Along with the Environmental Scan/Strategic Assessment, the Portfolio Narratives (contained in Annexes A through L)[2] were envisioned as the foundational analytical documents on which the annual CSSP Strategic Planning Guidance (SPG) would henceforth be based. Released annually in advance of the new fiscal year, the SPG provides guidance and direction related to the overall investment priorities of the CSSP. This streamlined planning process is captured in the diagram depicted in Chapter 3, which was used to socialize the new planning framework within DRDC CSS.

[1] The name change reflected the fact that the document in question made no claim to being comprehensive in its treatment of source material (environmental scans typically attempt to capture all relevant developments and/or pieces of information of interest). The final product was thus better described as a strategic assessment.

[2] The twelve narratives included here are the versions circulated for comment to external partners in December 2014 and January 2015.

2 CSSP Portfolio Narrative Templates

2.1 Version 1 (February 2014)

Name of Portfolio

Introduction

- What is the portfolio's main objective (i.e., why was it created/why does it exist/what is its scope of activity)?
- Who are your partners?

Strategic Direction

- Which federal and/or national strategies, action plans, and/or policies are driving the work of the portfolio?

Objectives

- What are the portfolio's objectives?
  - These should be specific to the portfolio, yet relatively high-level (i.e., significant enough to cover an ongoing, multi-stage work program with various lines of inquiry).
  - These should flow directly from the strategic policy documents cited above.

Priorities

- Consistent with these objectives, what are the portfolio's primary areas of focus?
  - These should be more specific/narrow in focus than the Objectives and capture both ongoing and future work.

Work Program

- What kind of work is being done to support these priorities?
  - Provide illustrative examples.
- What gaps are being addressed?

What's Ahead

- What needs to be done next (e.g., studies, scoping, options analysis, etc.)?
- Are there any emerging S&T developments and/or issues that are likely to require attention in the next three to five years?
- This section should identify what should be addressed in the next Call for Proposals.

2.2 Version 2 (August 2014)

Name of Portfolio

Introduction

DO NOT reference CSSP Outcomes in this section or anywhere else in the narrative as the basis for the portfolio's work program.

- What is the portfolio's main objective?
  - What safety and/or security problem/challenge was it created to address?
  - What is its scope of (S&T) activity?
- Who are your key partners (i.e., who do you most often work with)?
  - All federal government partners should be noted.
  - An annex may be attached to provide a more complete listing of partners, including the relevant sub-group, directorate, etc.
- What is your engagement strategy (i.e., who do you speak to in order to determine what's important in your domain)?
  - Community of Practice (if applicable), Working Groups, Other Bodies/Organizations, etc.
  - An annex may be attached to provide a more detailed list.

Strategic Direction

- Which federal and/or national strategies, action plans, and/or policies are driving the work of the portfolio?
  - DO NOT merely cite the relevant policies, etc. Identify the specific aspects which apply to the portfolio's domain of operations.
- Provide a summary of the analysis that underpins the portfolio's focus (i.e., what is the rationale for the portfolio's work program). This is the most important part of the narrative!!!!
  - If necessary, cite the relevant scientific reports that underpin this analysis. This can include everything from work done within DRDC and by other federal government scientists, to academic/think tank studies and publications, to reports issued by foreign government departments/agencies or international organizations.
  - The key here is to cite scientific sources or other analytical work.

Program of Work

- Describe the kind of work being done in support of the portfolio's objectives.
  - Provide illustrative examples, noting the gaps being addressed.

    - It is not necessary to provide a complete list of projects being managed by the portfolio.
- Use this section to highlight how S&T is being developed/employed in support of the portfolio's objectives.
- If possible, lay out a multi-year (three-year) plan for achieving the portfolio's objectives.
    - Based on work presently being conducted, identify the logical next step(s)?
    - How will anticipated future work build on what is being done now.

3 CSSP Annual Planning Process Diagram

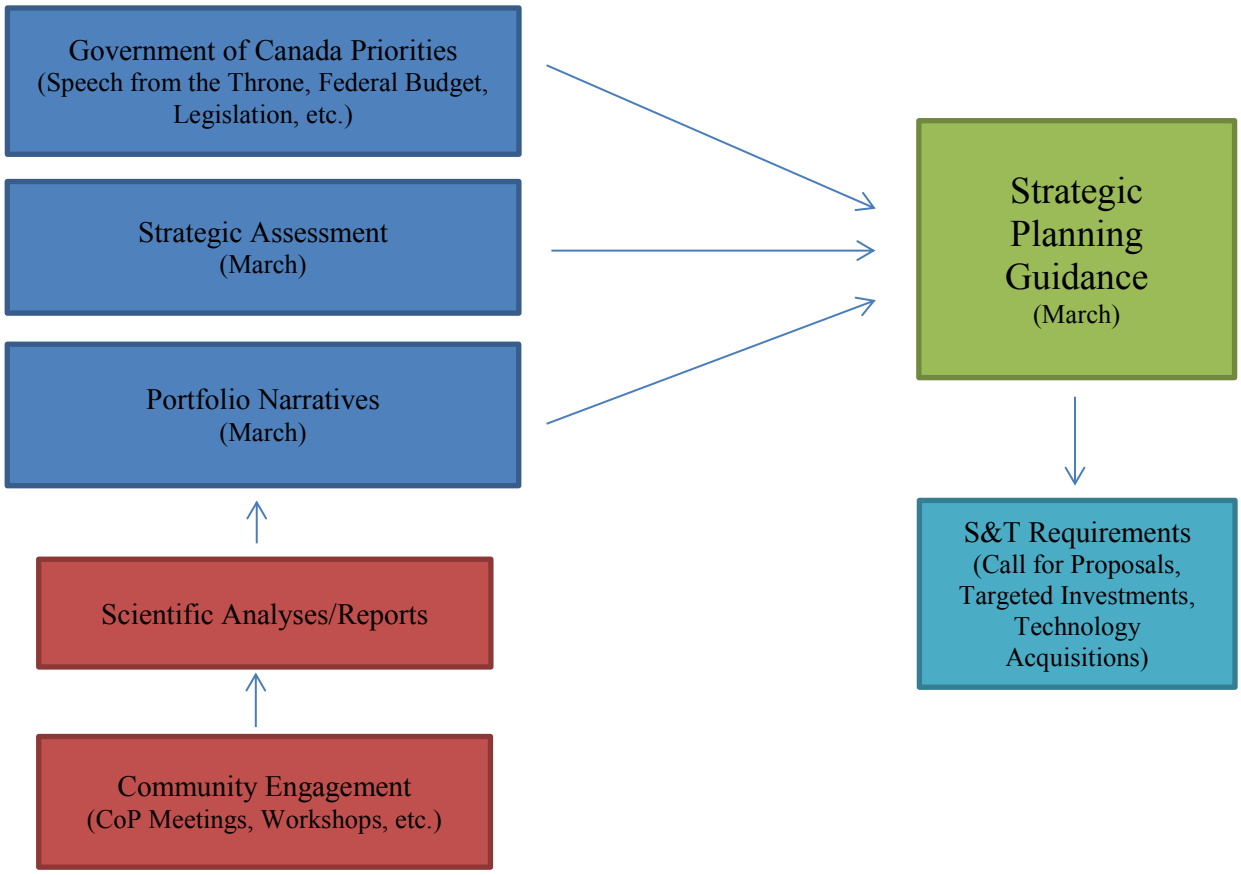


Figure 1: *CSSP Annual Planning Process.*

Strategic Planning Guidance: Provides guidance and direction related to the overall investment priorities of the Canadian Safety and Security Program (CSSP).

Strategic Assessment: Provides an overview of the key contemporary and short-term (one to three years) drivers and trends defining the context in which the CSSP is anticipated to operate.

Portfolio Narratives: Provide a summary of the work program in the CSSP's various domains of activity. Each narrative identifies the portfolio's main objective, its partners, sources of strategic policy direction, areas of focus (based on ongoing analysis), and work plan, including its projects and the gaps being addressed.

This page intentionally left blank.

References

Greene, B., CSSP Environmental Scan 2013, DRDC-RDDC-2014-R83, Defence Research and Development Canada, September 2014.

Greene, B., Strategic Assessment 2015, DRDC-RDDC-2017-L006 to DG DRDC CSS, Defence Research and Development Canada, 3 February 2017.

This page intentionally left blank.

Annex A Biological

Introduction

The Biological Hazards portfolio initiates, catalyzes, and coordinates the proactive development of S&T solutions that aim to negate the threat and minimize the impact of biological agents on public safety, security, and the economy. While traditionally the biological portfolio has viewed the risk associated with biological agents in terms of high impact events of low probability occurring in Canada, globalization has served to increase exposure, access, transportation, and dissemination of knowledge so that both the spectrum of threat agents and the CB-event probability have increased significantly. The intentional development of GM organisms (e.g. which could carry infectious diseases or highly infectious viral agents) or the use of synthetic biology (e.g. aerosolized inhibitory mRNA) are examples of new potential threats in the bio domain.

The objectives of the biological portfolio activities are to ensure that government policy makers have access to scientific expertise and advice on the hazards, threats, risks and countermeasures for biological agents while developing national policies; support the intelligence communities on scientific trends and advanced means to detect and identify early signs of hazards and threats; and support the research, development and transition to operations of new capabilities to prevent / mitigate, prepare for, respond to and recover from biological events in Canada. The scope of S&T needs addressed by the Portfolio is broad as it encompasses the terrorist use of biological agents traditionally considered as weapons (i.e. anthrax, etc.) as well as an expanding suite of non-traditional scenarios and agents that could jeopardize public security and the economic well-being of Canadians. Zoonotic avian influenza and the re-creation of the 1918 Spanish flu virus through synthetic biology are recent examples that speak to the evolving spectrum of biological agents and events that the Portfolio aims to address.

The delivery of the S&T agenda of the biological portfolio is greatly facilitated by the Biological Community of Practice that the Portfolio fosters. The CoP is a well-established network of mostly federal laboratory partners including Public Health Agency Canada, Canadian Food Inspection Agency, Agriculture and Agri-Food Canada, Public Safety Canada, Canadian Armed Forces/Department of National Defence, Defence Research and Development Canada, National Research Council, Royal Military College, Environment Canada, Canadian Security Intelligence Service, Royal Canadian Mounted Police, and the Department of Foreign Affairs, Trade and Development. Annex A provides an overview of each of their roles and mandates related to biological threat issues.

In addition to these CoP interactions, active collaboration with allied governments is integral to the program, particularly with the US (CTTSO, DHS, CDC), the UK (CPNI, Home Office) and Australia (DSTO). In addition, CSS is fully engaged in MCM development through the MCM Consortium, under the AU-CA-UK-US CBR MOU, for collaboration and burden sharing.

Policy and Operational Context

The Government of Canada has published several documents through Public Safety Canada including *An Emergency Management Framework for Canada* (2nd edition 2011)[1], the *National Emergency Response System* (2011)[2], *The Chemical, Biological, Radiological, Nuclear and Explosive Resilience Strategy for Canada* (2011)[3] and Action Plan (2011)[4] as well as other related documents such as *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (2011)[5]. The overall content of these documents provides overarching policy guidance for the large number of federal departments and agencies involved in achieving desired Government Public Safety and Security outcomes. Both the emergency management components and the strategic objectives provide general guidance to investment opportunities for the biological portfolio.

The North American Plan for Animal and Pandemic Influenza[6], the Quadrilateral Medical Countermeasures Consortium (MCMC) under the CBR MOU, and the Global Health Surveillance Initiative are examples of policy initiatives to elevate the response to pandemic threats to people, livestock, and food to the international level. Canada's susceptibility to biological threats like SARS and MERS, with origins overseas, for example, is of increasing concern. In addition to burden sharing and leveraging opportunities such collaboration affords (e.g. MCMC) it is now increasingly important to employ a more holistic approach that better recognizes the interconnectedness of public health, animal health, and food safety and that elevates Canada's situational awareness to the global level and integrates it with partner nation systems through leveraging efforts like the Global Health Security Initiative (GHSI). The aim is to coordinate a global response to threats such as SARS, Ebola, and H1N1. In this context, the biological portfolio is well positioned to capitalize on recent investments made and lessons learned from the development of CAHSN (CRTI-04-0004RD), CNPHI, bio forensics, and the development of rapid tests for high threat zoonoses (CRTI 0196RD).

Program of Work

The early CRTI program of work that the current biological portfolio is built off of significantly increased the Canadian biological laboratory capabilities and capacity to conduct world-class scientific work; it sponsored various projects that advanced technologies to understand the vulnerabilities and risks to Canada's food safety, and to improve animal disease emergency management. Other investments provided secure web-based capabilities for real-time surveillance, intelligence exchange and response to critical public health events by federal, provincial, and regional health authorities. The CSSP-funded development of biological detection methods and equipment have improved the capabilities of responders to rapidly conduct assessments and diagnostics on-site and are now employed across government. CSSP has also made investments to increase the protection of first responders and related interoperability

[1] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/index-eng.aspx accessed 05 March 2014.
[2] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-rspns-sstm/index-eng.aspx accessed 05 March 2014.
[3] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg/index-eng.aspx accessed on 05 March 2014.
[4] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-ctn-pln/index-eng.aspx accessed on 05 March 2014.
[5] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-eng.aspx accessed 05 March 2014.
[6] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nml-pndmc-nflnz/index-eng.aspx.

through the development of the first national standard of requirements for protective CBRN equipment[1].

The following provides a picture of the current and planned program of work within the portfolio focused on key areas of concern to the biological portfolio, as well as remaining challenge areas for each.

Rapid Diagnostics and Situational Awareness:

Past investments by the biological portfolio have focused significantly on containment of outbreaks of infectious diseases. Effective containment measures can have a significant impact on disease spread. Accordingly, part of the Portfolio effort has focused on the development of rapid diagnostics, with one recent effort currently wrapping up (Next generation sequencing, direct detection and genotyping of fungi, bacteria and nematodes in the agri-food system: CRTI 09-0462RD). In its present state, due to investments made, diagnostic capability and capacity is no longer rate-limiting in the response and containment of disease spread. Room for improvement identified in a recent table top exercise aimed at evaluating the capacity and capability of the laboratory network associated with the Canadian Animal Health Surveillance Network (CAHSN – developed under CRTI 04-0004RD) to respond to an outbreak of foot and mouth disease (FMD) includes improving the effectiveness of situational awareness and information exchange by immediately ensuring roll out of the CAHSN information exchange tool within the next 12 months.

There is a need for some investment to explore approaches to supplementing current capabilities with measures and processes to deal with emerging threats such as outbreaks of zoonotic diseases. A relatively recent project (Foresight and Capability-Based Planning for Animal Disease Emergency Management: CRTI 07-0109RD) highlighted the need for i) integrated public and animal health approaches to risk management; ii) better intelligence, information and data sharing, and iii) stronger anticipation capability, in order to manage future disease risks. Surveillance networks like CAHSN (CRTI-04-0004RD) and the Canadian Network for Public Health Intelligence (CNPHI – developed under CRTI 02-0035RD) that track disease occurrence in animal and human populations nationally, respectively, and associated intelligence gathering networks, such as the on-going project entitled Centre for Emerging and Zoonotic Disease Integrated Intelligence and Response (CEZD-IRR developed under CSSP-2013-CP-1022) have been established, in part, as a result. As we move forward from these efforts, it is now increasingly important to employ a more holistic approach that better recognizes the interconnectedness of public health, animal health, and food safety and that elevates Canada's situational awareness to the global level and integrates it with partner nation systems through leveraging efforts like the Global Health Security Initiative (GHSI). The aim is to coordinate a global response to threats such as SARS, Ebola, and H1N1. In this context, the CB Portfolio is well positioned to capitalize on recent investments made and lessons learned from the development of CAHSN, CNPHI, bio forensics, and the development of rapid tests for high threat zoonoses (CRTI 01-0196RD). Ideally, further investments in this type of pre-event/early-post-event S&T will ultimately help lead to detecting the disease off shore so that

[1] Canadian Standards Association (Committee Chair: Dr. Eva Dickson). Protection of First Responders from Chemical, Biological, Radiological, and Nuclear (CBRN) Events CAN/CGSB 205.1/CSA Z1610, A National Standard of Canada. CSA Group Publishing. ISBN 978-1-55491-501-9, 2011, 154 pages.

containment and preventative measures can be put in place prior to the disease impacting Canadian populations. Remaining challenge areas include elevating current bio situational awareness to the national and international level to inform decision makers through the harmonization and advancement of existing bio surveillance capabilities in animal and human health to address key bio areas of concern (i.e. inter-species disease transmission, AMR, pandemic) building on previous CSS investments in the Canadian Network for Public Health Intelligence and the Canadian Animal Health Surveillance Network.

Containment and Decontamination:

Early detection combined with 100% effective confinement are ideal for cessation of outbreak during the early exponential growth period when infected population numbers are small. To this end, the CB Portfolio has funded projects to develop decontamination methods that can increase confidence that measures in place within the 1km, 5km, 100km, etc. zones around farms are sufficient to guarantee negligible transmission of disease to other livestock and beyond the border. Building confidence in the capability to contain is essential to addressing the natural tendency to close the CA-US border upon first detection. In terms of economic impact, experience from BSE dictates that the closing of the borders costs millions of dollars in loss per day. To minimize this probability, the CB Portfolio has invested significantly in S&T to increase confidence in decontamination and containment measures so as to secure the food supply and minimize the risk of such catastrophic economic loss (for example, two recently completed projects entitled “Validation of decontamination processes in the Agri-Food context—CRTI 08-0122TD” and “S&T Solutions to Mitigate Vulnerabilities in Canada's Food Supply—CRTI 08-0203RD").

In principle, as with diagnostics, the impact of S&T that can contain disease within a 1, 5, 100 km, etc zone with high confidence is semi-quantifiable both in terms of decrease in infected population numbers and in terms of economic gain due to informed decision makers having the evidence they need to keep borders open. However, at this time, development of these metrics is relatively immature. Accordingly, evaluation via exercises that test the system is likely timely to evaluate and semi-quantify the effectiveness of investments made, to identify capability gaps to more effective containment, and to define the evidence needed by decision makers to be more confident in containment measures. Along this vein, addressing eroding training opportunities for first responders and receivers to capitalize on such investments is essential to ensure effective technology transition.

Medical Countermeasures:

The utility of medical countermeasures in the response to infectious agents has long been recognized by the CB Portfolio for both human and animal populations. The results of a recent study[1] on the impact of various containment techniques indicated that post-detection use of vaccines as prophylactics is the most effective post-detection method to mitigate consequences and minimize loss by as much as 90%. The impact of past investment in MCM S&T is perhaps best illustrated by the recent Ebola outbreak in West Africa where Canadian experimental

[1] Backer, J.A., T. J. Hagenaars, H. J. van Roermund, and M. C. de Jong. "Modelling the effectiveness and risks of vaccination strategies to control classical swine fever epidemics." *Journal of the Royal Society, Interface* 6, no. 39 (2009): 849-861.

medical countermeasures are being looked to as solutions to contain the disease and to treat victims of it. The vaccine [developed under CRTI 06-0218RD, 09-0453TD and CSSP-2013-CP-1017] and ZMapp antibody [CRTI 01-0087RD] MCMs being considered are the result of 12 years of commitment of the Biological Portfolio to develop MCM solutions to the threat of Ebola. As the world turns to these Canadian products and leadership in the area, and starts to invest millions of dollars in their development, the high impact and leveraging of investments made by the Portfolio in MCM development is clear. Remaining challenge areas include the need for efficacy studies for select Medical Countermeasures of interest to public security, as well as the development of protocols for the emergency transition of advanced medical countermeasures to civil authorities at the federal, provincial, territorial and large municipality levels, including an operational analysis of optimal stockpile locations and likely outbreak locations.

Biological Portfolio Partners

PS Canada – responsible for promoting and coordinating emergency management plans, and for coordinating the Government of Canada's response to an emergency

Canadian Armed Forces / Department of National Defence – military assistance to civil authorities in CBRNE response

Canadian Food Inspection Agency (CFIA) – Science-based regulator agency that safeguards Food, Animals and Plants , enhancing health, well-being, environment and the economy.

Health Canada / Public Health Agency of Canada – in response to a CBRNE event and upon request of a province or territory provide Emergency Health services that could include: public health, medical care, environmental health, medical equipment, pharmaceuticals and health care personnel

Environment Canada – provision of information and advice in response to a CBRNE event causing environmental contamination or wildlife disease

Defence Research and Development Canada – provide S&T support to the CF, DND and PS Canada

Canadian Security Investigation Service – investigation of suspected CBRNE attacks conducted with "political motivation"

Royal Canadian Mounted Police – investigation of suspected illegal or criminal use of active CBRNE agents

Department of Foreign Affairs, Trade and Development – coordinating and providing the Canadian position on CBRNE weapons of mass destruction to the international community

This page intentionally left blank.

Annex B Border and Transportation Security

Overview

The BTS portfolio's main objective is to support operations and inform development of strategy and policy in the border context with scientifically rigorous analyses and pilot programs that generate options for partners. The sub-objectives of the portfolio include informing and enhancing three main areas through S&T investment: 1) domain awareness in the air, land, and maritime border environments; 2) screening of cargo and security of cross-border supply chains; and 3) screening of travellers and luggage at border points of entry and in the transportation system.

There are many public sources[1] that describe the threat context for border security. Transnational crime organizations attempt to exploit the border for smuggling of narcotics, people, currency, contraband tobacco, and weapons. There are national security/terrorism threats associated with illegal entry into the country or conveyance of WMD across the border. Illegal migration and agricultural concerns (plant pests and animal diseases) and communicable diseases are also concerns at the border. Arctic sovereignty and arctic domain awareness have also emerged as drivers for the portfolio's activities.

In the area of transportation, the main threats are the 'bomb-in-a-box' scenario for air travel,[2] which overlaps significantly with the screening for smuggling of explosives, and the risks associated with transportation of hazardous materials and emergency response; the latter of which is addressed through other CSSP portfolios.

The portfolio's activities usually come in three main forms. *Pilot projects* are used to de-risk introduction of new technology by trialing them in operations. A previous pilot showed the use of marine radar surveillance networks on the Great Lakes and a current pilot is trialing facial recognition technology at Pearson Airport. *Specialized developments* within projects are used to tailor solutions from other contexts, such as defence, to border applications. Previous examples have included geo-spatial tools for management of border region alerting and enhancing X-ray screeners with an additional stage of neutron imaging to improve detection of explosives and narcotics in air luggage. *Analyses* of future technology or future operational/policy requirements are performed through studies. Previous examples have explored automated border control technologies, trends in biometrics, and trends in air travel.

There are a variety of Canadian federal and U.S. partnering organizations in the BTS Community of Practice. These include the RCMP, CBSA, Public Safety Canada, Transport Canada, the

[1] See for instance the Canada-US IBET Threat Assessment 2010 (http://www.rcmp-grc.gc.ca/ibet-eipf/reports-rapports/2010-threat-menace-eng.htm), IMSWG threat assessments [SECRET], or U.S. – Canada Joint Border Threat and Risk Assessments (http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/jbtra-ecmrf-eng.html).

[2] See the Government of Canada Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rspns-cmmssn/rspns-cmmssn-eng.pdf).

Canadian Coast Guard, Citizenship and Immigration Canada, DND, and the U.S. Department of Homeland Security (additional information on each organization can be found in the annex).

Other partners/stakeholders for the portfolio include industrial and academic partners, industry associations such as CADSI, port authorities, Offices of the Privacy Commissioners (provincial and federal), intelligence (CSIS, CSEC), and other international collaborating government organizations from the United Kingdom and Europe.

There are several self-coordinating groups in the community, such as the Integrated Border Enforcement Teams (IBETs) that include RCMP, CBSA, and US CBP, ICE, and USCG; the Great Lakes Marine Security Operations Centre (GL MSOC) that includes RCMP, DND, TC, CBSA, CCG, and US partners; and the Interdepartmental Maritime Security Working Group (IMSWG), led by TC, that includes many federal partners.

Policy and Operational Context

The Beyond the Border declaration[1] identifies four key areas of cooperation (both in the declaration itself and the Action Plan): Addressing Threats Early; Trade Facilitation, Economic Growth and Jobs; Integrated Cross-Border Law Enforcement; and Critical Infrastructure and Cyber-security. Many of the portfolio's activities support these key areas of cooperation, particularly that of addressing threats early, which includes enhancing domain awareness in the air, land, and maritime environments as a goal.
Canada's Maritime Security Strategic Framework[2] identifies three challenges and five strategic objectives.

[1] See the Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness Public Website at Safety Canada, http://www.publicsafety.gc.ca/cnt/brdr-strtgs/bynd-th-brdr/index-eng.aspx.
[2] See Maritime Domain Awareness Initiative Website at Transport Canada https://www.tc.gc.ca/eng/marinesecurity/initiatives-235.htm.

Maritime Domain Awareness Gaps
Lack of persistent wide area surveillance of Canada's Exclusive Economic Zone and approaches, acknowledging the particular challenges of the Arctic and the Great Lakes/St Lawrence Seaway;
Inadequate awareness of small vessels in waters under Canada's jurisdiction and approaches; and
Impediments to the sharing of routine information that enables MDA with particular note to legal, policy, and cultural challenges.
Maritime Domain Awareness Objectives
Track, Monitor, and Identify vessels;
Access and Maintain data;
Collect, Analyze, Disseminate, and Share Information;
Facilitate Awareness of MDA Activities; and
Monitor and Review MDA Performance.

Table 1: Canada's Maritime Domain Awareness Strategy, from IMSWG

The report of the Auditor General of Canada of Fall 2013[1] explicitly identifies two gaps: 1) a border surveillance gap, stating that the RCMP does not have the information it needs to assess the effectiveness of its interception activities; and 2) a screening gap, stating that CBSA lacks systems and practices, which is allowing individuals to pass through points of entry despite being on lookouts. Projects exploiting radar, hydro-acoustics, electro-optics, and geographical information systems have been funded by DRDC CSS to support the surveillance gap (in the Auditor General report, and the IMSWG strategy). Projects on biometrics, in particular facial recognition, have been funded to support the lookout gap.

Other national strategies that apply to the portfolio's domain of operations include *Building Resilience against Terrorism: Canada's Counter-Terrorism Strategy*; *Securing an Open Society: Canada's National Security Policy*; and various reports from the Senate Standing Committee on National Security and Defence, with coasts, border crossings, seaports, airports, and the Arctic as key areas.

In the 2014 budget, the government announced an allocation of $91.7 million to enhance its ability to combat contraband tobacco:

[1] See Chapter 5: preventing illegal entry into Canada http://www.oag-bvg.gc.ca/internet/English/parl_oag_201311_05_e_38799.html.

> *"…Building on recent investments, Economic Action Plan 2014 proposes to allocate $91.7 million over five years to enhance the RCMP's ability to combat contraband tobacco. The new funding will be used to increase intelligence-led policing efforts, including the creation of a Geospatial Intelligence and Automated Dispatch Centre and the deployment of a range of sensor devices to detect movement on the border in high-risk areas, from the Maine-Quebec border to Oakville, Ontario. Specifically, these enhancements would involve the deployment of high-end sensor devices including radar, sonar and unmanned ground sensors; mobile workstations; and long-range thermal video cameras to enable RCMP officers to respond in real time to high-risk alerts."*[1]

This indicates a requirement for the CSSP to support the RCMP for a large-scale investment in surveillance, which is currently ongoing in the portfolio.

The Arctic is still emerging as a transportation and border security concern. Canada's Northern Strategy[2] and DRDC's Arctic S&T Strategy are key documents describing how the portfolio should invest. IMSWG partners are putting attention to the Arctic from the perspective of both awareness (assessments of Arctic maritime domain awareness, etc.) and response, and will continue combined assessment with U.S. partners in the near future. The Canadian Coast Guard is in the initial stages of plans to offer services in emerging Arctic marine corridors.[3]

CBSA is in the midst of an internal 'border modernization' initiative to improve security and increase flow across the points of entry. This is motivated by a desire to improve efficiency ("faster, better, cheaper"), but also physical constraints on space in air terminals and a forecasted trend of increased air travellers.[4] According to Statistics Canada, the total number of passengers (domestic and foreign) arriving at Canadian airports increased 4.8 percent in 2012, to almost 119 million.[5]

In some technology areas, the landscape for the BTS portfolio is quickly evolving, particularly in biometrics, data analytics, and cyberspace. In other areas, such as broad area surveillance, trace detection and imaging, technologies are more established and only incremental improvements are expected. The technological strategy moving forward for the BTS portfolio is predicated on the thesis that there are marginal returns for physical screening technologies such as trace detection, and imaging technologies, in comparison to a higher return on investment for digital screening, or making better use of the large variety and quantity of public information and intelligence in targeting[6].

In the area of Biometrics, facial recognition in a semi-cooperative context, but also iris, fingerprints, and other emerging biometrics, such as vein matching, are steadily improving the ability to quickly confirm identity. This will have an impact on the effectiveness of watch lists

---

[1] 2014 Federal Budget, p. 211, http://www.budget.gc.ca/2014/docs/plan/pdf/budget2014-eng.pdf.
[2] Canada's Northern Strategy, http://www.northernstrategy.gc.ca/index-eng.asp.
[3] Canadian Coast Guard Priorities, http://www.ccg-gcc.gc.ca/IBHRP/Section3-Priorities.
[4] Survey of Technologies for the Airport Border of the Future, Contractor Report, DRDC-RDDC-2014-C65, April 2014.
[5] Statistics Canada. Airport activity, 2012. http://www.statcan.gc.ca/dailyquotidien/130920/dq130920c-eng.htm.
[6] See discussions in http://www.dataversity.net/big-data-on-the-border/ and http://www.nytimes.com/2014/05/08/business/your-digital-trail-follows-you-to-the-border.html.

and offer improved levels of service to legitimate travellers. In the future, biometrics will be integrated into automated border control (ABC) applications linked to electronic documents. There are privacy requirements and cultural acceptance, as well as operational concepts that still need to be addressed. When coupled with video analytics to support multi-camera surveillance systems, biometrics can provide real-time location of individuals within a given area to support interdiction activities at points of entry.

Mobile computing platforms that bring information to the hands of front-line border staff are bringing power to the edge.[1] In the domain awareness context this enables self-dispatch, in which RCMP staff are able to respond faster because they have local access to real-time information through a geo-spatial information system (GIS) for sensor and track management. At points of entry, mobile computing can improve efficiency for both cargo and people by allowing a distributed many-to-many engagement between staff and travellers/cargo rather than the traditional one-to-many engagement at primary inspection lanes.

In many border contexts, the cyber implications are unknown. This applies to vulnerabilities of integrated, digital automation in the supply chain and to networks that link sensors at points of entry for cargo and travellers and at remote locations for illegal entry.

Domain Awareness technologies such as radar, sonar, thermal cameras, and satellite surveillance are well established in other contexts such as defence, but can be further exploited to provide input to a common operating picture for border security. In particular, detection of small vessels from space-based radar and cameras is needed to support maritime domain awareness. Developing new technologies in this area requires a scale of R&D that is likely outside the reach of CSS. Our incremental investment over what is already invested by other government departments may yield marginal returns on CSSP outcomes[2]. However, partners will want to exploit capabilities from the defence context for in-land waterways and Arctic surveillance.

Imaging technologies to support screening for explosives (e.g. neutron scanning added in serial with X-ray systems[3]) are following a traditional evolution path for technology and have reached a maturity where it is now expensive to gain marginal improvements. X-ray screeners, for instance, are close to their optimal performance. Complementing these with other imaging technologies is proving expensive. There is room to improve the pattern recognition algorithms for adjudication of imagery from screeners, leading back to investment in image processing and data analytics. Trace detection is following a similar path in that marginal improvements to current capabilities come at expensive research effort. One known investment is CATSA's piloting of a two-mode system (RF and ultra-sound) to screen liquids for air travel.

Perhaps the biggest technological driver in the BTS context is so-called 'Big Data'[4]—taken to mean the real-time processing and searching of comprehensive data from disparate non-integrated databases on travellers (as individuals), shippers and cargo manifests as well as intelligence

[1] Power to the Edge: Command and Control in the Information Age / David. S. Alberts, Richard E. Hayes, CCRP Publication Series, 2003. http://www.dodccrp.org/files/Alberts_Power.pdf.
[2] Hubbard, P and Muenier, Pierre, Maritime Domain Awareness in the Canadian Safety and Security Program, DRDC CSS Letter Report 2013-042, December 2013.
[3] See project CSSP-2013-CP-1004 Beyond the Border Enhanced Cargo Screener.
[4] The best recommended resource on this topic is Wikipedia: http://en.wikipedia.org/wiki/Big_data.

sources and sensors providing pervasive surveillance. The key opportunity from Big Data is to change the approach to the needle-in-the-haystack problem associated with finding smuggled goods or illegal entries amongst the enormous amount of legitimate trade and travellers. The solution is transitioning from the traditional use of human intelligence, experienced staff interviews, and physical searches, to a solution composed of data-mining, data analytics, and machine-learning to draw out suspicious activity. The key trend is the not just the sophistication of the database management and search tools, but the comprehensiveness of the accessible data. In the end-game of comprehensive data sets, heuristics (for instance, an individual is suspicious due to point of origin and one way ticket) are replaced by statistical inference engines that use pattern recognition to identify high-risk individuals and cargo. These engines can make use of new sources of information and databases that might provide a history of previous travel or perhaps recent financial or other activity of an individual. The barriers to this are the lack of computing and network infrastructure and the extent to which databases can be (or are permitted to be) shared or accessible and available for data-mining algorithms. While travellers may have a lowered expectation of privacy at the border[1], privacy impact assessments are still required to balance the value of increased security with the impact on Canadians [2]. In the context of Big Data, any CSS investment should likely be on data analytics (software) rather than the infrastructure to support it (hardware and networking).

As a general assessment, the BTS portfolio has a healthy program on domain awareness that is addressing gaps in maritime and land border surveillance, including surveillance of inland waterways, information sharing with the U.S., and bringing geo-intelligence to land border dispatch. The BTS portfolio also has a healthy program historically on biometrics addressing the use of facial recognition and other biometrics and video analytics at ports of entry. However, there has been little or no investment directed at the "big data" challenges and opportunities faced by border management stakeholders. Future investment should focus on the capture, manipulation, securing and exploitation of data associated with borders, quantitative / operational research on border crossings and empowering frontline personnel with access to intelligence produced from data analytics.

Program of Work

The following is the portfolio's program of work. For each, the current and planned future program is given as well as a theme for the remaining challenges in the area.

Biometrics and passenger screening

- Work Program currently includes:
    - CSSP-2013-CD-1063 Accelerated multi-camera retrieval.
    - CSSP-2013-CD-1064 Privacy-by-design architectures for storing biometrics.
    - CSSP-2013-CP-1020 Risk analysis for Iris biometric (continues into 14/15)

[1] See Checking In - Your privacy rights at airports and border crossings, https://www.priv.gc.ca/resource/fs-fi/02_05_d_45_e.pdf.
[2] See the discussion of sharing of Canadians' health information with US agencies, http://www.cbc.ca/news/canada/windsor /canadians-mental-health-info-routinely-shared-with-fbi-u-s-customs-1.2609159.

    - Study on emerging border security technologies (biometrics and screening)[1]
- Activities for 2014/15 :
    - CSSP-2014-CP-2000 Faces on the Move: Multi Camera Watchlist Screening project will demonstrate the readiness of face recognition technology for surveillance at the border in an airport environment. It will address technical performance and establish the privacy protocols and Government of Canada operations policies essential to the successful use of this technology for public safety.
    - Conduct joint CSS-DHS S&T meetings to calibrate activities and/or share data sets for semi-cooperative face recognition and/or exchange experiences with multi-mode biometric assessment facility.
- Theme / Remaining Barriers:
    - Exploitation of other data sources to enhance targeting solutions.
    - Quantitative assessments of passenger flow (simulations or perhaps OR studies).
    - Exploration of networked screeners at airports for centralized adjudication.

Technologies to increase passenger safety

- Work program currently includes:
    - CSSP-2013-CP-1004 BTB enhanced screener (continues 14/15)
    - CSSP-2013-CP-1014 Air cargo automated registration (continues 14/15)
    - CSSP-2013-CD-1068 Raman Spectroscopy for stand-off detection
- Activities for 2014/15 :
    - CSSP-2013-CP-1004 and 1014 will continue to address the "bomb-in-a-box" threat to air travel.
    - CSSP-2013-CP-1004 to be supported with a Technology Acquisition of Neutron Generator.
- Theme / Remaining Barriers:
    - Explore the detection and screening for plastic weapons (3D printing).

Technologies supporting fast screening of containers

- Work Program currently includes:
    - Nil
- Activities for 2014/15:
    - No planned projects
- Theme / Remaining Barriers:
    - Quantitative analysis of queuing and wait times at borders (e.g. analysis of "fluidity model" data from TC).
    - Pilots for efficient container management [CFP priority area]
        - Real-time tracking of containers and tamper-proof technologies.
        - Tech support to Secure Corridors initiative.

[1] This resulted in the contractor repot from NRC CISTI, Survey of Technologies for the Airport Border of the Future, Contractor Report, DRDC-RDDC-2014-C65, April 2014.

- Support/analysis to Harmonization with U.S./screen once, accept twice.
- Handheld mobile units.
- Cyber security assessment/generation of options for networking sensors for CBSA.

Assessing the cyber vulnerabilities of the supply chain and border sensor networks:

- Work program currently includes:
  - Nil
- Activities for 2014/15:
  - Exploratory joint work plan DHS S&T on Maritime Cyber Commerce (eCargo) Resilience: identify and engage stakeholders, perform risk assessment on threat, means, vulnerabilities, and consequence.
- Theme / Remaining Barriers:
  - Develop awareness of cyber threats to supply chain through collaborative workshop with DHS S&T.

Supporting domain awareness for Arctic security

- Work program currently includes:
  - Participation in IMSWG Arctic MDA working group.
- Activities for 2014/15:
  - Participation in Arctic GOC research workshop.
- Theme / Remaining Barriers:
  - Support exploitation of existing operational picture by RCMP, CBSA and CCG.

Supporting domain awareness through data Integration and analysis

- Work program currently includes:
  - CSSP-2012-TI-1018 CAN/US Sensor Sharing Pilot (CUSSP)
  - CSSP-2013-TI-1035 Maritime radar feeds and historical analysis for GL MSOC
  - CSSP-2013-CP-1007 IBET Geospatial COP viewer (continues 14/15)
  - CSSP-2013-CP-1012 Border Integrity Sensor Fusion and Dispatch (continues 14/15)
- Activities for 2014/15:
  - CSSP-2014-TI-2036 CUSSP 2.0
  - CSSP-2014-CP-2001 S2I Shiprider
  - Support RCMP with a ‘buy-rent-or-own’ workshop on surveillance infrastructure.
- Theme / Remaining Barriers:
  - Video analytics as a means to reduce staffing requirements/costs and improve exploitation of sensors – currently staff needed for PTZ camera control. Not sustainable with more cameras.
  - Methods to support self-dispatch of border staff (e.g. pilots of mobile computing platforms providing situational awareness from border sensors).

Annex: BTS Partners

The RCMP is responsible for border security between ports of entry; in particular, the Integrated Border Enforcement Teams (IBET) or their successors in the reorganized RCMP, Technical and Protective Operations Facility (TPOF), and the operational border integrity staff deployed across the country.

The CBSA is responsible for the air, land, and sea border points of entry, including people and cargo. CBSA has a Science and Engineering Directorate within its Information, Science and Technology Branch that is very active in CSSP projects. Other key personnel include those involved in the border modernization program within the Strategic Risk and Modernization Directorate of the Programs Branch.

Public Safety Law Enforcement and Border Strategies directorate "provides federal policy leadership, coordination and coherence on a variety of border issues such as customs, immigration, and cross-border law enforcement." The Border Policy and International Affairs directorate "provides federal policy leadership with respect to advancing domestic public safety priorities through international partnerships and activities."[1]

Transport Canada regulates air, sea, road, and rail transport across the country. This would include passenger safety, as well as resilience and protection of the supply chain. Canadian Air Transport Security Authority (CATSA) is responsible for screening air travellers and their baggage.

The Canadian Coast Guard (CCG), part of Department of Fisheries and Oceans, has a mandate to "protect the marine and freshwater environment, maintain maritime safety, facilitate maritime shipping and commerce and maritime accessibility, as well as support marine scientific excellence and Canada's federal maritime priorities." The CCG is also involved in maritime security based on its obligation to support departments and agencies mandated to provide security and enforcement within Canada under the Oceans Act.

Citizenship and Immigration Canada links immigration services with citizenship registration and has responsibility for Passport Canada.

The Department of National Defence is both a supporting responder (when requested) to border incursions and a key provider of surveillance data on maritime and air approaches and intelligence information.

Department of Homeland Security S&T (DHS S&T) is a key collaborator through the Critical Infrastructure Protection and Border Security (CIPABS) agreement with DRDC CSS. CSS and DHS S&T are jointly/collaboratively exploring border technology issues, which is essential to de-risking and harmonizing border technologies and processes in the long term.

[1] Public Safety Canada website – Border Strategies Section, http://www.publicsafety.gc.ca/cnt/trnsprnc/nfsrc-eng.aspx.

DHS – Customs and Border Protection (CBP) includes a border patrol component and is the operational counterpart to the RCMP for border surveillance/protection between ports of entry. CBP is also responsible at the ports of entry.

Annex C Critical Infrastructure

Overview

The main objective of the Critical Infrastructure (CI) portfolio is to address safety and security gaps through S&T activities to support CI resilience across the four pillars of emergency management (EM), namely, mitigation/prevention, preparedness, response, and recovery.[1] Given the breadth of the portfolio and the finite amount of funding, the scope of S&T activities needs to be focused on high importance issues, such as CI interdependencies, enhancing information sharing among stakeholders, and the link between cyber security and CI. Since much of the CSSP touches on most of the CI sectors,[2] there is overlap with many other CSS portfolios (for example, Border and Transportation Security, E-security, Psychosocial and Community Resilience, Explosives, etc.).

Key Partners

CI resilience is a multi-stakeholder issue, with a shared responsibility among federal, provincial, and municipal governments and CI owner/operators, who come from the private and public sectors. "In light of the interconnected nature of Canada's critical infrastructure, partnerships are required among government and critical infrastructure stakeholders, including owners and operators, law enforcement and the research and development community."[3]
Key partners for the CIR portfolio include federal, provincial, and international partners. Additional project partners include universities and industry partners.

Federal Partners

Public Safety Canada (PS) is a key federal partner, having the responsibility for national CI policy. Other federal government departments also play significant roles in CI across the spectrum of EM. For example, various departments are leads for the ten CI sectors (as identified in Annex A), others have roles in intelligence and operations (for example the Royal Canadian Mounted Police (RCMP) National Critical Infrastructure Team), yet others perform research related to CI (for example, the National Research Council (NRC)). Current CSSP federal project partners in the CIR portfolio are PS, Industry Canada (IC), Natural Resources Canada (NRCan), and NRC.

Provincial Partners

---

[1] "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." Public Safety Canada. National Strategy for Critical Infrastructure. (2009). Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx.

[2] Public Safety Canada (PS) has defined ten CI sectors: Energy and Utilities, Finance, Food, Transportation, Government, Information and Communication Technology (ICT), Health, Water, Safety, and Manufacturing.

[3] Public Safety Canada. Critical Infrastructure Partners. (2014). Available from: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-prtnrs-eng.aspx.

Provincial government departments are also key partners, given their role in provincial CI policy and operations. DRDC CSS began working with Emergency Management British Columbia (EMBC) in 2008 in preparation for the Vancouver 2010 Olympics. Other provincial partners engaged on CI include the New Brunswick Department of Public Safety (NB DPS) and Saskatchewan Emergency Management and Fire Safety (EMFS). Current CSSP provincial project partners in the CIR portfolio are EMBC and NB DPS.

International Partners

International partners play an important role for information sharing and leveraging expertise. The United States (US) Department of Homeland Security (DHS) Science and Technology (S&T) Directorate and DRDC CSS share similar mandates and have identified common S&T issues of interest. The US also has several national laboratories working in CIR S&T. For example, Argonne National Laboratory's Infrastructure Assurance Center works on energy infrastructure analysis, interdependencies, geographic information systems, risk analysis and assessment, and modeling and simulation. Notably they have developed tools for the Regional Resilience Assessment Program implemented by DHS and adopted by PS.

Other international organizations, such as universities and industry, have expertise in CI and partnerships have been and are being established to progress S&T for CI resilience.

CI Owners and Operators

The private sector is estimated to own/operate approximately 80-85% of CI in Canada and must be engaged in efforts regarding CI resilience. Private sector engagement is primarily through established working groups, including both industry associations and individual company representatives, as indicated below.

Engagement Strategy

Until 2012, DRDC CSS co-chaired a CI Community of Practice (CoP) with several other government departments. The CoP consisted primarily of federal government department representatives. Since 2012, the CI landscape in Canada has evolved, largely due to strides made by PS along with a growing recognition of CI at the provincial level. In particular, the private sector has been actively engaged by governments in efforts to enhance CI resilience. Acknowledging the diversity of stakeholders from government, industry, and academia, including representatives from policy, intelligence, operations, and S&T, the value of leveraging existing CI communities, such as cross-sector forums and sector working groups, was recognized. Consequently, the engagement strategy for the portfolio is to connect with existing CI groups to develop an awareness of their gaps, challenges, and S&T needs. In particular, PS spearheads a number of working groups related to CI and has welcomed CSS participation.

Engagement currently occurs through the following communities:

- National Cross Sector Forum (NCSF): Led by PS, membership of the NCSF is drawn from the ten sector networks and intended to be representative of a broad base of owners and operators, associations, and federal, provincial, and territorial governments;[1]

[1] Public Safety Canada. National Strategy for Critical Infrastructure. (2009). Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx.

- Multi-Sector Network (MSN): Led by PS, the MSN is similar to the NCSF in representation but is more of a "working level" rather than a management/executive group;

- Federal-Provincial-Territorial (FPT) Critical Infrastructure (CI) Working Group (WG): Led by PS, the FPT CI WG consists of CI representatives from the provinces, territories, and PS, and is co-chaired by a provincial representative and PS;and

- Provincial CI Program Managers and Networks: CSS is engaged with several provincial CI program managers and their networks, such as EMBC and the British Columbia CI Steering Committee and Saskatchewan EMFS and the Critical Infrastructure Assurance Network.

- Energy and Utilities Sector Network: Led by Natural Resources Canada (NRCan), the sector network includes representation from federal government departments, regulatory and portfolio agencies (e.g. National Energy Board), provincial/territorial governments, industry associations (e.g. Canadian Electricity Association), and the North American Electric Reliability Corporation. In the spring 2014, DRDC CSS facilitated an information sharing workshop with DHS S&T and energy sector representatives from the federal government.

- Global Navigation Satellite Systems (GNSS) Coordination Group: This group is led by Industry Canada and sponsored by the Canadian Space Agency, Communications Security Establishment Canada, Fisheries and Oceans, Department of Foreign Affairs, Trade and Development, Natural Resources Canada, Public Safety, and Transport Canada. In the spring 2014, DRDC CSS facilitated an information sharing workshop between the coordination group and DHS S&T. DRDC CSS currently participates in a newly established GNSS Vulnerabilities Working Group.

- Water Sector Network: This group involves PS, the Canadian Water and Wastewater Association, regional water suppliers, academic representation, etc.

- DHS S&T Resilient Systems Division (RSD): DHS S&T RSD focuses on Adaptive Risk Mitigation, Agile Disaster Management, Resilient Infrastructure, and Effective Training, Education and Performance.[1] DRDC CSS has been engaging with RSD for information sharing and potential collaboration in areas such as CI interdependency modelling, the electrical grid, and Global Positioning System (GPS).

- Individual Subject Matter Experts (SMEs) :Individual SMEs are engaged and consulted through existing relationships with CSS, such as ongoing projects and the Project

[1] U.S. Department of Homeland Security. Science and Technology Directorate Resilient Systems Division (2014). http://www.dhs.gov/st-rsd.

Management Board. Links with international SMEs are made through various fora, such as conferences, symposiums, and other working groups.

Relationships with additional communities not specifically mentioned, such as other sector working groups and academia, are being developed as opportunities permit.

Policy and Operational Context

Key Acts, Strategies, and Plans

Key acts, strategies, plans, etc. related to the work of the CI portfolio are identified below. The Emergency Management Act, Federal Emergency Response Plan, and Emergency Management Framework for Canada define federal responsibilities and plans for emergencies and a framework for federal, provincial, and territorial (FPT) EM initiatives, including those related to critical infrastructure. The National Strategy for Critical Infrastructure, Action Plan for Critical Infrastructure (2014-2017), and Canada-United States Action Plan for Critical Infrastructure provide more specific guidance and plans with respect to CI resilience across the federal government, provinces /territories, and border.

Emergency Management Act[1]

The Emergency Management Act specifies the EM responsibilities of federal ministers, specifying that ministers are responsible for identifying risks within their area of responsibility, including those related to critical infrastructure, and preparing, testing, maintaining, implementing, and exercising plans in accordance with those risks.

Federal Emergency Response Plan (FERP)[2]

The FERP is the Government of Canada's all-hazards response plan. It recognizes that critical infrastructure dependencies and interdependencies are one of the risk factors that increase the potential for disasters to transcend geographic or jurisdictional boundaries and challenge the EM capacity of provincial and federal governments.

Emergency Management Framework for Canada[3]

The Emergency Management Framework for Canada is a result of a joint effort among FPT governments to establish a common approach for FPT EM initiatives to ensure better alignment among the initiatives.

National Strategy for Critical Infrastructure

"The purpose of the National Strategy for Critical Infrastructure (the Strategy) is to strengthen the resiliency of critical infrastructure in Canada. The Strategy works toward this goal by setting the

[1] Government of Canada. Emergency Management Act (S.C. 2007, c. 15). Available from: http://laws-lois.justice.gc.ca/eng/acts/E-4.56/.
[2] Government of Canada. Federal Emergency Response Plan. (January 2011) Available from: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-eng.aspx.
[3] Public Safety Canada. An Emergency Management Framework for Canada, Second Edition, Ministers Responsible for Emergency Management (January 2011). Available from: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/index-eng.aspx.

direction for enhancing the resiliency of critical infrastructure against current and emerging hazards."[1]

In particular, the strategy identifies three objectives:

1. Build partnerships to support and enhance CI resilience. CI resilience is a multi-stakeholder issue, involving CI owners and operators predominantly from the private sector on one hand, and government agencies on the other. Building partnerships is critical in order to enhance resilience and effectively mitigate, prevent, prepare for, respond to, and recover from incidents.
2. Implement an all-hazards approach to risk management. In the context of the strategy, an "all hazards approach" is advocated in order to consider threats and hazards resulting from intentional, accidental, and natural events;
3. Advance the timely sharing and protection of information among partners and key stakeholders. This objective goes hand in hand with building partnerships and allows for collaboration and situational awareness in order to perform effective risk management and to mitigate/prevent, prepare for, respond to, and recover from events.

Action Plan for Critical Infrastructure (2014-2017)[2]
The Action Plan for CI specifies action items for each of the three strategic objectives of the National Strategy for CI. One of the projects in the program of work supports a specific deliverable under the action plan, that is, the development of a national CI interdependencies model.

Canada-United States Action Plan for Critical Infrastructure[3]
"The purpose of the Canada-U.S. Action Plan is to strengthen the safety, security and resiliency of Canada and the United States by establishing a comprehensive cross-border approach to critical infrastructure resilience."

Portfolio Focus
Below are the primary areas of focus for the CI portfolio, each of which has broad-ranging stakeholder interest:

- Identifying and modelling CI dependencies and interdependencies for increased understanding of risk and the cascading effects of failure. CI dependencies and interdependencies are complex, difficult to accurately capture and characterize, and cascading effects are often unknown, yet are essential for assessing risk.
- Improving information sharing among CI stakeholders. The advancement of timely sharing and protection of information among partners is a strategic area under the

[1] Public Safety Canada. National Strategy for Critical Infrastructure. (2009). Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx.
[2] Public Safety Canada. Action Plan for Critical Infrastructure (2014-2017). (2014). Available from: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-eng.aspx.
[3] Public Safety Canada and U.S. Department of Homeland Security. Canada-United States Action Plan for Critical Infrastructure. (2010). Available from: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-eng.aspx.

National Strategy for CI, and is a challenge given the diversity of partners and concerns over sharing and protecting proprietary and sensitive information.

- Understanding the link between cyber security and critical infrastructure. The importance of the link between cyber security and critical infrastructure is a key area, one that has been funded by the CSSP to date in relation to SCADA systems in the energy sector (mainly under the E-security portfolio). The cyber threat to CI continues to grow and represents "one of the biggest threats to security."[1] The interplay between cyber and physical security is becoming increasingly important[2] and is not well understood. This area presents synergies with the E-security portfolio and opportunities to collaborate.

The areas of focus, including current portfolio projects, align with the following priorities identified by the PS-led National Cross-Sector Forum (NCSF): to better anticipate evolving threats and vulnerabilities to critical infrastructure; enhance provincial-territorial and regional engagement in national level critical infrastructure initiatives; support more research and development and move forward on interdependency modelling; better prepare for cyber threats and prioritize the threat vectors in each of the critical infrastructure sectors; and obtain a greater understanding of supply chain dependencies .[3]

PROGRAM OF WORK

The current program of work is described using the CSSP instruments as laid out below.

Call for Proposal (CFP) Projects

The work program of the CIR portfolio currently includes the following projects under the CFP investment instruments:

- Identifying and modelling CI dependencies and interdependencies for increased understanding of risk:
    - Supply Chain Risk Analysis & Management, CSSP-2013-CP-1027 (2014-2017). Led by New Brunswick Department of Public Safety, the goal of this project is to design a CI supply chain risk management framework for the NB energy, food and transportation sectors.
- Improving information sharing among CI stakeholders:
    - Critical Infrastructure Protection – Information Sharing Protocol, CSSP-2013-CP-1026 (2014-2017). Led by New Brunswick Department of Public Safety, the objectives of this project are to understand CI information sharing requirements, legislative and legal constraints, develop an information sharing model and pilot a Commercial-Off-the-Shelf solution.

[1] Statement made during key note speech by Samora Moore, Chief of Cyber Security Officer for the Office of the Under Secretary for Science and Energy in the US, at the US National Symposium on Resilient Critical Infrastructure (NSRCI), Denver, August 2014.
[2] According to Rosemary Wenchel, the DHS Deputy Assistant Secretary for Cyber Security Coordination, DHS plans to merge their cyber security and infrastructure security groups into one. Stated during key note speech at the US NSRCI, Denver, August 2014.
[3] From NCSF Meeting Summary, distributed 11 July 2014 by S. Wong.

- Établissement d'un cadre d'échange d'informations sensibles dédiées aux interdépendances entre les réseaux de telecommunications, CSSP-2014-CP-2004 (2014-2016). Led by Industry Canada and École Polytechnique, the goal of this study is to define a framework for sharing sensitive information to analyse interdependencies between telecommunications networks.

Targeted Investments (TIs)

The work program of the CI portfolio currently includes the following projects under the TI instrument:

- Identifying and modelling CI dependencies and interdependencies for increased understanding of risk:
  - Development of a National CI Interdependency Model, CSSP-2012-TI-1142 (2012-2016). Led by PS and DRDC CSS, the objective of this project is to develop an integrated national CI interdependencies model to support sectors in national CI resilience. This project is aimed at providing insight at the national level.
  - Critical Infrastructure Assessment Tool for Local Governments in Canada, CSSP-2014-TI-2038 (2014-2015). Led by EMBC and the Justice Institute of British Columbia, the goal is to evolve the Critical Infrastructure Assessment Tool and process developed through DRDC pilot projects with EMBC to produce a deployable, sustainable, CI self-assessment tool along with appropriate guidance for local governments in Canada.

Technology Acquisition (TA)

The work program of the CI portfolio currently includes the following projects for capital equipment purchase under the TA investment instrument:

- Understanding the link between cyber security and critical infrastructure:
  - Equipment for Virtualized Training and Technology Assessment for SCADA Systems in the Energy and Utilities Sector, CSSP-2014-TA-2059 (2014-2015).
- Enhancing structural resilience:
  - Furnace Equipment for Resilience Assessment of Critical Cable and Long-Span Bridges, CSSP-2014-TA-2058 (2014-2015).

Community Development (CD) Workshops

Each CSS portfolio hosts community development workshops subject to available funding. For the CI portfolio, planned workshops for the 2014/2015 fiscal year are:

- Identifying and modelling CI dependencies and interdependencies for increased understanding of risk:
  - CI Interdependencies Analysis Workshop. This workshop, intended for early 2015, will be co-hosted by CSS and PS and aims to bring together international

SMEs to discuss challenges and approaches related to CI interdependencies analysis.

- Improving information sharing among CI stakeholders:
    - "Technical Challenges and Solutions for Sharing Sensitive Information for Enhanced Safety and Security" Workshop. In September 2014, the CI and Border & Transportation Security Portfolio Managers co-hosted a workshop to explore challenges and solutions for sharing sensitive information across organizations. This was in response to the recognition of an emerging pattern in various sectors where capability gaps in information sharing have similar technical/governance/policy challenges. The goal of the workshop was to identify how these problems might benefit from a study to capture best practices and leverage work across sectors.

CONCLUSION

The complex nature and challenges of CI dependency/interdependency modelling and analysis, improving information sharing, and understanding cyber security links with CI implies that investments are more likely to generate insight, best practices, and advance the state of knowledge rather than definitively "solve" the problems. Looking ahead, the cyber security component of the portfolio, in conjunction and alignment with the E-security portfolio, should be emphasized.

Annex A

Sector Lead Federal Departments and Agencies

Sector	Federal Department/Agency
Energy and Utilities	Natural Resources Canada
Finance	Finance Canada
Food	Agriculture and Agri-Food Canada
Government	Public Safety Canada Treasury Board Secretariat Privy Council Office
Health	Public Health Agency of Canada
Information and Communication Technology	Industry Canada
Manufacturing	Industry Canada National Defence
Safety	Public Safety Canada
Transportation	Transport Canada
Water	Environment Canada

(Provided by PS CI Directorate)

Annex D Emergency Management Systems and Interoperability

Overview

"From day-to-day incidents to large-scale emergencies, emergency responders are often disadvantaged by the inability to communicate or share critical voice and data information with other jurisdictions or disciplines. This inability to communicate threatens the safety and security of both emergency responders and Canadians"[1]. To a large extent, this statement made 11 years ago remains true today, and addressing this challenging issue is a main driver behind the Emergency Management, Systems and Interoperability (EMSI) Portfolio. Ultimately, "Emergency response agencies, at all levels of government, must have seamless interoperable communications to manage response, establish command and coordination, maintain situational awareness and function within a common operating framework. This will lead to improved response capabilities and provide a more comprehensive approach to disaster management, which will lead to increased safety for all Canadians. Domestically and internationally, Canada has learned firsthand how crucial effective emergency communications are to response and recovery efforts. This lesson was learned during the ice storm of 1998, the response to the Haiti earthquake, and the responseto hurricane Katrina. The more recent experiences of the 2010 Olympic Winter Games and the G8/G20 Summits reinforce the view that interoperable communications are required for the full spectrum of response ranging from local incidents to major events. Equally important are the smaller and more frequent incidents that occur every day in communities across Canada, such as natural and human induced disasters. These events often expose the lack of communications interoperability capabilities and the inability of emergency responders and government leaders to manage response activities and perform essential functions."[2]

To address these capability gaps, the Emergency Management and Systems Interoperability (EMSI) portfolios are focused on enabling communications and technical interoperability. Communications interoperability is defined as "the ability of public safety and service agencies to exchange information within and across jurisdictions via voice, data and/or video transmission in realtime, when needed."[3] and technical interoperability is defined as "The ability to communicate and exchange information and to integrate equipment and technical capabilities"[3]. The primary objective of the portfolios is then to establish activities that transfer knowledge on, or develop the ability to provide evidence-based S&T advice on communications interoperability systems, devices, and related technologies and applications as they relate to safety and security needs. Furthermore, EMSI is focused on capabilities required for complex emergencies defined as "an emergency that is complicated by the involvement of multiple agencies or jurisdictions, by its severity, duration or required resources or by the threat actors or the nature of the target."[3]

[1] Public Safety Radio Communications Project, Final Report, Prepared by RBP Associates and L'ABBE Consulting Services under contract with Industry Canada, March 2003.

[2] Communications Interoperability Strategy for Canada, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/ntrprblt-strtg-eng.pdf.

[3] Emergency Management Vocabulary, http://www.bt-tb.tpsgc-pwgsc.gc.ca/btb.php?lang=eng&cont=1149#c.

1. In support of the primary objective mentioned above, the EMSI Portfolios seek to establish activities that transfer knowledge on, or develop ability to provide evidence-based technical advice on: Interoperable wireless/mobile decision support and communication systems and National implementation(s) of a Public Safety Broadband Network (PSBN).
2. Public Notification and Warning by advancing the National Public Alerting System to ensure that Canadians are aware and prepared of emerging emergency events.
3. National Situational Awareness Systems for the inter-agency information sharing between the emergency services (police, fire, paramedic), provincial/territorial emergency management and federal; agencies that will disseminate information and knowledge toallow organizations to anticipaterequirements and to prepare for emergency events.
4. Information Exchange architectures, standards, and technologies.

The EMSI portfolios include Wireless Technologies, Emergency Management Systems & Disaster Resiliency and Information Integrity and Interoperability (I^3). EMSI portfolios are cross cutting within CSSP and in the wider community. Due to this cross cutting aspect the EMSI portfolio interfaces with the following governance bodies: F/P/T Interoperability Working Group, F/P/T Public Alerting Working Group, Federal Emergency Operations Centre Working Group, Canada/United States Communications Interoperability Working Group and the Canadian Association of Chiefs of Police Information, Communication and Technology Committee. There are a variety of Canadian and U.S. partnering organizations in the EMSI portfolio. These include Public Safety Canada, P/T Emergency Management Organizations, Industry Canada, DND, and the U.S. Department of Homeland Security First Responders Group. Other partners/stakeholders for the portfolio include industrial and academic partners, FirstNet, Paramedics Chiefs of Canada, Canadian Associations of Chiefs of Police, Canadian Association of Fire Chiefs, the Canadian Interoperability Working Group (CITIG), Public Safety Communications Research (PSCR) and the National Public Safety Telecommunications Council in the U.S.

There are also several self-coordinating groups in the community, such as the Federal Emergency Operations Centres Working Groups that include all Federal Emergency Operations Centres and the CA/US Deployables Working Group, the Broadband Working Group and the Cross-Border Working Group (NPSTC).

Policy and Operational Context

A key strategic driver of the portfolios is the Communications Interoperability Strategy for Canada (CISC) which “is a strategic document that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises to promote interoperability voice and data communications” where ”The desired end-state of the CISC is that emergency responders can communicate as needed and as authorized across all levels, on demand.” Furthermore, “In the event of a large-scale complex emergency the CISC promotes the vision of a comprehensive and integrated capability for communications interoperability across Canada and coordinated with United States (U.S.) partners as required” . The CISC governance body is the

Senior Officials Responsible for Emergency Management (SOREM) and a FPT Interoperability Working Group established to focus efforts.

While the scope of the CISC and its action plan are broader than EMSI portfolio objectives, CSS is a key partner in advancing the CISC. Two key CISC focus areas for EMSI are the Public Safety Broadband Network (PSBN) and the Multi-Agency Situational Awareness System (MASAS). The PSBN is the largest public safety communications initiative to ever be considered in Canada. This will provide secure high speed mobile service to first responders and other public safety users and is considered a transformative capability to improve the safety of Canadians. Still within the PSBN, a key consideration of EMSI is the area of deployable systems (DS), as it is unfeasible to provide ubiquitous permanent broadband coverage in remote/isolated areas of Canada. As such, DS are an important tool to bring broadband communications to incidents that occur in such areas with no permanent PSBN coverage. Furthermore, DS can be deployed where PSNB coverage does normally exist but has been compromised or damaged due to a disaster. DS are also important to temporarily augment coverage and/or capacity of the permanent PSBN in locations where special events are expected or unforeseen incidents occur. In the second key area of focus, situational awareness (SA) is essential to the planning and execution of emergency response efforts. Those working in critical environments, like first responders, incident commanders, or emergency managers, are highly dependent on SA information to make decisions and perform their duties. Several different SA tools are used across Canada, and the ability to connect these different tools for shared SA is a critical capability that is needed in order to improve interoperability and ensure a more efficient and effective response. MASAS enables pan-Canadian and Canada/United States interoperability, and is recognized as a leading pilot project that enables communications interoperability among Canada's public safety community.

The Canadian Emergency Management landscape is also a strategic driver of the EMSI portfolio. The Emergency Management Framework states that "Clear communications by appropriate authorities are a critical and continuous process before, during and after an emergency"[1]. With respect to the anticipation, prevention and mitigation components of this framework, wireless systems can be used for advanced warning using wireless sensor networks. Also, the PSBN, Next Generation 911 and Public Alerting/Notification systems are key capabilities for the response to and recovery from emergencies such as natural or man-made disasters, severe accidents, crime and acts of terrorism.

Still within the area of Emergency Management, a key strategic trend is the availability of a wide range of smart mobile devices and the feature rich applications they support. They are the main driver behind the ever increasing demand for capacity in wireless networks. Add to this the expected proliferation of devices brought on by the Internet of Everything (IoE) and the increase in wireless network traffic caused by emerging cloud-based services, and the demand for wireless capacity becomes even greater. This unprecedented growth is expected to continue for many years to come. It is predicted that"…there will be over 10 billion mobile-connected devices by 2018, including machine-to-machine (M2M) modules."[2]

[1] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/mrgnc-mngmnt-frmwrk-eng.pdf.
[2] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

In 2011 the Prime Minister of Canada and the President of the United States issued Beyond the Border: A Shared Vision for Perimeter Security and Economic Competiveness, which is also a key strategic driver for EMSI. This declaration is focused on establishing an improved border perimeter to ensure efficient movement of people and goods. As stated in the action plan Canada and the United States "have the largest bilateral trading relationship in the world, with two-way trade in goods and services of over $700 billion in 2012, supporting millions of jobs in each country" [1]. The EMSI portfolios are focused on CA/US interoperability as a means of harmonizing cross-border emergency communications efforts. To improve response coordination during binational disasters EMSI portfolios are focused on activities that promote the harmonization of the Canadian Multi-Agency Situational Awareness System with the U.S. Integrated Public Alert and Warning System (IPAWS) to enable sharing of alert, warning and incident information to improve response coordination during binational disasters. To support CA/US interoperability, the Canada/U.S. Resiliency Experiment series is focused on Enhancing Trans-Border Resilience in Emergency and Crisis Management through Situational Awareness interoperability. This ongoing experiment series is jointly sponsored by the U.S. Department of Homeland Security's Science and Technology Directorate First Responders Group, the DRDC CSS, and Public Safety Canada. The experiment series is integrating and harmonizing CA/US situational awareness systems and providing evidence[2] [3] that this S&T-based capability facilitates the development of shared situational awareness among the partnering emergency management (EM) organizations, and enhances the planning, coordination and delivery of cross-border responses. With the CAUSE series, the current focus is on emerging capability related to Digital Volunteer Management with social media and PSBN DS.

In the area of cooperation for Cross-border Law Enforcement, one initiative is to "Provide interoperable radio capability for law enforcement actors." Cross-border wireless communication interoperability strategies that can assist in this area are a common LMR channel, communication among distinct LMR systems, LMR to LTE interworking, and PSBN to FirstNet/ PSBN to commercial interoperability.

In the area of Critical Infrastructure and Cyber Security within the strategy, there is an initiative to "protect vital government and critical digital infrastructure of binational importance, and make cyberspace safer for all our citizens" . Canada's PSBN and the U.S.'s FirstNet will both be part of this critical digital infrastructure. In this same area, Intelligent Transportation Systems (ITS) could be used to "mitigate the impacts of disruptions on communities and the economy by managing traffic in the event of an emergency at affected border crossings".

With the emergence of internet protocol systems and PSBN networks the Cyber Security Strategy is another key element. One of the pillars of the Strategy is to "Secure vital cyber systems outside the federal Government"[4]. A prime example of such a vital cyber system is the PSBN initiative that will provide secure high speed mobile service to first responders and other public safety users. Another example is the vast and increasing proliferation of Wi-Fi networks and devices that will require enhancements to the security of their connections to the Internet. In a more general sense, more and more people, devices, sensors in the Internet of Everything (IoE) are

[1] http://actionplan.gc.ca/grfx/psec-scep/pdfs/bap_report-paf_rapport-eng-dec2011.pdf.
[2] CA/US CAUSE II Joint Report http://cradpdf.drdc-rddc.gc.ca/PDFS/unc128/p537613_A1b.pdf.
[3] CA/US CAUSE I Joint Report http://cradpdf.drdc-rddc.gc.ca/PDFS/unc118/p536604_A1b.pdf.
[4] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

connected to cyberspace via wireless technology."Overall, mobile data traffic is expected to grow to 15.9 exabytes per month by 2018, nearly an 11-fold increase over 2013. Mobile data traffic will grow at a CAGR of 61 percent from 2013 to 2018".[1]

While considering the challenges in the above strategies, it becomes evident that the initiatives within the Emergency Management, Systems and Interoperability portfolio are of high importance.

Program of Work

The following are key areas of work. For each, the current program is given as well as themes for the remaining challenges in the area.

Wireless Technologies

On-going projects:

- CSSP-2012-TI-1059- The Communications Interoperability Research Test and Evaluation Centre (CIRTEC) is a wireless test and evaluation facility in the west end of Ottawa for public safety purposes. In essence, it is a 3 cell Long Term Evolution (LTE) network operating in Band 14 (public safety) and covering over 100 km². Its fundamental purpose is to investigate broadband wireless technologies for public safety use, ensure interoperability and assess application and device performance. By doing so on a real network, the risks of introducing new communications technologies for mission-critical activities to assist public safety organizations can be mitigated.
- PSTP-2011-3782-PSBN Technical Advisory Group is focused on developing the network architecture for a national, interoperable, resilient, secure and cost-efficient Public Safety Broadband Network (including interfaces with legacy Land Mobile Radio systems). This includes defining operational, security and interoperability requirements.
- CSSP-2013-CP-1021- The Field Operational Test Facility for Next Generation Interoperable Mission-Critical Communications explores the use of in-field deployable public safety broadband wireless technology, targeting specifically disasters and incidents where conventional communications infrastructures are either damaged, non-existent or do not meet the required capacity needs. This project will build on the Simon Fraser University Telematics Research Lab's (SFU) expertise in developing mission critical networks for extreme environments, including the Canadian High Arctic.
- CSSP-2014-TI-2085- The Canada - U.S. Enhanced Resiliency Experiment (CAUSE) III includes a western scenario focused on wireless communications. The capabilities of both Land Mobile Radio (LMR) and deployable Long Term Evolution (LTE) technologies (PSBN) will be demonstrated along the borders of Alberta, Saskatchewan and Montana, with an emphasis on interoperability. Increased community resilience during the response to a widespread wildfire will be appraised and measured.

Remaining gaps:

- Conducting a PSBN pilot based on a limited leave-behind deployment is critical to the successful implementation of an eventual nationwide PSBN network in Canada. EMSI will need to play a key role in this initiative. Self-Organizing Networks (SON) and Dynamic Prioritization (DP) will both be key areas of investigation.

[1] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

- Determine how deployable systems (DS) can be used to rapidly provide broadband communication capabilities to first responders during planned and un-planned incidents.
- Investigate the use heterogeneous networks to augment public safety broadband capability. This includes the integration of or interfacing with emerging Wi-Fi technologies on the PSBN as well as all other upcoming wireless offloading technologies i.e. small cells.
- The notion of the Internet of Things (IoT) is of significant importance to the public safety community. Adding machine-to-machine and sensor network capabilities to their communications arsenal will enhance first responder's capability to anticipate, respond to and recover from incidents.
- The PSBN will enable a wide variety of uses and support for devices (smart phones, tablets, laptops) that is significantly more diverse than the LMR public safety communication ecosystem. Is it important to know what type of devices will be on the PSBN and their expected uses.
- Network sharing techniques: Sharing networks between commercial users and public safety users is considered to be the most promising way to achieve cost efficiencies for the PSBN. FirstNet has publicly stated its desire to share under-utilized spectrum with non-public safety users. There is currently little development in this area.
- Body-worn cameras, vital signs monitors, and other sensors are expected to emerge in the near future as important tools for first responders. It will be important to examine how the information collected by the sensors can be integrated within a Personal Area Network and then carried over the PSBN.

Emergency Management Systems

On-going projects:

- CSSP-2014-CP-2006: Wireless Public Alerting Service (WPAS) development of a pilot Wireless Public Alerting Service that will provide an end-to-end Service validated in a Canadian community and advancement of standards and specifications for wireless alerting.
- CSSP-2013-CP-1018: INTERSECT Situational Awareness Network is focused on enhancing all-hazard situational awareness in the National Capital Region amongst emergency first responders and emergency management partners.
- CSSP-2012-TI 1061: MASAS focused on developing and transitioning a national information exchange capability of situational awareness information of emergencies for the emergency services and emergency management sectors.
- CSSP-2013-TI-1033: Improving End-To-End Tsunami Warning for Risk Reduction on Canada's West Coast to support long-term development of sustainable, reliable and integrated West Coast Canadian end-to-end public warning and emergency communication systems.
- CSSP-2014-TI-2085: Canada/ U.S. Enhanced Resiliency Experiment (CAUSE) – Social Media for Emergency Management, CA/US Alerts/Notifications.
- CSSP-2014-TI-2024: Next Generation 911 Online Simulator to provide access to technology on NG911 so as to facilitate public safety community self-assessment of the implications of this emerging disruptive technology.

Remaining challenges:

- Enhanced Situational Awareness of Emergencies through the fusion of social media information, near real time analysis and reporting. Furthermore, there is a need for

national architecture focused on next-generation situational awareness systems that would consider PSBN, NG 911, Public Alerting and Notification Systems.
- While the Wireless Public Alerting Service project will pilot wireless public alerting and provide key technical standards, policy and coordination work is required to ensure this capability will become part of the National Public Alerting System.
- NG911 services will be launched in Canada. The architecture for NG911 should consider the interfaces to the PSBN and other networks that NG911 is expected to touch.
- Modern buildings and underground structures strongly attenuate wireless signals. When first responders enter these structures it is desirable that they be able to access their information networks. Define use-cases for in-building wireless communications, including how to provide in-building communications inside LEEDS buildings and deep structures when there is no power.
- Disorientation in a smoky burning building is a significant risk to fire fighters. The ability to locate them in 3 dimensions would assist the incident commander to guide the fire fighters to exits or targets, or to help extricate them in case of trouble.

Information Integrity and Interoperability (I^3)

On-going projects:

- PSTP-2011-3782-PSBN Technical Advisory Group: The PSBN Technology Advisory Group has been developing recommendations for the architecture, interoperability and security of LTE-based wireless communications infrastructure for first responders. Since this infrastructure is meant to allow all first responders to communicate amongst themselves as well as access their own organisational information resource, there is a strong requirement for an ICAM capability. The interoperability requirements for the PSBN contains a chapter on ICAM.
- CSSP-2013-TI-1046 CBSA Secure Data Exchange: The objective is to look at the feasibility of introducing multi-caveat data protection capabilities into an operational environment to secure sensitive information in a multi-agency context.

Remaining challenges:

- While technologies exist to manage access to information, they generally implement access control to services rather than to information assets proper (i.e. controlled access to a file server as opposed to files). This requires better understanding of information asset labelling and more sophisticated access control mechanisms based on user credentials.
- Identity, Credential and Access Management (ICAM) is the centre piece of user identity and credential management. In order to implement access management based on these information sources, organisational requirements must be derived from the business requirements and activities that are carried out by organisations having more complex requirement with respect to access to any resource. ICAM is not a well understood concept. It goes beyond simply accessing IT infrastructure, services and data assets, it is also about using the same credentialing capabilities to mange access to other resources, including buildings, conference rooms, other facilities and even stand-alone items such as vehicles. It is the integrations on multiple services that leads to the implementation of an ICAM capability. In the context of the PSBN ICAM is a capability that is required to manage quality of service parameters as well as to manage access to services and information that can be made available by multiple agencies. For a system like MASAS,

for example, some of the services provided by ICAM could allow sensitive information to also be shared with the users holding the required credentials.

- National Information Exchange Model (NIEM) is designed to bridge the information gap between systems, facilitating the flow of knowledge and enabling faster, more effective cooperation between two or more organizations. In 2011, on the recommendation of the Informatics sub-committee, CACP endorsed NIEM for use within the Canadian Law Enforcement community. In the US, many organisations are adopting NIEM as an information exchange framework. This framework allows organisations to define information exchange structures that define vocabularies and semantics to be used when exchanging information. Additionally, this framework was designed to support information exchange across the Canada/US border. While the US has developed many NIEM-based specifications and have implemented exchange protocols, Canada remains far behind in the development of specifications, the deployment of protocols and in standardized cross-border information exchange.
- Confidentiality and integrity are two of the most important requirements when dealing with information that is used in decision support circumstances. Police officers must be able to justify decisions made while responding to emergency events. There is a requirement for information management systems that support the guaranty of the integrity of information (i.e. non-repudiation). Additionally, there are circumstances where the same information must remain confidential. There remains a significant amount of work to develop systems that integrate these capabilities in a seamless manner.

Annex E E-security

Overview

The E-security portfolio's primary objective is to support the E-security aspects of Critical Infrastructure Protection as defined by Public Safety and the Canadian Cyber Security Strategy. Critical infrastructure consists of the essential systems and facilities underlying our society and consists of physical assets, digital assets contained within the cyberspace defined by computers and networks, services that are provided through them and other assets essential to the health, safety, security and economic well-being of Canadians. E-security may be defined as a level of confidence provided through a variety of means to protect digital information residing and moving within networked digital systems from either physical attack of the infrastructure or cyber-attack of the digital information itself[1].

Through initial interdepartmental working groups and the Cyber Community of Practice (Cop) it focusses to bring together cross-domain subject matter experts from government, industry and academia to gain better understanding of the various mandates relating to cyber security. Assess required cyber security capabilities, identify gaps that need strengthening; and identify the niche areas that should be targeted for maximum influence on outcomes that matter to Canadians with the resources available while maintaining alignment with priorities and ensuring that outputs get used by related clients, adding value to their organization.

Key partners include other federal government departments and agencies (NRCan, NRC, RCMP, CSIS, Industry Canada, Public Safety Canada, CRTC, DND, DFATD, DRDC); provincial governments (British Columbia, Ontario, Quebec); academia (Carleton University, Dalhousie, University New Brunswick, University of Victoria, École Polytechnique, University of Waterloo, British Columbia Institute of Technology); industry (banking, telecommunications, and energy and utilities companies) and international partners (United States, United Kingdom, Australia, Sweden).

Influences and Drivers for Change

The key driver for change in this area is the realization that national digital infrastructure and the valuable data it contains are under increasing risk through targeted cyber-attacks. The E-security Community is influenced and focused by the following national and bi-national strategies and action plans[2]:

1. The National Strategy for Critical Infrastructure (Public Safety Canada, 2009),
2. The Action Plan for Critical Infrastructure (Public Safety Canada, 2009),
3. The National Cyber Security Strategy (Public Safety Canada, 2010) and
4. The Canada US Cybersecurity Action Plan (Public Safety Canada and the US Department of Homeland Security, 2012).

[1] Canadian Defense and Foreign Affairs report outlining a comprehensive approach for Canada in CyberSpace, http://www.cdfai.org/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf.
[2] Public safety Canada specifies these as related to National Strategies, http://www.publicsafety.gc.ca/cnt/bt/index-eng.aspx#.

Op Capabilities supported by the Community

In an effort to achieve the related goals of CSSP program to contribute to closing some of the identified gaps associated on the cyber front, the E-security Community is fully aware of the 3 pillars that have been defined for Canada's Cyber strategy & mandates which are:

1) Securing Government systems;
2) Partnering to secure vital cyber systems outside the federal Government; and
3) Helping Canadians remain secure on-line.

The principal collaborators within the E-security Community are:

- Public Safety Canada (PS Canada)
- The Royal Canadian Mounted Police (RCMP)
- Industry Canada (IC)
- Natural Resources Canada (NRCan)
- National energy Board (NEC)
- CIP Energy Sector (Oil, Gas and Hydro)
- Banking Sector (Banking, Trusts, Bank of Canada)
- Bell Canada
- British Columbia Institute of Technology (BCIT)
- Ontario Hydro
- Quebec Hydro
- Canadian Radio/Telecommunications Commission (CRTC)
- Canadian Security Intelligence Service (CSIS)
- The Department of National Defence (DND) / Defence Research and Development Canada (DRDC) Ottawa, Valcartier and the Centre for Operational Research and Analysis (CORA)
- The University of Ottawa
- École Polytechnique de Montréal
- ThinkRF
- Solana Networks

Policy and Operational Context

As stated above, the principal strategic policy drivers in the Cyber Security portfolio is the *National Cyber Security Strategy (CSSP)*; The CSSP E-security mainly focusses on supporting pillars **two** and **three**.
The key driver for investment in this area is:

a) Realization that National Digital Infrastructure and the valuable data it contains are under increasing risk through targeted cyber-attacks.
b) CSSP investments enable DRDC, CSS to coordinate and support projects and activities that respond to Canadian public safety and security priorities and address capability gaps.
c) The CSSP Cyber Security program is influenced by the following national and bi-national strategies and action plans:
    1 The National Strategy for Critical Infrastructure (Public Safety Canada, 2009),
    2 The Action Plan for Critical Infrastructure (Public Safety Canada, 2009),
    3 The National Cyber Security Strategy (Public Safety Canada, 2010) and
    4 The Canada US Cybersecurity Action Plan (Public Safety Canada and the US Department of Homeland Security, 2012).

Therefore in support of the **second** pillar, the CSSP is partnering with the owners and operators of Canada's digital infrastructure in the telecommunications and energy and utilities sectors. As a result of technological innovation in telecommunications structures and the evolution of Smart Grid Technologies in power generation, distribution, and consumption, Canada's telecommunications and energy and utilities firms are facing a fast-evolving threat environment[1].
The E-security Portfolio functions to fulfill the mandate that the CSSP follows. It coordinates and supports projects and activities that respond to Canadian public safety and security priorities and addresses capability gaps. Ultimately, these efforts contribute to achieving the CSSP's primary strategic goal of ensuring that Canada's people and institutions have a greater resilience to global and domestic public safety and security threats and hazards.

Program of Work

In the telecommunications and energy and utilities sectors, the CSSP aims to identify the relevant cyber security needs/requirements in these areas, provide targeted knowledge generation, dissemination, and application, as well as technology development. The CSSP also provides assessments of changes in the effectiveness of protective measures and the resiliency of private sector networks. In addition, the CSSP provides an evidence-based decision-support mechanism by gathering, analyzing, and disseminating information on security threats, vulnerabilities, and incident vectors, this provides the basis to invest in projects that provide countermeasures, and best practices to help inform private sector cyber security decisions and subsequent actions.
Sandbox-(knowledge disseminating):
Various dissemination techniques were analyzed and it was determined that the best mechanism would be to build 'Sandboxes, a testing environment that isolates untested changes and outright experimentation from the production environment or repository' Additionally, The 'Sandbox'

[1] A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative: http://bipartisanpolicy.org/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf.

provides a tightly controlled set of resources for members to build out cyber-defense capabilities that can be equally used by all members, as well as provide a partnering mechanism that remains neutral. One of the main provisions of the 'Sandbox' required it to remain neutrally owned and operated thereby giving equal weight to all its members. The formulation developed was established as:

- The 'Sandbox' must be refined and obstacles removed. This is a ongoing process.
- Concurrently CSSP cyber funded projects are aligned under the appropriate 'Sandbox'
- Governance structures and advisory groups must be formed to provide a basis to disseminate the information.
- The way forward to self-sustainability must be developed for each Sandbox
- This mechanism must be leveraged to capture new unknown cyber challenges
- New emerging challenges must be documented and used as a basis for the CSSP's Call for Proposals

The extent of the emerging threat relates to the advent of the Bitcoin, a universal payment system. We have everything we need within our Personal Digital Devices to pay for everything, but a universal payments system with no friction or interchange costs disrupts the whole monetary system.

Beyond fostering collaborative relationships, the objective of this work is to better understand the problem space in which Canada's telecommunications and energy and utilities firms operate. The ultimate goal is to have each sector gradually assume greater ownership of the problem. The study phase provides the outputs followed by the dissemination of the untapped complex challenges still existing. With the completion of this, the focus has now shifted to developing solutions for these challenges and implementation these solutions into a 'Sandbox'. With the 'Sandbox' objective in place, the build-out for each one is now evolving. Ultimately, the objective is that these 'Sandboxes' are to become self-sustaining and perpetually effective. Project 31x (03-431eSEC) Industrial Control Sector (ICS) and Supervisory Control and Data Acquisition (SCADA) Network Security and Network architecture analysis, assessment and evaluation, provided the groundwork for an entity that housed within an environment a provision for law enforcement, Natural Resources Canada, and academia to collaborate with the private sector. The capability that was developed provided the community ability to do analysis of vulnerabilities in SCADA and Smart Grid in a national and International Environment.

In the financial sector, the CSSP is focused on providing innovative methods to identify and mitigate cyber threats and to facilitate public/private sharing of protected information, as well as the development of scenarios and case studies of safer and riskier online behaviours in order to better inform the general population. E-security Project currently providing building this out is the Targeted Investment piloting a National Cyber and Forensics Training Alliance (NCFTA) adding Canada as a stakeholder to a multi country endeavour.

As in the telecommunications and energy and utilities sectors, the fundamental challenge in the financial sector is getting firms to work together to address common problems. The CSSP's objective is to facilitate that process through projects that seek to define the relevant problem space and set priorities for the sector going forward.

Annex F Explosives

Introduction

The Explosives Portfolio works toward addressing critical gaps in Canada's capability to effectively Prevent, Detect, Deny, and Response to threats and attacks involving explosives. Specific S&T areas addressed by the portfolio include understanding the fundamentals of explosives formulation techniques and blast effects, existing and novel techniques for explosives detection, improvised explosives device defeat techniques (including post blast analyses), explosives threat forecasting, and sustainment of capabilities associated with these activities (support to explosives exercises and training for first responders and scientific support). Ultimately, these activities will positively impact the national capability for prevention of terrorist activities involving explosives, the timely detection of such activities, denying the means and opportunity to carry out such activities, and response to and mitigation of the effects of terrorism involving explosives.

The explosives portfolio has a number of key partners across the Canadian federal government, all of whom are engaged in work related to explosives threats as part of their core departmental mandates. These include the RCMP, CAF/DND and DRDC, CSIS, NRCan, CBSA, Public Safety Canada, Transport Canada, and D FAT D. Annex A provides an overview of each of their roles and mandates related to explosive threat issues. In addition, provincial and municipal law enforcement agencies and forensic laboratories regularly partner on portfolio efforts. Active collaboration with allied governments also occurs regularly, particularly with the US (CTTSO and DHS), the UK (CPNI) and Australia (DSTO).

The explosives portfolio has a regular and robust engagement strategy led primarily through the explosives community of practice (CoP). The CoP holds monthly teleconferences to discuss progress on on-going activities and to discuss new issues as they arise. They also hold twice-yearly face-to-face meetings to discuss gaps and strategic direction for the portfolio. In addition to the CoP activities, the portfolio manager is engaged in the Canadian Explosives Technicians Association (CETA) and regularly engages with the US Technical Support Working Group (TSWG) efforts related to explosives.

Policy and Operational Context

Canada's counter-terrorism strategy[1] provides the framework to counter domestic and international terrorism in order to protect Canada, Canadians and Canadian interests. Within this strategy, violent Islamist extremism is identified as the leading threat to Canada's national security, with several Islamist extremist groups having identified Canada as a legitimate target. Given that explosives are a key vector used by these groups to inflict terror, the objectives of the strategy are paramount to guiding the strategic direction of the explosives portfolio. Building resilience is the strategy's core principle, which operates through four pillars: Prevent, Detect, Deny, and Respond. These elements map very well with the activities of the explosives portfolio and can be used as a metric against which to assess the balance of investment within the portfolio.

[1] Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-eng.aspx) .

Another key strategy that drives the work of the explosives portfolio is the Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy for Canada[1]. The purpose of the strategy is to enhance and sustain Canada's resilience to Chemical, Biological, Radiation, Nuclear, Explosives (CBRNE) terrorist events by providing the policy framework to guide the creation and maintenance of sustainable capabilities and common standards in CBRNE policies, programs, equipment and training. The CBRNE Resilience Strategy is framed against the four components of emergency management of prevention/mitigation, preparedness, response, and recovery, which align with those of the Counter-terrorism strategy mentioned above. The strategy identifies five strategic objectives that are considered core to developing CBRNE resilience, with specific action items identified to achieve these objectives, all of which help guide the work and direction of the Explosives Portfolio.

The National Strategy for Critical Infrastructure[2] and supporting Action Plan establish a collaborative approach for federal, provincial, territorial and critical infrastructure sectors to strengthen critical infrastructure resiliency. Because most terrorist attacks involving explosives target infrastructure as well as people, the explosives portfolio considers this strategy in defining the targets and implications of terrorist activities involving explosives. In a similar fashion, the Beyond the Border declaration[3] is also of interest to the portfolio, particularly in regards to its efforts in enhancing joint integrated threat assessments and info sharing, reporting on deployment of new explosives screening technologies, and efforts to establish binational CBRNE emergency response plans and capabilities.

Understanding the emerging threat environment is key to ensuring that the explosives portfolio remains relevant and effective. To that end, the explosives portfolio is privy to classified threat assessments prepared by the law enforcement, intelligence communities and international partners on a regular basis that describe the explosives threat to Canada, Canadians and its allies. In addition, Public Safety publishes a yearly overview of the terrorist threat to Canada, which deals in part with explosive threats[4]. The longer standing threat of the 'bomb-in-a-box' scenario for air travel[5] concerns both the explosives and border and transportation security (BTS) portfolios. All of these documents provide context to the strategic direction of the explosives portfolio, while also identifying specific vulnerabilities and risks to support future portfolio S&T investment decisions.

In addition to the high-level strategies and specific threat assessments related to explosives threats, the portfolio is involved in several working groups engaged in assessing technologies, techniques and emerging issues. The US Counterterrorism Technology Support Office (CTTSO) hosts a yearly meeting with partners to share the explosives threat world picture and discuss new way of preventing, detecting and neutralizing novel homemade explosives formulations. Within Canada, the Explosives Safety and Protection Working Group, chaired by the RCMP, also meet regularly to discuss explosives safety issues of relevance to responder and security personnel.

---

[1] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg/index-eng.aspx.
[2] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx.
[3] http://www.publicsafety.gc.ca/cnt/brdr-strtgs/bynd-th-brdr/index-eng.aspx.
[4] 2014 Public Report on the Terrorist Threat to Canada (http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2014-pblc-rpr-trrrst-thrt/index-eng.aspx) .
[5] See the Government of Canada Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rspns-cmmssn /rspns-cmmssn-eng.pdf.

From an air security perspective, Transport Canada chairs an Air Transport threat evaluation working group with participation from several CoP members that consider novel ways of inflicting harm (mainly using explosives) to the Air Transportation sector.

Program of Work

Using inputs such as threat assessments described above, the Explosives Portfolio has established a series of realistic scenarios describing threats that could potentially be used against Canada and Canadians (and which have already occurred in Western society). These scenarios, listed below, help frame portfolio investment priority setting and decisions. By analysing these scenarios for their technical feasibility and potential impact, it is possible to prioritize the most pressing scenes and to evaluate the effort needed to mitigate the potential impact.

- Letter/small package bomb at a commercial office building (including government building) which target people;
- Vehicle-Borne Improvised Explosives Device attack of a 1000kg or less against people and-or infrastructure in an urban gathering ;
- Suicide bomber on a bus or train targeting people (with a device of 25kg or less);
- Explosive package comprising a few kg on a plane i.e. target the air transportation industry:
- Use of smaller vessel carrying over 1000kg of explosive to attack a ship (cruise or others)
- Ship-borne explosives used to attack a port that could be over 20,000kg;
- Large explosives device used to attack critical infrastructure like bridge or tunnel.

Consideration of necessary national capabilities for effective prevention, preparedness, and response to each of these scenarios along with an assessment of existing capabilities provides insight into gaps that require some degree of investment. Those gaps that require a scientific or technical solution are in the interest of the portfolio and are considered together with an assessment of the current threat picture and an assessment of previous related investments. The following provides a picture of the current and planned program of work within the cluster focused on prevention, preparedness and response, as well as remaining challenge areas for each.

Prevention

- Current projects:
    - CSSP-2013-CP-1015: Enhanced Detection of Contraband in Cargo Containers by Vapour Sampling.
    - CSSP-2014-CP-2011: Development of Blast Resistant Window Anchor Systems.
    - CSSP-2014-CP-2013: MTKDG2 (Classified project).
    - CSSP-2014-TI-2034: Electronic Countermeasures (ECM) Techniques for Public Security Applications.

- Activities for 2014/15:
    - On-going ECM efforts in collaboration with the US
- Remaining challenge areas:
    - Technologies for tracking and forecasting threats that involve explosives

- Methods to secure vital infrastructure against explosive threats

Preparedness

- Current projects:
  - CRTI 07-0153RD: Consolidated Assessment of Threats for the Transport of Combustible Liquid/Gaseous Fuels (FAE)
  - CSSP-2013-CP-1001: Rapid City Planner for Extreme Events
  - CSSP-2014-CP-2012: Homemade explosives (HME) All Hazards Training
  - CSSP-2014-TI-2034: Scientific and Technical Support to RCMP National Protective Operations
- Activities for 2014/15:
  - S&T exercises in support of training in explosives, including post-blast evidence gathering for investigative purposes
  - Understanding the blast effects of explosive threats in Urban Environments including effects on historic masonry. This was brought to the forefront by the attempt of the Toronto 18 group to position a Large Vehicle Bomb Improvised Explosives device near Canada's Parliament Buildings.
- Remaining challenge areas:
  - Detection and characterization of novel Home Made Explosives (HME) so first responders can properly handle and dispose of devices containing HME.
  - Development of HME simulant materials to support safe detection training to front line personnel (border and airport).

Response

- Current projects:
  - CRTI 08-0142RD: Immersive haptic tele-robotic system for improvised explosive device disposal
  - CRTI 09-0531TD: Improvised Explosives Assessment Tool Enhancement and Deployment
  - CSSP-2012-TI-1098: Noise-Flash-Distraction-Device (Flash Bang) Technical Evaluation
- Activities for 2014/15:
  - Protocols for characterizing and testing Improvised Explosives (HME), modeling blast effects in urban environments, and testing detection equipment
- Remaining challenge areas:
  - Development of improved Improvised Explosives Device (IED) Defeat and Render Safe procedures (e.i., device construction, neutralization and mitigation techniques), including development of tools and equipment for defeating Improvised Explosives Devices

Annex: Explosives Partners

- PS Canada – domestic security and public safety, CIP
- CF / DND – military operations (international and domestic support)
- DRDC – provides explosives S&T support to the CF, DND and PS Canada
- CSIS – investigation of terrorist attacks conducted with a “political motivation”
- RCMP – investigation of suspected terrorist (explosives) incident
- NRCan –legislative framework for the fabrication and use of explosives in Canada
- CBSA – interdiction of inadmissible goods (and people) at the ports of entry
- TC – maintenance of a transportation system that protects Canadians by developing and enforcing transportation security regulations
- DFAIT – coordination and development of the Canadian position on counter Terrorism to the international community
- Provincial/Municipal Law Enforcement – protection of the public from terrorism act
- Provincial forensic Labs – timely analysis of forensic evidence to support provincial/municipal law enforcement
- International Government Organizations including CTTSO (US), CPNI (UK) and DSTO (AUS)

This page intentionally left blank.

Annex G Fire Services

Overview

The Fire Services portfolio has two primary objectives. The first is to develop Science and Technology (S&T) solutions that meet national Fire services requirements and fit within the scope of the CSSP program. The second is to inform decisions pertaining to Fire Service operations and policy through proactive dissemination and sharing of S&T information and knowledge that is relevant to stakeholders within and external to the fire community. To achieve these objectives, the portfolio performs the following primary functions[1]:

- **Identify** operational and/or policy gaps that warrant research, investigation, scientific analysis, or the building of collaborative networks to develop solutions;
- **Prioritize** the operational and/or policy gaps through an analysis that aligns the needs of the fire services within the scope of the annual CSSP Planning process and associated investment instruments.
- **Influence** the development and implementation of solutions to the operational/policy gaps that are relevant to the community and meet operational and/or policy requirements within the scope of the project charter;
- **Disseminate/Transition** the program outputs to the national stakeholders to ensure the full potential of the new knowledge or technology is realized; and
- **Assess** the impact of Program outputs upon the community, in line with CSSP established values and metrics. Use the assessment results to inform future planning.

The Fire Service portfolio engages the Canadian Association of Fire Chiefs (CAFC), Canadian Association of Fire Chiefs (CAFC), and the Council of Canadian Fire Marshals and Fire Commissioners (CCFMFC). CAFC is an independent, non-profit organization with a voluntary membership. It's the national public service association dedicated to reducing the loss of life and property from fire. They also play a role in advancing science and technology for the Fire and Emergency Services and represent fire services management across the country. CCFMFC is a 15-member council formed in 1921 and consists of the senior fire officials (Fire Marshall or Fire Commissioner) of each province and territory along with the Department of National Defence. Some board members are also members of the Senior Officials Responsible for Emergency (SOREM). The Fire Services Portfolio also engages with the Ministère de la Sécurité Publique Québec, the National Research Council (NRC), Underwriters Laboratories Canada (ULC), the National Fire Protection Association (NFPA), the Canadian Interagency Forest Fire Center (CIFFC), Mine & Industry Firefighting (Vale), the First Nations Emergency Services Society (FNESS - BC), Labour – International Association of Firefighters (IAFF), and the Canadian Volunteer Fire Services Association (CVFSA).

To enable knowledge sharing within the community and to provide strategic advice to DRDC CSS, the Fire Services Community of Practice (CoP) was created to engage with multiple

[1] As per the DRDC Centre for Security Science: Organizational Roles, Responsibilities and Accountabilities (2013).

organizations within the fire domain. Membership represents a broad spectrum of organizations that are vital to informing the future of the Fire services in Canada. These include members from national associations, research organizations, as well as private sector, academic, media, and standards development organizations.

Policy and Operational Context

The Fire portfolio's policy and legislative oversight includes a variety of statutes which encompass all jurisdictions. The Canadian Labour Code, guiding document for the development of the Canada Occupational Health and Safety Regulations, provides guidance on the operation of fire services and fire safety regulations. The National Building Code of Canada, guiding document for the National Fire Code of Canada, provides direction and guidance on all issues relating to occupational safety. The US National Fire Protection Association (NFPA) standards [1]were developed to address all matters relating to fire safety and fire service operations. They've been adopted across most jurisdictions in Canada, as no Canadian standards exist. From these documents, the provincial and territorial fire codes/response plans were established and tailored to suit specific regions.

The fire service also has a variety of legislative responsibility at the federal level, which include federal lands and infrastructure (i.e. DND, federal parkland and First Nations reserves). For example, we have five federal departments holding fire safety responsibilities with First Nations communities, through Aboriginal Affairs and Northern Development Canada who administer funding agreements for fire protection services[2]. Additionally, at least nine federal agencies have mandates which focus on aspects of wildfire, through various Acts and policy oversight.[3]

Guiding strategies, policies and plans:

- **Transportation of Dangerous Goods Act**[4] sets out the rules and regulations regarding the safe and effective transportation of dangerous goods and the requirements for the continued development and use of CANUTEC operated by the Transport Canada (TC) which enables responders to effectively respond to incidents involving transportation modalities. Additionally, TC provides guidance and planning for the response to transportation emergencies such as rail incidents. Currently, CSS is providing S&T guidance to TC and their Emergency Response Task Force regarding the transportation of crude oil by rail.
- **Federal Emergency Response Plan**[5]identifies the areas of risk that all areas of Canada must be able to respond to including the traditional spectrum of natural and human-induced hazards: wildland and urban interface fires, floods, oil spills, the release of hazardous materials, transportation accidents, earthquakes, hurricanes, tornadoes,

[1] National Fire Protection Association Standards http://www.nfpa.org/.
[2] First Nations Fire Protection Strategy: http://www.aadnc-aandc.gc.ca/eng/1317308114314/1317308317352.
[3] Canadian Wildland Fire Strategy: Background Syntheses, Analyses, and Perspectives http://www.ccfm.org/pdf/cwfs_analysis_en_web.pdf.
[4] Transportation of Dangerous Goods Act https://www.tc.gc.ca/eng/acts-regulations/acts-1992c34.
[5] Federal Emergency Response Plan http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-eng.aspx.

health or public health disorders, disease outbreaks or pandemics, major power outages, cyber incidents, and terrorism. The response capabilities of all fire services across Canada directly support these objectives.

- **Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Resilience Strategy for Canada**[1] promotes the vision of an integrated capability across Canada by framing a scalable, responsive, dynamic, sustainable and evidence-based approach for all contributors to CBRNE events. This approach is equally based on the four components of Emergency Management: prevention / mitigation, preparedness, response and recovery. Canadian Fire Services in many communities are the lead organizations for emergency management activities or provide assistance in all of these areas, in line with key portfolio priorities.
- **Communications Interoperability Strategy for Canada (CISC)**[2]is a strategic document that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises to promote interoperable voice and data communications. "The desired end-state of the CISC is that emergency responders can communicate as needed and as authorized across all levels, on demand." The CISC governance body is SOREM and FPT Interoperability Working Group was established to focus efforts. The Fire Community is a key stakeholder in the CISC. CSSP's EMSI Portfolio is focused on supporting initiatives related to CISC. Specific areas of focus include the Public Safety Broadband Network (PSBN) and the Multi-Agency Situational Awareness System (MASAS).

To further understand the Fire Services Science and Technology requirements a document titled "Report on Intermediate Science and Technology Priorities of Canadian Fire Services"[3] was published by DRDC. Its focus was to identify and validate a list of current priorities or issues which resonate throughout the Fire community. Through analysis of the gaps in policy and operations, identified through a broad and proactive engagement across the portfolio stakeholders, the Fire Services Portfolio has identified three key categories that will serve as priority domains over the following three to five year cycle. These include:

Evidence-Based Decision Making

One of the key issues relates to the transition of fire services towards evidence based decision-making and policy development. Gaps in this regard are linked to the shortage of national level information on fire statistics. This was highlighted in the National Fire Database Report, where it states that the" collection of fire statistics can contribute to a reduction in the incidence of fire and related death, injury and damage, and ensuring the safety of the public through civil protection"[4] Establishing national level information on fire statistics will enable the building of sustainable fire services for the future by improving the ability of communities to continue to financially support their current models of providing fire protection services or develop new more efficient and effective models. Another key aspect of evidence-based decision

[1] CBRNE Resilience Strategy for Canada, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg/index-eng.aspx.
[2] CISC, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-eng.aspx.
[3] DRDC CSS CR 2013-049, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p538428_A1b.pdf.
[4] National Fire Database Report, University of Fraser Valley.

making is the use of Risk-based methodologies and models. This is key for improve decisions making in the areas of fire threats, logistics and dispatch.

Dangerous/Hazardous Goods

The Transportation of Dangerous goods is an essential part of the Canadian economy and supply chain. Specifically in the relation to Crude Oil rail has become a key transportation mechanism. "Information from the Railway Association of Canada (RAC) indicates that shipments of crude by rail have risen exponentially in recent years. In 2009, Class I railways moved only 500 carloads of crude, while current estimates are in the range of 130,000–140,000 carloads per year. With an estimated average of 600 barrels per carload, that amounts to about 230,000 barrels per day. The continuing development of these oil reserves is expected to result in an even greater volume of crude oil being transported by rail in future years." [1] The tragedy at Lac Megantic of the Derailment and Fire has focused attention on this sector. Transport Canada has established the Emergency Response Task Force which is identifying and creating mitigation, preparedness and response plans for the transportation of crude oil by rail. A key gap identified by the by the Transport Canada ERAP WORKING GROUP "identified the lack of data as a serious constraint in providing detailed risk analysis and recommendations for addressing specific gaps in response capacities at any given community in Canada." [2] Specific to the Fire Services Portfolio is to enable the development of a standardized list of resources and enable the information sharing of existing inventories of equipment and supplies for flammable liquid firefighting.

Smart Fire Fighting

A key emerging domain in the Fire Community is the concept of Smart Fire Fighting which is focused on using Research and Development to enable improved Fire Response. A recent report from the National Institute of Standards and Technology on Smart Fire Fighting highlighted that "The "smart firefighting" of tomorrow is envisioned as fully processing collected information and transmitting germane information in a timely manner to improve the safety and functionality of every firefighter." To enable Smart Fire Fighting Science and Technology investments are key. As stated in the report there are "New opportunities to fuse emerging sensor and computing technologies with building control systems and firefighting equipment and apparatus are emerging. The resulting cyber-physical systems will revolutionize firefighting by collecting data globally, processing the information centrally, and distributing the results locally."[3] Key areas to enable Smart Fire Fighting include real/time information of the fire situation (e.g., video, sensors), wireless wearable environmental sensor, people tracking, and asset tracking. To enable Smart Fighting a key foundational element is the planned Public Safety Broadband Network (PSBN). The PSBN is the largest public safety communications initiative to ever be considered in Canada. This will provide secure high speed mobile service to first responders and other public safety users and is considered a transformative capability to improve the safety of Canadians. To enable Smart Fighting Standards and Specifications will also be key including in the area of data integration, educational curriculums and information exchange.

Program of Work

1 http://www.tc.gc.ca/media/documents/tdg-eng/5807-2014-3477-F-BT8821720-ERAP-WG-Report-and-Recommendations-FINAL-21-en-rev-AAA-rev.pdf.
2 http://www.tc.gc.ca/media/documents/tdg-eng/5807-2014-3477-F-BT8821720-ERAP-WG-Report-and-Recommendations-FINAL-21-en-rev-AAA-rev.pdf.
3 http://dx.doi.org/10.6028/NIST.SP.1174.

The priorities developed by the Fire portfolio are and designed to enable fire domain organizations to make sound, informed and substantiated decisions and policies.

1. Evidence-Based Decision Making

Existing work:

A recently completed CSSP study, "Report on the Feasibility of a Canadian National Fire Information Database" identified a way forward for creating the data and analytics required, on a national basis, for better evidence based decisions to be made in the fire service. Also a completed CSSP project which developed a "The Right Decision – Evidence-Based Decision Making for Fire service Professionals" manual, developed to enable Canadian Municipal fire service leaders to make better informed and evidence based decisions. This manual is now being redeveloped to provide the same assistance for the policing community.

Remaining gaps:

- The construction of national level fire incident reporting and statistics is a pressing gap for the Fire community. Although work has begun on collecting this data, continued efforts will be required to expand the data collection points and create the governance and analytics required.
- A Technical Risk-based framework reflecting trends in future demand on fire service including frequency of calls and the type of calls within the context of urban fires, wild land fires and the wild land/urban interface.
- Better risk identification and assessment methodologies, modeling and resource planning abilities and improved risk assessment related to fire threats, infrastructure and building codes by region.
- The development of plans, strategies and technologies to better prepare for, respond to and recover from large scale natural or manmade incidents.

2. Dangerous/Hazardous Goods

Existing Work

Within the "Atlantic Canada - New England Hazmat Response" project, CSSP is building on past international response resources by sharing agreements and developing a scaled response plan for interprovincial and international sharing of hazmat response resources. This projects purpose is to develop the agreements for resource sharing across jurisdictions, municipalities, provinces and the nation. It will also introduce a standardized list of resources and create the foundational components for fire and dangerous goods response.

Remaining gaps:

- The continued framework and agreement development concerning interagency, interprovincial, and/or international collaboration of resource sharing and coordination of resources. This includes the development of standardized clauses for use in sharing agreements, and standardized resource typing to allow for identification of resources for inclusion in sharing agreements.
- Standardized resource typing for all fire services to establish team value and resource value, including the infrastructure to maintain and update the resource typing system.

- The standardization of a national Incident Command/Incident Management System to better enable multiple agencies to work together seamlessly during large and small scale incidents.
- The development of training regimes and curriculums to enable response organizations to improve their interoperability and familiarity.
- The increased ability to provide real time data on the transportation of dangerous goods to the communities they pass through.

3. Smart Fire Fighting

Existing Work

The "Fire Dynamics" project will result in the development of a new national educational curriculum based on science and technology research. This will update the current standards while considering the advancements in building technologies and the new progression of fires. This will also develop new training tools and apparatus including the development of web based curriculum tools. Key in the development of standards specifications is the CSS project with the National Research Council's Fire Laboratories to purchase new equipment to improve its capability of identifying products of combustion, burn rates, and to analyze firefighting techniques and equipment. In turn, this will allow the Fire community to develop new codes/standards and improve its equipment and safety devices. The EMSI Portfolio has research projects underway to enable development of PSBN.

Remaining gaps:

- Modern buildings and underground structures strongly attenuate wireless signals. When first responders enter these structures it is desirable that they be able to access their information networks. Define use-cases for in-building wireless communications, including how to provide in-building communications inside LEEDS buildings and structures when there is no power.
- Disorientation in a smoky burning building, sudden fire events, and collapses are significant risks to fire fighters. The ability to locate them in 3 dimensions would assist the incident commander to guide the fire fighters to targets for increased effectiveness or exits in case of sudden fire or structural events, or to help extricate them in case of trouble.
- The continued development of real-time situational awareness capabilities such as the use of Unmanned Aerial vehicles (UAV) and other sensors to increase the amount and quality of data available to incident commanders.
- Codes and standards development to ensure the continued and increased safety of firefighters and residents.

Annex H Paramedic Services

Overview

The Paramedic portfolio has two primary objectives. The first is to develop Science and Technology (S&T) solutions that meet national paramedic services requirements and fit within the scope of the CSSP program. The second is to inform decisions pertaining to paramedic operations and policy through proactive dissemination and sharing of S&T information and knowledge that is relevant to stakeholders within and external to the paramedic community. To achieve these objectives, the portfolio performs the following primary functions[1]:

- **Identify** operational and/or policy gaps that warrant research, investigation, scientific analysis, or the building of collaborative networks to develop solutions;
- **Prioritize** the operational and/or policy gaps through an analysis that aligns the needs of the paramedic services within the scope of the annual CSSP Planning process and associated investment instruments;
- **Influence** the development and implementation of solutions to the operational/policy gaps that are relevant to the community and meet operational and/or policy requirements within the scope of the project charter;
- **Disseminate/Transition** the program outputs to the national stakeholders to ensure the full potential of the new knowledge or technology is realized; and
- **Assess** the impact of Program outputs upon the community, in line with CSSP established values and metrics. Use the assessment results to inform future planning.

The Paramedic portfolio engages the Paramedic Chiefs of Canada, the Paramedic Association of Canada, provincial associations, and other domestic and international committees to understand current and emerging issues that affect the paramedic service in Canada. The portfolio collaborates with the Department of Homeland Security Science and Technology, as well as other research organizations such as universities and standards development organizations. Federally, the Portfolio is maturing relationships with Departments such as Public Safety Canada, Health Canada, and the Public Health Agency of Canada.

To enable knowledge sharing within the community and to provide strategic advice to CSS the Paramedic Community of Practice (CoP) was created to engage with multiple organizations within the paramedic domain. Membership represents a broad spectrum of organizations that are vital to informing the future of the paramedic services in Canada. These include members from national associations, research organizations, as well as private sector, academic, media, and standards development organizations.

[1] As per the DRDC Centre for Security Science: Organizational Roles, Responsibilities and Accountabilities (2013).

Policy and Operational Context

The policy and operational context of the Paramedic Portfolio is compiled from a number of sources. There are several national strategies and action plans that are relevant to the Paramedic Services portfolio including:

- Canadian Pandemic Plan for Health Sector[1] – led by the Public Health Agency of Canada;
- Federal Emergency Response Plan- notably with regards to the strategic objectives to saving lives, reducing personal injuries, and protecting and maintaining public health
- CBRNE Resilience Strategy and Action Plan for Canada[2]- by determining capability needs and understanding the threats and hazards of imminent as well as emerging hazards.
- Communications Interoperability Strategy (CISC) – notably with regards to Public Safety Broadband Network (PSBN);
- Rural and Remote Access to Healthcare – working with partners in northern regions, including the Aboriginal Affairs and Northern Development Canada;

Strategic direction is also influenced by an array of national publications/papers that encompass the complexity of the profession. The legislative framework is comprised of a combination of laws, regulations, and by-laws that are administered through a governance structure in Canada that varies between provinces, to include private owner/operator, municipal, contracted and dedicated provincial services. It is well recognized that the existing legislative framework in Canada is not inclusive of key services that are often fulfilled by paramedic professionals, yet warrant support. These include specialty teams such as marine units, rapid response units, tactical paramedics, Heavy Urban Search and Rescue.

Other examples of policy documents and papers that have been used to inform the direction of the Paramedic portfolio include:

- The Paramedic Chiefs of Canada (PCC) White Paper (2006) and their strategic goals.[3]
- The Paramedic Association of Canada (PAC) 2014 strategic goals[4].
- The Recommended Equipment List (2013).[5]
- Physical Demands Analysis Project[6]
- Post-Traumatic Stress Disorder Annotative Bibliography and Literature Review[7]
- National Paramedic Standards Framework

[1] http://www.phac-aspc.gc.ca/cpip-pclcpi/.
[2] http://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/chmcl-blgcl-rdlgcl-eng.aspx.
[3] http://www.emscc.ca/docs/EMS-Strategy-Document.pdf.
[4] http://paramedic.ca/wp-content/uploads/2014/02/PAC-2014-2016-Strategic-Plan.pdf.
[5] http://psprc-crpsp.ca/EN/rel/pages/default.aspx.
[6] http://pubs.drdc-rddc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3DKEYWORDS+INC+'que'+ORDER+BY+Repdate/Descend%26M%3D5%26K%3D534210%26U%3D1.
[7] http://cradpdf.drdc-rddc.gc.ca/PDFS/unc142/p538641_A1b.pdf.

- Medical Records Integration Report
- National Standard Z1610 Personal Protective Equipment to CBRN Events[1]

The strategic direction is also informed through research projects that have been completed for the purpose of understanding and identifying priorities for the Paramedic service in Canada, such as the Gap Analysis for EMS, S&T Research[2], and the Canadian National Emergency Medical Services research Agenda.[3] Through analysis of the gaps in policy and operations, identified through a broad and proactive engagement across the portfolio stakeholders, the Paramedic Portfolio has identified four key categories that will serve as priority domains over the following three to five year cycle. These include:

Mobilized health care

The existing health care system in Canada is under pressure with respect to traditional practices for delivering medical and health care services. The trend has become one to explore how paramedics can use their critical thinking and skill set to help deliver care in a proactive model. There is a need to better understand how the paramedic profession will enable the capacity of healthcare in the future. This includes an understanding of how the application of technology can be used to inform policy and protocols as the profession moves to a mobilizing healthcare model. With an aging Canadian population older adults will place increase demands on the healthcare system. Consideration for the paramedic services to move to a more holistic healthcare model that is more proactive rather than the traditional reactive service delivery models needs to be considered.

Evidence-Based Decision Making

The health sector is becoming increasingly dependent upon the rigour of evidence-based decisions, supported through the collection and analysis of large volumes of data. There is a need to build upon established databases to help establish and understand both clinical and operational performance metrics and the associated economic impact of paramedic programs and practices within Canadian communities. This includes a deeper understanding of how data and data management can be used to inform evidence based decisions and policy creation.

Practitioner Well-Being

Existing and emerging literature[4] is helping society to understand the degree to which the well-being impacts the quality and capacity of the paramedic profession. Today, society is confronted with pandemic outbreaks that threaten the well-being of our communities. As well, Canadian society is also coming to grips with the increasing awareness of mental health issues within the ranks of Canada's Paramedics. This affects the capacity within Paramedic Services to meet the system demands including the economic impact. The well-being of paramedics is directly relevant to the resilience and well-being of Canadian communities. A greater understanding on how we can protect paramedics is required.

Standards Development

1 http://shop.csa.ca/en/canada/occupational-health-and-safety-management/cancgsbcsa-z1610-11/invt/27032372011.
2 http://www.premergency.com/media/consultancy/GapAnalysisFINALreportDec2012Web.pdf.
3 http://cjem-online.ca/v15/n2/p73.
4 http://www.paramedicchiefs.ca/docs/bcs/PCC_Ad_hoc_Committee_on_Stress_Injury_Report.pdf.

The role of paramedics and paramedicine in Canada is highly dynamic and in steep growth. There is a requirement for the creation of paramedic specific standards related to the paramedic community across Canada. As well, there is a need for performance based standards that are measured to inform the economics of community safety and well-being. Currently, there does not exist national standards for paramedics and paramedic equipment across Canada. This limits the ability to quickly and efficiently move personnel and assets in times of crisis.

Program of Work

The priorities developed by the Paramedic community are designed to enable the paramedic organizations to make sound, informed and substantiated decisions and policies.

1. **Mobilizing Health Care**

Existing Projects

Economic Value of Community Paramedicine Program: This project will examine the economic benefit of community paramedicine programs in both the rural and urban environments and measure the financial impact of these programs on the global healthcare system. Looking retrospectively to determine a target population of clients, a 12 month pilot will see paramedics visiting patients prior to them accessing the healthcare system. A detailed costs analysis will then be completed to look at the costs to these patients pre and post pilot phases.

Remaining Gaps

- Research and technology that supports sustainable community paramedic programs that show benefits to the community and the healthcare system.
- Technologies that allow paramedics to monitor patients in their home and help patients maintain a safe and healthy living environment.
- Development and application of telemedicine and tele-monitoring (remote monitoring) technologies, protocols, and policies in support of safe and healthy communities.

2. **Evidence-Based Decision Making**

Existing Projects

Paramedic Mega Database: This project is amalgamating a set of clinical and operational data from several paramedic services and currently has data from over 1.2 million calls. Using electronic patient care records, information is collected in a central database to help in establishing benchmarks. Response time, clinical procedures, equipment used and paramedic interventions are recorded and all are searchable.

*Electronic medical record integration:*This project will produce a report that outlines a framework for paramedic electronic records and the option to fully integrate with hospitals for the sharing of patient care records. Key stakeholders will be engaged to establish such a framework and process for transmission. Through increase collaboration between the paramedic community and hospital community key technology components will be identified.

Remaining Gaps

- Establishing key performance metrics regarding levels of service and deployment and understanding the economic impact.
- Responding to calls for service including defining response times, better understanding of which patients could benefit from urgent and emergency response, improved measurement data, and communicating targets and performance.
- Understanding scalable response phasing and the interoperability efficiencies when dealing with large scale emergencies.
- Roles within community safety and the broader landscape for opportunities to increase community resiliency.
- The demographics of the paramedic community.

3. **Practitioner Well-Being**

Existing Projects

*Paramedic Physical Demands Analysis:*This was the first National observational study that helped identify and characterize the physically demanding tasks encountered by paramedics that were critical to the profession across Canada. This study will help support future development of evidence based bona fide physical demands for both pre-employment screening tests and return to work initiatives.

Paramedic Communication Centre Workload Analysis and Predictive Modelling: This project will implement CAE Deploy within the operational environment in the Ottawa Central Ambulance Communications Centre. It will be used as a decision tool to provide regular unit deployment recommendations to the Communications Officers and support their deployment strategy. A workload analysis will be conducted of the Communications Officer to compare workload levels post implementation, with outputs to inform the broader paramedic domain.

Remaining Gaps

- Infection Control: Further research and technology is required to inform decisions regarding the control of infection, notably for paramedics who are often the first to receive patients. Challenges exist in the awareness and information flow between healthcare organizations. This domain also calls for a need to protect patients and hospital ‘first receivers’ from the spread of infection, including the development of protocols/standards for disinfection, and deployable personal protective equipment.
- Mental/Psychological Resilience: Further research is required to support decisions regarding the development and implementation of programs to help prevent, mitigate and address mental health issues within the paramedic services.
- Physical Health: There is a requirement for further research to understand the physical demands and physical health risks associated with paramedic tasks, and how these risks can be mitigated through new technologies, equipment, and evidence based developed protocols or procedures.

4. **Standards Development**

Canadian Standards Framework: This project worked with the Canadian Standards Association and developed the first strategic framework for standards creation for Paramedic Services in Canada. By identifying the most appropriate areas for future work in terms of standards development, a strategy for implementing standards can be created.

Recommended Equipment List (REL) for CBRNE: This project will update and refresh the REL information and knowledge to inform CBRNE practitioners in Canada. The goal is to create a web based platform to connect the first responder communities in information sharing and establish an agreement covering the ongoing support and evergreening for the REL outputs consistent with the principles of the REL format Hazard Identification and Risk Assessment (HIRA), Capability Based Planning (CBP), and resource typing.

Remaining Gaps

- Standardize equipment classifications (e.g. Ambulance vehicles, disposable equipment, portable medical supplies, and specialized equipment such as CBRNE, USAR or Tactical response).
- Defining competencies for entry-to-practice and measurement for continuing education competence. Education and training practices and protocols, including the effective use of modeling and simulation.
- Performance standards that inform economic decisions pertaining to community safety.
- Standards related to speciality services like community paramedicine.

Annex I Police and Law Enforcement

Overview

The Police-Law Enforcement (PLE) portfolio's objective is to create paths linking researchers and users in an effort to leverage scientific research in support of more effective and efficient policing policies, programs, practices, and evidence-based decision-making. Community safety is highly complex and requires a collaborative multi-agency approach that goes well beyond the traditional policing domain. This core element was recognized and discussed in the "*Institute for International Strategic Studies on Full Circle Community Safety"*[1] report, published in 2012. The portfolio is integral to the CSSP's broader goals of integrating elements of innovation from a range of science and technology providers, with the needs of policy, operations, and intelligence. The scope of work incorporates rigorous scientific/engineering methodologies to support informed decisions pertaining to community safety. Examples include: social and physical science, engineering, statistical analysis, as well as components of standardization, interoperability, performance measurement and operational evaluation. The portfolio routinely engages leaders from organizations and other pertinent stakeholders through formal priority setting forums, integrated project management and delivery teams. The following entities are engaged within the scope of portfolio activities:

- Canadian Association of Chiefs of Police;
- Federal, Provincial, and Municipal Police Services;
- Federal Government Departments with an interest in policing policy and operations, (Public Safety Canada, Transport Canada);
- Canadian educational institutions (Universities, Colleges and Police Colleges);
- Non-Government Organizations and volunteer groups (Red Cross); and
- International organizations (US Department of Homeland Security, UK Home Office, US Counter-terrorism Technical Support Working Group).

To enable further collaboration, a PLE Community of Practice (CoP) was established in 2012. It is co-chaired by leaders from within the PLE community, who are well informed and involved in national level issues. The CoP is a primary source for synthesising policy and operational requirements and is made up of representatives from across the PLE community, including academics, policy writers and leaders from various operational police services.

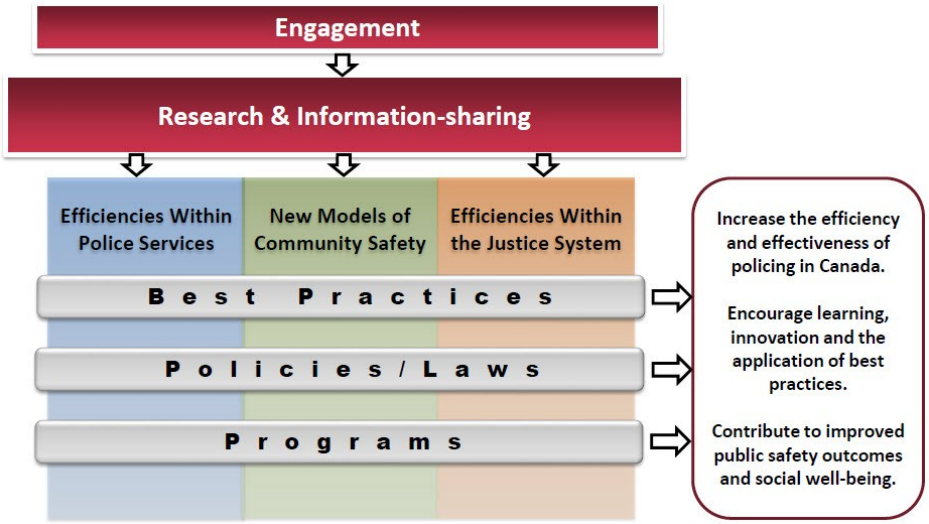
Policy and Operational Context

The portfolio's strategic influence derives from formal policies originating from a multitude of regional governance models. To ensure that the CSSP's efforts have the greatest impact, the portfolio is guided by new and emerging S&T requirements identified by local, provincial, federal and international police and policing research organizations. Examples include projects by: DRDC, the Defense Advanced Research Projects Agency (DARPA), published works from the UK, Australia, U.S. (National Institutes of Justice) and the National Institutes of Technology Standards. The contributing factors in identifying CSSP research investments are directly

[1] http://www.cacp.ca/ISIS/admin/Documents/upload/ISIS_2012_English_Handbook_for_website.pdf; A Handbook and Guide in Support of New Multi-Agency Metrics for Community Safety (2012).

associated with national priorities of the community. The *CACP Research Foundation's Research Agenda*[1], published in 2014, is a prime example of national priority coinciding with our research investments as it provides key information on national policing research gaps.
Other key guiding policies and strategic documents include:

- **Economics of Policing - Shared Forward Agenda (2014)**[2]:Emphasizes the Federal, Provincial, and Territorial need for research into policing to increase effectiveness and reduce costs through a comprehensive and holistic approach to public safety;



- **Chemical, Biological, Radiological, Nuclear, and Explosives Resilience Strategy**[3] **for Canada** which provides direction in support of interoperability;

  "The Strategy enhances timely and effective decision-making through improving integration, coordination and interoperability amongst CBRNE contributors from plans, to standard operating procedures, to equipment and/or training. The Strategy is designed to work in conjunction with existing jurisdictions and mechanisms, such as the Federal Emergency Response Plan (FERP), the National Emergency Response System (NERS), the Federal Nuclear Emergency Plan (FNEP), the National Counter-Terrorism Plan, and F/P/T/M response plans. Provincial / territorial and regional response arrangements are also included".

- **Communications Interoperability Strategy for Canada (CISC)**[4]with a key area being the transformative capability which will be provided by the Public Safety Broadband Network (PSBN);

  Information is the lifeblood of effective day-to-day operations within the public safety community. In making countless decisions every day, officials must have immediate access to timely, accurate, and complete information. It has become clear that effective decision-making requires information that must often be shared across a broad landscape of systems, agencies, and jurisdictions. For example, the adoption of common tools such as open standards is a key element in enabling public safety agencies to deal with this growing and complex problem. The CISC envisions that

[1] https://www.cacp.ca/media/research/efiles/42/FINAL_-RF_Executive_Agenda_-_Mar._2014.pdf.
[2] http://www.publicsafety.gc.ca/cnt/cntrng-crm/plcng/cnmcs-plcng/shrd-frwrd-gnd/index-eng.aspx.
[3] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg/index-eng.aspx.
[4] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-eng.aspx.

the emergency management and response communities will adopt common or compatible processes and tools that enable multi-agency coordination and joint service operations.

- **CACP Research Foundation's *Research Agenda***[1] which represents policing at all levels in Canada provides key information on national policing research gaps. Issues related to funding and financing are a clear priority for Canada's police executives—both today and in the years ahead. Three questions are of particular concern to them:
    - What key indicators/metrics can be developed to reflect the costs and effectiveness of policing?
    - How can the use of information management strategies and technologies across the public safety system reduce costs?
    - How can we quantify the impacts of policing?

Through analysis of the gaps in policy and operations, identified through a broad and proactive engagement across the portfolio stakeholders the Police and Law Enforcement Portfolio has identified key categories that will serve as priority domains over the following three to five year cycle.

Improving the Economics of Community Safety through Evidence-Based Decision Making and Knowledge Sharing

The underlying theme of Community Safety is outlined in both the CACP Research Foundation Research Agenda and the Economics of Policing. This priority focuses on scientific knowledge and technologies that enable the development and institutionalization of mechanisms and processes that facilitate a robust and informed decision-making enterprise within police and law enforcement organizations including those associated with policy, procedures and technology to improve the economics of community safety. In addition, this priority will focus on the development knowledge and capabilities to support decisions regarding investments in PLE programs, notably those associated with low-use/high-risk programs that are critical to the PLE mandates, as well as more routine high cost programs that warrant a specific level of scrutiny.

Employing Emerging Technology and Engineering to Increase the Effectiveness of Police

The CACP Research Foundation highlights the importance of enhancing Information Management and Information Sharing. Specifically, "Canadian police executives believe that better management and sharing of information—data, evidence, research, or best practices—will help to ensure that the right people have the right information at the right time." Related to the economics of community safety is the potential for technology and engineering to improve the effectiveness of policing. With the transformative capability that will be available from the Public Safety Broadband Network (PSBN) many emerging technologies have the potential to positively impact the policing community.

Program of Work

The program of work for the outlined priority areas are below:

[1] https://www.cacp.ca/media/research/efiles/42/FINAL_-RF_Executive_Agenda_-_Mar._2014.pdf.

Improving the Economics of Community Safety through Evidence-Based Decision-Making and Knowledge Sharing

Existing Projects

- *Emergency Responder Posttraumatic Stress Disorder (PTSD) Scoping Study:* project improves efficiency and effectiveness of police PTSD management through a review of Canadian Forces research directed toward the effective management of PTSD cases in their ranks and identifying those practices, procedures and research base that apply to emergency responders.
- *Police Emergency Response Teams Regional/National Risk Assessment and Interoperability Working Group Study:* develops methods for ERT teams in a province to become interoperable at the tactical level and provides a baseline of planning for all departments through the use of risk, evidence and economic reality based scenarios. The eventual goal of this work is a standardized model of increased operational response in the most economically efficient and tactically effective uses of resources from multiple police organizations.
- *Multi-Discipline Multi-Agency Missing Person Investigative Initiative:* project addresses a gap in the ability of police investigators throughout Canada to access specialized scientific expertise to assist with missing persons and unidentified remains investigations. The results of this project not only increase the effectiveness of investigation time but also reduce costs through the leveraging of highly specialized scientific support.
- *RCMP Federal Policing Re-Engineering:* project provides a scientific evidence-based approach to this and any other police organization for decision makers to implement an efficient and effective design, implementation, policy, audit and measurement of a large program delivery element. The goal is to retain or increase operational effectiveness while reducing costs, all measured for conformity over time.
- *Linking RCMP Skills Acquisition & Recertification in Simulated Environments to Tri-services:* this project addresses the transferability of evidence collected during the police use of simulators and simulation to Fire and Paramedic communities. The operational effectiveness while improving resource costs are at the forefront of this effort.

Remaining gaps:

- Implementation of simulation technologies in support of basic, advanced or specialized training, skills retention, as well as proficiency training to include certification/re-certification practices.
- Examine existing common police and law enforcement programs to identify and/or further develop metrics that measure program effectiveness in the context of community safety. Including results analysis with the intent to enable equivalent or similar programs within Canada. Example projects include: anti-drug use, school safety, street-proofing, traffic accident reduction, family violence, auto theft, fraud and internet based anti-luring/children safety.
- Establish the metrics for specialized services within police and law enforcement organizations. These metrics will inform investment decisions regarding PLE programs that are based on population, population density, distance (to nearest service), and/or full time/part-time postures. Examples of specialized services include Air Services, Dive Teams, Tactical Teams (ERT, SWAT, TRU etc.), and Public Order Teams.

- Implementation of best practices in evidence-based decision-making through the collection, storage, analysis and sharing of calls for service and criminal case management data to enable timely access to the analytical results in support of key decisions affecting operational and organizational issues.
- Formal adoption of enterprise risk management principles through a common approach for assessing risks associated directly with community safety and organizational risks inherent to any personnel based service.
- Effectiveness of incorporating modeling and simulation to support informed decision-making within the PLE community.

Employing Emerging Technology and Engineering to Increase the Effectiveness of Police

Existing Projects

- *National Law Enforcement Information Management Study:* is gathering evidence related to police use of criminal case management systems and verifies whether or not they are interoperable with each other.
- *Next-Generation 911:* project identifies technical and scientific evidence in support of the next generation 911 policy, service, capacity and capability.
- *Emergency Facility Management Building Tactical Information System:* project is focused on improving the response time of emergency responders when called to very high risk scenes in large structural facilities by providing three dimension layouts of the structure(s) directly transmitted to them through the 911 system.
- *Body Worn Video: project* is underway to address the police use of body worn video as a tool to increase the effectiveness of uniformed officer investigations and to reduce the liability to the individual officers and the police organizations that employ them.
- *Innovative Policing Practices: Information and Communications Technologies in a Crowd Control Setting: project* analyzes data from multiple crowd control events occurring in Quebec of 2012 and 2013 with the purpose of identifying the ideal state of collection, analysis and resultant action based on information/communications technology. The practices and procedures will be made available throughout Canada for police crowd control purposes.

Remaining gaps:

- Modern buildings and underground structures strongly attenuate wireless signals. When first responders enter these structures it is desirable that they be able to access their information networks. Define use-cases for in-building wireless communications, including how to provide in-building communications inside LEEDS buildings and deep structures when there is no power.
- Further research into the use cases of next generation 911 that involve integration with emerging capabilities related to body worn video and building tactical information system and PSBN.
- Implementation of high reliability two-way communications between responders and response management sites including live audio and video being transmitted with or without intervention from the responder and in Canadian locations not currently served by standard service providers.
- Implementation of long range unmanned aerial reconnaissance capability as a means of leveraging existing human resources in rural and remote locations in Canada in support of community safety, missing persons cases and collaborative efforts with other services

responsible for forest management and wildlife populations studies (including migration patterns).

In addition to these priority areas existing projects are underway in the Forensic domain in the following area:

Reducing the Cost and Time of Investigations through Improved Forensic Work

Police in Canada are tasked with discovering, collecting and analyzing evidence related to crimes for the purpose of presenting the perpetrator(s) before a court with the evidence. Forensic research is focused on reducing the uncertainty around evidence found at crime scenes to make the evidence more compelling and to raise certainty the correct perpetrator(s) have been identified. Secondly, expert testimony in Canadian courts is treated differently than witness testimony with a much lower tolerance for claims that can be made by experts. Over time, cases lost due to inadmissible evidence and the loss of the investigation time (typically in the millions for homicide cases) has become a significant burden to police organizations. The forensic research encompasses efforts to increase the quality of evidence collection and analysis while significantly affecting a reduction in time spent on the background investigation.

Existing Projects

- *Accelerant Signatures on Cadavers:* this project is developing evidence-based methodology and protocols for the collection of accelerants from cadavers. The evidence of accelerants on the skin of cadavers is much more compelling than the traditional collection of accelerant signatures from the crime scene.
- *Deep Sea Taphonomy:* project is developing decomposition data of cadavers in ocean environments for the purpose of establishing time of death. Testing and data collection is taking place in two ocean environments with different characteristics to determine the evidence-base for future investigations.
- *DNA Immortalization:* through evidence-based research, this *project* is developing collection and preservation techniques of DNA evidence. The project is developing methods of collecting DNA previously lost or degraded due to environmental harm and testing better long term preservation materials and methods.
- *Enhancing Forensic Entomology Applications in Canada using Molecular Tools: project* attempts to improve murder investigations by developing, testing and verifying improved scientific methods where entomology is used to determine time of death on cadavers found in land environments.
- *Web Support for Admissibility of Fingerprint Evidence: project* addresses recent trends in the loss of criminal cases where expert testimony has been rejected by the courts due to the phrasing of the expert witnesses describing the accuracy and possible error rate of their evidence. When reasonably possible, the project has attempted to simulate court challenges to produce evidence-based results.
- *Multi-Discipline Multi-Agency Missing Person Investigative Initiative:* project addresses a gap in the ability of police investigators throughout Canada to access specialized scientific expertise to assist with missing persons and unidentified remains investigations. This project not only increases the effectiveness of investigation time but also reduce costs through the leveraging of highly specialized scientific support.

Remaining gaps:

- None at this time. However, emerging court decisions can change this quickly.

Annex J Psycho-Social

Overview

The Psycho-Social portfolio investigates the "human factors" dimension of safety and security capability gaps related to: 1) countering radicalization and violent extremism (CVE); 2) preparing for, responding to, and recovering from natural disasters, pandemics, and other high-impact events; and 3) resilience at the individual, organizational, sectoral, and community level.
The current portfolio has evolved from the psycho-social cluster, formally established in 2007 under the Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Research and Technology Initiative CRTI program. The cluster brought together researchers and practitioners from the psycho-social and behavioural public safety and security domains (mainly government and academia) in order to address, through investment in scientific research, priorities around "Public Confidence and Psychosocial Factors" related to CBRNE terrorist threats. Within the current Canadian Safety and Security Program, the scope has been broadened to include S&T investment for all-hazards.

There is a major interest and a pressing need in Canada to address the "human factors" aspects involved in the lead-up and aftermath of events derived not only from terrorist threats, but also other man-made and natural disasters. Understanding these aspects can improve the well-being of the emergency services (fire, police, and paramedic), as well as individuals and communities, when they are facing disasters, extremist threats, or other adversities. The Resilience and Psycho-Social Portfolio is cross cutting in nature; hence, the priorities are also based on community requirements from the Emergency Management and Disaster Resilience, Emergency Services (fire, police, and paramedic); and Surveillance, Intelligence, and Interdiction (SII) portfolios.

As underlined in a previous (2010) proposal to organize and manage the psycho-social community,[1] a series of workshops were held between 2007-2009 to establish a "community of practice," crossing disciplines, professions, and sectors, and focused on "creating and exchanging knowledge of psychosocial elements that can prevent the occurrence of high impact events, and improve the preparedness and resilience of Canadian society from the threat and occurrence of such events at the individual, community, organizational and societal levels". Given the nature of the areas covered by this portfolio, much of the subject matter expertise resides academics, Non-Governmental Organizations (NGOs), and various service-based agencies. Two main streams were identified for activities within this portfolio, which also described the constituency of partner sub-groups within the portfolio: 1) the radicalization and countering violent extremism (CVE) stream, and 2) the resilience/social-cohesion stream, which has been subsequently split into aspects that deal with: a) preparing for, responding to, and recovering from natural disasters, pandemics, and other high-impact events; and b) resilience at the individual, organizational, sectoral, and community level. To date, the portfolio program of work has been shaped though engagement with the "community of practice" described above, whose constituency and structure reflects what was proposed in the 2010 document.

[1] Lemyre, L., Corneil, W., Pinsent, C., and Boutette, P., 2010, Centre for Security Science Strategic Plan and Business Case Proposal.

Key federal partners within the CVE stream include Public Safety Canada, Canadian Security Intelligence Service (CSIS), Corrections Canada, and the Royal Canadian Mounted Police (RCMP). There is a large academic component to the CVE stream, which was also bolstered by the Kanishka project, a five year $10M initiative managed by Public Safety Canada to "invest in research on pressing questions for Canada on terrorism and counter-terrorism, such as preventing and countering violent extremism."[1], To date, the CSSP has focused on supporting projects and initiatives that complement Kanishka-funded research.

An additional area of active research within the portfolio is providing psycho-social care to victims of disasters and other mass casualty events (including intentional criminal/terrorist acts). This implies developing appropriate training for emergency services first responders (fire, police, and paramedic) and health care first receivers (emergency room/hospital personnel) to address psycho-social aspects. At the same time, the first responders/first receivers themselves have psycho-social needs that need to be addressed when such events occur. Key federal partners in these areas include Health Canada and the Public Health Agency of Canada. Academic partners include JIBC and Royal Roads University. First responder organizations benefit from projects supported through this priority area by incorporating findings into their training packages, developing/updating procedures and standards for response, recovering, and providing care, both to the public and to the first responders themselves.

Finally, in the area of community resilience key federal partners are Public Safety Canada, Natural Resources Canada, and Aboriginal Affairs and Northern Development Canada (AANDC). There are a number of active partners in academia (such as Justice Institute of British Columbia (JIBC), Royal Roads University, Wilfrid Laurier University), as well as provincial and municipal partners. Also, activities in this area would benefit from closer engagement with existing groups such as the Resilient Communities Working Group under the Canada's Platform for Disaster Risk Reduction.

Policy and Operational Context

With economic and social costs associated with the aftermath of disasters steadily increasing in Canada and worldwide, governments are looking to shift their focus towards better preparedness, mitigation, and increased resilience. With analytical and financial support from the CSSP, Public Safety Canada is developing a risk and resilience framework to support the rollout of the National Disaster Mitigation Program (NDMP), a $200 million initiative announced by the GoC as part of its 2014 Budget.[2] More broadly, Public Safety Canada is re-examining their approach to Emergency Management, with an increased focus on building resilience through engaging the whole-of-society. International jurisdictions are also focused on similar strategies. For example, Australia has adopted a "whole-of-nation, resilience-based approach to disaster management" as underlined in their National Strategy for Disaster Resilience.[3]

Other strategies, action plans driving/influenced by areas of interest within the portfolio:

[1] Kanishka Project, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/r-nd-flght-182/knshk/index-eng.aspx.
[2] National Disaster Mitigation Program, http://actionplan.gc.ca/en/initiative/national-disaster-mitigation-program.
[3] Australian Government's National Strategy for Disaster Resilience, http://www.ag.gov.au/EmergencyManagement/Pages/NationalStrategyForDisasterResilience.aspx.

- Counter-Terrorism Strategy
- Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Strategy and action plan
- Disaster Mitigation Strategy
- Federal Emergency Management Response Plan
- Public Health Agency of Canada (PHAC)/Health Canada (HC) Response Plans.

Much of the program of work for this portfolio still relies on the 2010 proposal discussed in a relevant section above[1]. Additionally, reports documenting consultations with stakeholders, supported by DRDC CSS through Community Development funding, provided additional input into shaping the focus and scope of current work in this domain.[1,2]

An examination of past and current projects indicate that, while there has been increased effort towards an "all hazards" scope to the portfolio activities, it has remained issue-driven, rather than derived from a coherent and comprehensive understanding of the role, structure, and needs of the community. This was the intent behind another Community Development project, "Revitalizing the Psycho-Social &Community Resilience CoP" (CSSP-2013-CD-1121). As part of that project, a Value-Focused Thinking approach was adopted to build an objective model for the portfolio in order to help re-examine its mandate and scope, and to identify research and membership gaps, priorities of those gaps, and ways to address them.[3,4] It is possible that additional research themes can be identified, together with ways to bolster applications of the research generated, by reaching out to a broader mix of psycho-social disciplines.

Looking into the future, there are a number of emerging issues and S&T developments that are likely to influence the program of work in this domain in the next three to five years. They are summarized in the paragraphs below.

Kanishka Project
The Kanishka Project is about better understanding what terrorism means in the Canadian context, how this understanding is changing over time, and what can be done to support effective policies and programs to counter terrorism and violent extremism in Canada. Through Kanishka sponsored research and other activities, the countering-violent extremism segment of the resilience and psycho-social portfolio has grown in both size and interconnectedness of collaboration networks, with new partners in government, academia, and non-governmental organizations, addressing knowledge gaps on a range of relevant topics. Research topics have grown broader as well, addressing security and counter-terrorism questions that go beyond countering violent extremism, including research that speaks to issues of collaboration at the organizational, community and national level. By all accounts, the Kanishka Project has been very successful; this is one reason why the expiration of the funding associated with the project in 2016 prompts the search for avenues to leverage knowledge already generated, as well as alternative funding avenues to continue knowledge generation in a continuously evolving security landscape.

---

[1] First Receiver HazMat/CBRNE Preparedness Workshop Summary, CSSP-2013-TI-1062 Z-01, Dec. 2013.
[2] Bowles, R., and Ursuliak, D., Building Resilient Communities Workshop Report, DRDC-RDDC-2014-C131, June 2014.
[3] Adamson, J., Value-focused objectives model for community resilience: Final report, DRDC-RDDC-2014-C82, April 2014.
[4] Verga, S., A value focused thinking approach to building a community resilience objective model – focus group discussion summary, DRDC-RDDC-2014-L42, April 4, 2014.

Whole of community resilience

In order to maintain stability and proper functioning, societies require well informed and current public policies. Disasters, and crises in general, often bring to the spotlight requirements for policy review and renewal; this is true both in terms of updating policies to better guide the society's response to a crisis, as well as of adjusting policies to acknowledge and account for emerging patterns in collective behaviour. Therefore, better understanding the processes that shape public policy can potentially lead to improved governance and effective change.
In addition to societal changes, the new economic reality facing governments challenges traditional approaches to public policy, and requires a re-examination of roles that individuals, businesses, community organizations, response organizations, various levels of government, and NGOs, can play, and how they can do it together. Community resilience is a prime example of a public safety and security problem that could benefit from a systems thinking and a "whole of community" approach.

Science can be brought to bear by employing methods and tools in new and innovative ways in order to address the needs of policy development in the modern world. For example, a scientific study of resilience and stakeholder community conducted in support of Public Safety Canada's efforts to develop a new national resilience strategy explored how network analysis tools and methods can be employed to better understand policy links, and where and how the concept of "resilience" can fit in terms of new and existing policy and governance structure.[1] Through literature reviews, policy research, and surveys administered to stakeholders, data was collected and analyzed which allowed them to build a multi-mode network map with layers that show linkages between policy, legislation, programs, and activities, as well as a social network of people currently engaged in resilience building programs and activities. This type of analysis can provide an enhanced understanding of the resilience stakeholder community, and of the structure of relationships and activities, as well as their links to legislation and policy.

Social media

Social media has gathered global momentum, but its potential to be used for the good of the "global community" is yet to be fully explored. There remains a significant need for further study and research in this area. There is a high level of interest to better understand the growing role of social media in emergency management, which has already been reflected in CSSP supported efforts to gain insights into how to maximize and integrate digital volunteer engagement in disaster response.[2] Social Media can potentially support a number of additional aspects related to the resilience and psycho-social domain: addressing the needs and engaging the vulnerable sector, as well as the responder community, engaging community organizations and groups to bolster community resilience, and possibly others. Additionally, there are psycho-social implications

[1] Kaminska, K., Norton, S., and Verga, S., Mapping of legislation and policy instruments related to emergency management and national security, DRDC CSS LR 2013-026, February 14, 2013; Kaminska, K., Norton, S., and Verga, S., Results of the resilience stakeholder community survey, DRDC CSS LR 2013-027, May 10, 2013; Verga, S., Kaminska, K., and Norton, S., Results of the resilience stakeholder community survey—second phase, DRDC CSS LR 2013-028, September 5, 2013; Verga, S., Norton, S., and Kaminska, K., Analysis of the multi-layer meta-network of legislation, policy, organizations, activities, programs, and projects related to resilience, DRDC CSS LR 2013-029, October 18, 2013.
[2] Kaminska, K., and Rutten, B., Social Media in Emergency Management, DRDC-RDDC-2014-R16, May 2014.

associated with the impact of pervasive social media use on privacy and virtual identity that need to be better understood.

Increased convergence and assemblage

This area of research investigates the multi-agency approach to public safety/security problems from new angles. It considers, on a conceptual, cultural, and functional level, emergent conditions under which different actors "come together" to approach complex problems.[1,2] This "coming together" encompasses the three functions of cooperation, coordination, and collaboration, and is understood as the requirement for individuals, groups or organizations to alter or amend aspects of how they normally operate, and to assemble novel capabilities and attain a greater agility to solve unique problems or respond to emergent situations.

Big Data

The quantity of data generated in the e-age, with its smart phones, social media, and sensor-equipped everything, is growing at an unprecedented rate, and in turn is spurring a revolution in computational and statistical methods. The "quantification movement" is generating more and more interest in the social sciences domain because of its potential to help solve problems in human society.[3] The amount of data increasingly available is bound to influence the way social scientists conduct empirical research and will likely generate interdisciplinary initiatives, bringing together statistical researchers, who have knowledge of modern data analysis tools and techniques, with social scientists who are leaders in qualitative aspects of their fields. This area holds a huge application potential across a range of fields, from academia and science, to industry, public health and medicine, security and government, and international development. Community Resilience is one of the many areas that can benefit from the application of novel algorithms to the increasing volume of available data. This applies to both unstructured, or "search" data, and structured data. Sifting through social media data before, during, and after natural disasters and other types of crises and looking for patterns of behaviour and activity, as well as social "mood", can reveal correlations between crisis outcomes and characteristics of communities and populations.

Super-diversity

Understanding the implications of super-diversity to community safety, security, and resilience is a largely untapped research area. Super-diversity refers to an unprecedented level and type of social complexity not previously experienced in a particular society. The global movement of people over the last few decades have generated complex social phenomena, which are only now beginning to be understood.[4] Some of the variables thought to provide insight into these new social phenomena include: country of origin (with possible subset traits such as ethnicity, language, religious tradition, regional and local identities, cultural values and practices), migration channel (often related to highly gendered flows, specific social networks and particular

---

[1] Okros, A.C., Verdon, J., and Chouinard, P., The Meta Organization: A Research and Conceptual Landscape, DRDC CSS TR 2011-13, 2011.

[2] Peach, J., O'Keefe, D., Schryer, E., and Okros, A., Social psychology theories in the meta-organizational context, DRDC CSS CR 2012-025, December 2012.

[3] Big data and positive social change in the developing world: A white paper for practitioners and researchers, Rockefeller foundation, http://www.rockefellerfoundation.org/uploads/files/c220f1f3-2e9a-4fc6-be6c-45d42849b897-big-data-and.pdf.

[4] Berga, M.L., and Sigonab, N., Ethnography, diversity and urban space, in Identities: Global Studies in Culture and Power, 20(4), 2013http://www.tandfonline.com/doi/abs/10.1080/1070289X.2013.822382?journalCode=gide20.

labour market niches), and legal status (with numerous categories considered in order to determine entitlements and restrictions). The dynamic interplay of these variables may influence integration outcomes in "host" societies, alongside factors surrounding migrants' human capital (particularly educational background), access to employment, local conditions (related especially to economic conditions, but also to the presence of other immigrant and ethnic minorities), and the responses by local authorities, services providers and local residents (which tend to be influenced by assumptions based on previous experiences with migrants and ethnic minorities). Migration flows and patterns of diversity in a variety of settings around the world is an emerging field of research that is likely to generate increasing interest in the near future. It is likely that a better understanding of aspects pertaining to super-diversity can be applied to improve community resilience.

Program of Work

The following are the portfolio's key areas of work. For each, the current program is given as well as themes for the remaining challenges in the area.

Counter-violent extremism

On-going projects:

- CRTI 09-428RD - National Security Data Initiative to enhance the Canadian evidence base for national security policy and operations (2011-2015)
- CSSP-2013-TI-1050 - Mitigating threats from violent extremist offenders in correctional institutions and communities (2013-2015)

Remaining gaps:

- Expand the evidence base and develop analytical tools and methods to support a better understanding of the mechanisms that lead to violent extremism and develop effective means of countering it.
- Develop and pilot methods for the effective use of social media and "Big Data" for improved intelligence.

Psycho-social support to first responders and the public

On-going projects:

- CRTI 08-0180TD- Establishing an integrated National CBRNE Training System for Health, Psychosocial and Communication Responders (2009-2014)
- CRTI 08-0114RD - Simulation Training & Exercise Collaboratory (SIMTEC): Enhancing CBRNE and All Hazards Psychosocial Capacity and Capability Management

Remaining challenges:

- Improve knowledge of psycho-social elements related to the prevention, preparedness, and resilience to the threat and occurrence of CBRNE and other high-impact events. Also, increase awareness among practitioners and decision makers of their importance. Included here are:
    - Education about psycho-social aspects of high-impact events.
    - Development of standards within the health care system for the psycho-social treatment of victims of CBRNE and other high-impact events.
    - Psychosocial care for First Responders/First Receivers.

Community resilience

On-going projects:

- CSSP-2013-TI-1048 - Survey of Emergency Preparedness and Resilience
- CSSP-2013-TI-1034 Social Media for Emergency Management – increase the **value of social media-aided cooperation** between digital volunteers, EM officials, first responders and humanitarian workers for better recovery outcomes

Remaining challenges:

- Better understand the behavioural implications of effective communications, in order to inform strategies on:
    - Effectively shaping and conveying information in order to induce desired public behaviour in disasters and other mass casualty events, and
    - Volunteerism (i.e., the recruitment, sustainment, and retention of volunteers).

  Differences between communication needs in Canada's North, compared to the South, should be considered.
- Develop effective "whole-of-community" approaches for building community resilience. These might include:
    - The development of sustainable and cost-effective tools and methods that support communities to mobilize and fully exploit existing capacity in order to improve resilience and
    - The development of metrics for measuring resilience for a Canadian context.

Cross-cutting challenge areas

The challenge areas identified below may relate to one or more of the above psycho-social/community resilience areas, as well as other CSSP portfolios:

- The development of baseline data related to countering violent extremism, community resilience, and an improved disaster database in a Canadian context.
- The development of mechanisms for the better alignment and connection across research, operational and policy communities.
- Research and development of policy, methods, and tools for the effective use of social media in the many aspects of preparedness, prevention, mitigation, response and recovery to disasters and other high-impact events.
- Research to improve understanding of how super-diversity of communities can be used to improve community resilience.

This page intentionally left blank.

Annex K Radiological and Nuclear

Introduction

The Radiological and Nuclear (RN) portfolio focuses on addressing the security threat posed by radiological and nuclear materials. There are several threat areas associated with RN materials. Direct vulnerabilities include the threat of nuclear terrorism and nuclear accidents, while indirect vulnerabilities derive from those risk areas and include, for example, nuclear legacy issues, border security, emergency management and critical infrastructure. Terrorism, whether by extremist groups, radicalized individuals or criminals is still a plausible threat and, according to the Canadian Security Intelligence Service (CSIS), it is the greatest threat to the national security of Canada.[1] Although there is debate[2] on the margin of nuclear safety that now exists more than a decade after 9/11, experts agree that enhanced national and international vigilance against nuclear terrorism is necessary. The U.S. – Russia Joint Threat Assessment on Nuclear Terrorism[3] concluded that *nuclear terrorism is a real and urgent threat*. In addition to the extremism exhibited by radical groups, the threat drivers include the availability of information on nuclear technology, the availability of weapons-useable nuclear materials, and the globalized economy which facilitates the movement of technology, materials and people.

The portfolio investment strategy is focused on developing and implementing S&T solutions to strengthen capabilities in the pillars of emergency management: prevent, prepare, respond and recover. By horizontal support of other government organizations, it works to identify and fill gaps across the response spectrum. As the RN threat is evolving, so is the RN portfolio's objectives. Broad goals of the portfolio include: improving capability for early detection, location and identification of RN threat materials, including Special Nuclear Materials (SNM); developing methodologies, tools, and networks to minimize the impacts of a radiological event; enhancing forensic capabilities in conjunction with policing organizations; developing tools and protocols to facilitate scientific reach-back for those on the front lines; supporting exercises and real-world operations through the deployment of knowledge and S&T solutions; and capacity building.

The RN portfolio engages with these partners primarily through the RN community of practice (CoP). The RN CoP includes a number of key partners across the Canadian federal government, all of whom are engaged in work related to radiological or nuclear materials as part of their departmental mandates. These include Health Canada, AECL, CBSA, CNSC, CSIS, DND/DRDC, DFATD, Environment Canada, NRC, NRCan, PHAC, PS Can, RCMP, and Transport Canada. Annex A provides an overview of each of their roles and mandates in nuclear safety and security issues.

Other active members of the RN CoP are outside the Federal Families and include academia and private sector companies. The RN CoP has very little or no municipal, provincial and territorial

[1] Canadian Security Intelligence Service, Public Report 2010–2011, p11.
[2] Todd Masse, Nuclear Terrorism Redux: Conventionalists, Skeptics, and the Margin of Safety, Orbis, Spring 2010.
[3] The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism, Belfer Center for Science and International Affairs and the Institute for U.S. and Canadian Studies, May 2011, p10.

partners at this time. However, recent projects addressing first receiver gaps have engaged some provincial and regional actors[1].

Other partners and organizations that are regularly engaged through portfolio activities but who are not regular members of the RN CoP also have an influence on our program direction through consultation and funding of activities of common interest. They include the Technical Support Working Group (TSWG), the Domestic Nuclear Detection Office (DNDO) within the Department of Homeland Security (DHS), UK scientists at the Atomic Weapons Establishment (AWE[2]), and the Quadrilateral Group on Chemical, Biological and Radiological Counterterrorism, formed by Australia, Canada, the UK and the US.

Policy and Operational Context

Strategic direction of the RN Portfolio is provided by a number of federal statements, action plans and policy documents.

The core principal of Canada's counter-terrorism strategy[3] revolves around building a more resilient society against violent extremist ideologies. It is anchored on the four elements of *Prevent, Detect, Deny and Respond* and specifically refers to the CBRNE threat and emphasizes the need to prevent access to CBRNE materials. These elements map very well with the activities of the RN portfolio and can be used as a metric against which to assess the balance of investment within the portfolio.

Another key strategy that drives the work of the RN portfolio is the Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy for Canada.[4] This strategy recognizes the unique global challenge of the CBRNE threat and is implemented through its associated Action Plan.[5] Examination of selected action items of the plan that have a specific S&T dimension[6] outlines recurring themes behind the Action Plan that are aligned very well with the activities of the RN portfolio. These include the need for a strong S&T knowledge network and reach-back capabilities through community development activities, workshops, R&D and knowledge development, including national and international engagement as input to policy and program development; evidenced-based assessment of emerging CBRNE threats and risks and their mitigation strategies; capability-based planning of CBRNE investments across all components of emergency management including the role, capacity and function of laboratories during CBRNE events; and interoperability through common tools, equipment, technology and procedures, including their development through training, exercises and education.

---

[1] CSSP project Early Triage for Radiological and Nuclear Events (ETRNE), CSSP-2013-CP-1009.
[2] AWE is home to the U.K.'s nuclear deterrent but also provides S&T solutions to national nuclear security issues: http://www.awe.co.uk/ .
[3] Building Resilience Against Terrorism, Canada's counter-terrorism strategy, 2nd edition, Government of Canada, 2013, ISBN: 978-1-100-22422-0.
[4] Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy for Canada, Government of Canada, January 2011, ISBN: 978-1-100-17623-9.
[5] Chemical, Biological, Radiological, Nuclear and Explosives Resilience Action Plan for Canada, Government of Canada, January 2011, ISBN: 978-1-100-17649-9.
[6] This is solely based on the author's assessment. Bearing in mind that some of the strategic objectives intersects science, policy and program objectives. The reader should consult the CBRNE Action Plan for a fuller assessment.

Canada's counter-terrorism and CBRNE strategies are complemented by civil emergency plans and policies.[1] The response to a nuclear emergency in Canada is supported by the FNEP,[2] which coordinates the federal technical and scientific preparedness and response to RN emergencies. The plan, albeit not explicitly addressing policy, has a predominant influence on the RN portfolio through its S&T multi-organization governance. Through exercises, support to security and surveillance, and gap analysis, the actors of the plan (e.g., members of the Federal Radiological Assessment Team) provide regular input to the strategic direction of the RN portfolio.

As we have seen recently during the Fukushima-Daiichi accident, nuclear emergencies and RN threats transcend borders and have trans-national effects. Consequently, there are a number of additional international commitments that provide guidelines to the strategic direction of the RN portfolio.

The Nuclear Security Summit, initiated by President Barack Obama in 2010, provides a forum for world leaders to establish objectives toward the prevention of nuclear terrorism around the globe.[3] The last summit, held in The Hague in 2014, was an occasion for world leaders to assess progress made since 2010 and chart the path for future years. The Communiqué of 2014[4] reaffirms the fundamental responsibility of States in securing RN materials and the role of international cooperation in nuclear security; acknowledges the contributions of the Global Initiative to Combat Nuclear Terrorism (GICNT) and the Global Partnership Program (more on that below); and reaffirms the need to maintain effective emergency preparedness, response and mitigation capabilities for nuclear safety and security. Furthermore, the communiqué outlines specific areas requiring attention over the coming years:

- **Information and cyber security** recognises the growing concerns to information security and computer systems and the need for further cooperation between government, industry and academia to prevent their exploitation for malicious purposes. It further emphasises the need to address the *growing threat of cyber attacks, including on critical information infrastructure and control systems, and their potential impact on nuclear security.*[5]
- **Nuclear transportation** *reaffirms the determination to further enhance the security of nuclear and other radioactive materials while in domestic and international transport.*[6]
- **Illicit trafficking** underlines *the vital importance of using all tools at our disposal to locate and secure nuclear material out of regulatory control* [including] … *nuclear detection, forensics, law enforcement, and the development of new technologies to enhance enforcement capacity of customs personnel.*[7]
- **Nuclear forensics** welcomes *the progress and recent development of several instruments that improve the use of traditional forensic methods, and emphasizes the need to further develop innovative forensic methods and tools for investigating incidents involving*

[1] See, for example, the Emergency Management Act, Government of Canada, S.C. 2007, c. 15; and E.g. Federal Emergency Response Plan, Government of Canada, January 2011.
[2] The Federal Nuclear Emergency Plan, Ibid.
[3] Work Plan of the Washington Nuclear Security Summit, Washington, D.C., 2010.
[4] The Hague Nuclear Security Summit Communiqué, The Hague, Netherlands, 25 March 2014.
[5] Ibid., p. 6.
[6] Ibid., p. 6.
[7] The Hague Nuclear Security Summit Communiqué, Ibid., p. 6.

nuclear and other radioactive materials. It further encourages *enhancing traditional and nuclear forensics capabilities, where feasible, and establishing national nuclear forensics databases to enable better determination of the origin of material*[1].

The Global Initiative to Combat Nuclear Terrorism (GICNT[2]), jointly initiated in 2006 by Russia and the U.S., is a voluntary international partnership of nations and international organizations which aims to strengthen global capacity to prevent, detect and respond to nuclear terrorism. The GICNT pursue three objectives: to strengthen the overall counter-terrorism global architecture by integrating collective capabilities and resources; to bring together expertise in non-proliferation, counter-proliferation and counter-terrorism; and to provide a forum for nations to share expertise. It does so through three themes organized in working groups: nuclear detection, nuclear forensics and response/mitigation. The influence of the GICNT strategic vision is exercised through yearly senior-level plenary meetings where past achievements are reviewed and where the strategic vision and future priorities are established.

Through the Global Partnership Program (GPP[3]), Canada supports the international efforts to combat the risks associated with Weapons of Mass Destruction (WMD) proliferation and terrorism. Previously focused on the threat from countries of the former Soviet Union, the program is now implementing projects in the Americas, Africa, Asia and the Middle East. Since the renewal of the program in 2012, the RN investments focus on five pillars: physical protection of nuclear materials, safe and secure transportation of nuclear materials, radiological security, preventing illicit nuclear trafficking and the reduction of nuclear materials and plutonium disposition.

The International Atomic Energy Agency (IAEA[4]) also provides influence, through Canada's international non-proliferation and safeguards commitments and its support of the agency's mission. Since the Fukushima accident, the agency has strengthened its commitment to *nuclear safety, emergency preparedness and radiation protection of people and the environment.*[5] Furthermore, the IAEA publishes nuclear security technical guidance and recommendations relating to the *prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities*.[6] The IAEA[7] also collects and distributes data on the number of incidents involving illicit nuclear trafficking.

The Speech from the Throne, which opens every parliamentary session, and the Federal Budgets also provide valuable insight into the Government of Canada's immediate priorities. In its last three budgets,[8] the Government of Canada seeks to improve the secure and efficient flow of

[1] Ibid., p. 6–7.
[2] www.gicnt.org.
[3] www.international.gc.ca/gpp-ppm/global_partnership-partenariat_mondial.aspx.
[4] www.iaea.org.
[5] IAEA Action Plan on Nuclear Safety, endorsed by the IAEA General Conference during 22 September 2011.
[6] http://www-ns.iaea.org/security/ .
[7] Incident and Trafficking Database: http://www-ns.iaea.org/security/itdb.asp .
[8] The road to balance: creating jobs and opportunities, Minister of Finance, Government of Canada, 11 February 2014; Jobs, growth and long-term prosperity, Economic Action Plan 2013, Government of

goods and people across the border. The Canada-U.S. Beyond the Border Action Plan provides a road map to accelerate trade at border while enhancing security.[1] The plan calls for the development of common approaches to assessing threats and identifying those who pose a risk, preparation of joint, integrated threat assessments to improve intelligence and national-security information sharing, developing a harmonized approach to screening inbound cargo and investment in improving shared border infrastructure and technology. The plan also specifically identifies needed improvements in bilateral capabilities for emergency management of CBRNE events:

- Establish joint training opportunities and share lessons learned to enhance preparedness for, and response to, CBRNE events in both countries;
- Establish bilateral information-exchange opportunities to share advancements in policies, plans, science and technology, and lessons learned;
- Establish a strategy that can enhance bilateral interoperability for conducting CBRNE response; and
- Develop a mutual-assistance CBRNE concept of operations.[2]

Program of Work

One of the bases for informing investment priorities is through quantitative and qualitative threat assessment and risk informed methodologies. The analysis of nuclear security threats and risks differs from traditional assessment involving common criminal acts for several reasons:

- The limited number of nuclear security events impedes on the ability to accurately assess risk and threat; hence the ability to identify useful metrics is difficult.
- Technical capability and scientific knowledge of RN materials are an essential element of the threat assessment.
- The availability and potential use of RN materials is a defining aspect of the threat assessment.[3]

The risk scan[4] produced, through interviews with subject matter experts, portfolio managers and CoP leaders, a risk assessment capability profile for CBRNE and forensics. It concluded that the RN domain was mature and well understood with a broad spectrum of science-based and first responder stakeholders. The analysis reveals that the CBRNE capability has evolved from a terrorism-centric focus of understanding threats and hazards to a broader focus that includes industrial accidents, consequence management and resilience. The risk scan identified communications within and across the stakeholders' communities as a major challenge and the availability of intelligence to non-federal communities as an area of concern.

Canada, 21 March 2013; and Jobs, growth and long-term prosperity, Economic Action Plan 2013, Government of Canada, 29 March 2012.

[1] Beyond the border: a shared vision for perimeter security and economic competitiveness, action plan, Government of Canada, 2011. ISBN: 978-1-100-53904-1.

[2] Ibid, p. 30.

[3] Threat assessment and risk-informed approach for implementation of nuclear security measures for nuclear and other radioactive material out of regulatory control, draft implementing guide, to be published, IAEA, Vienna.

[4] I. Bayne and S. K. Friesen, Risk scan: a review of risk assessment capability and maturity within the CSSP, DRDC-RDDC-2014-R36, June 2014.

The Consolidated Risk Assessment[1] is also used to inform program investment priorities. However, because its output depends on intelligence assessments, it is classified Secret. The CRA process consists of analysing a set of relevant vignettes for their technical feasibility and potential impact to achieve a vulnerability assessment, which is combined with an intelligence assessment that considers the capability and intent of groups to carry out such an attack, resulting in a series of risk ratings for each vignette. This provides a means to prioritize the most pressing scenes and to evaluate the effort needed to mitigate the potential impact.

Additional sources of input into the RN portfolio investments include gap analysis, CoP workshops, table top and field exercises, presence at major events through science town and lessons learned from major events.

Annex B lists the RN portfolio investments for 2012/13 and 2013/14. These investments are in line with previous observations, policy drivers, risk analysis and gap assessments. Broad areas of current and future work are delineated below:

- The current Targeted Investment initiative in ***Nuclear Forensics*** is a significant example of the S&T role that CSS plays towards the development of national instruments and strategies to combat illicit nuclear activities, and to respond to nuclear accidents. The natural development for this capability is in a National Nuclear Forensics Program which would then evolve towards providing support to national security practitioners. Hence it is envisaged that the future work in the RN portfolio will address gaps identified during the pilot project and facilitate the operationalization of nuclear forensics to first responders. Therefore two areas of priorities include:
  - Scoping work to identify gaps in nuclear forensics capability in Canada
  - Workshop and exercises of Nuclear Forensics products by first responders

- ***Detection of Special Nuclear Material (SNM)*** at borders is still an issue. CSSP has made significant investment in this area in the past. However, the S&T under development has yet to manifest itself at the operational level. Priority areas:
  - Review of existing and emerging technologies for detection and interception of SNM at borders, with the intent of identifying promising candidates.
  - Experimental program of field trials such that promising S&T at low TRL can be advanced if successful.
  - Implementation of replacement technology for portal monitors at borders.

- Investments in ***exercises and capability reach-back*** from operational theatres are core competencies of the CSS. Areas of priority, in response to perceived and actual gaps, include:
  - Defining role and responsibilities following an RN event or Nuclear Emergency.
  - Support training issues and non-core mandate initiatives in the RN community.
  - Tools and protocols to facilitate S&T reach-back.

[1] CBRNE Consolidated Risk Assessment, DRDC CSS R 2010-01, May 2010.

- Implication and involvement of trans-jurisdictional actors (provincial/municipal) and first receivers.
- Harmonisation and/or exploitation of cross-cutting capabilities.

- Past cyber-attacks have shown that power plants can be vulnerable. ***Cross-cutting objectives with critical infrastructure protection*** will be identified and a plan to better understand the vulnerabilities and S&T solutions developed.

- As we have seen recently (i.e. Fukushima-Daiichi), RN events and threats transcend borders and therefore future priorities in this portfolio should encourage linkage, harmonisation and ***exploitation of cross-cutting capabilities with our partners*** (UK/US). This includes encouraging initiatives that contribute to international counter-terrorism fora, including the Global Initiative to Combat Nuclear Terrorism, the Nuclear Security Summit and the Global Partnership Program.

Annex A: List of Federal Partners

The following lists of Federal partners are actively involved in the activities of the RN Portfolio via projects and other activities of the Community of Practice (workshops, science day, etc.). We provide below a short list of their role and mandate in nuclear safety and security issues.

- Atomic Energy of Canada Ltd (AECL).[1] *As Canada's premier nuclear science and technology (S&T) organization AECL serves an important public policy role in nuclear matters, providing advice, counsel and service as an agent of the federal government.*

- Canadian Border Services Agency (CBSA).[2] *To ensure the free flow of legitimate people and goods, the CBSA monitors, investigates, detains and removes those people or goods in violation of the relevant laws. We do this by putting in place programs and services to: ensure trade security, manage access to Canada and work together with business and other government organizations.*

- Canadian Nuclear Safety Commission (CNSC)[3]. *The Canadian Nuclear Safety Commission (CNSC) makes independent, fair and transparent decisions on licensing nuclear related activities. The Commission is supported by more than 800 scientific, technical and professional staff which ultimately enforce compliance with the Nuclear Safety and Control Act, regulations, and any license conditions imposed by the Commission.*

- Defence Research and Development Canada Ottawa (DRDC – Ottawa). *DRDC – Ottawa Research Centre is the DND's lead authority and centre of expertise for radiation effects.*

- Department of Foreign Affairs, Trade and Development (DFATD)[4]. *The mandate of Foreign Affairs, Trade and Development Canada is to manage Canada's diplomatic and consular*

[1] www.aecl.ca.
[2] www.cbsa-asfc.gc.ca.
[3] www.nuclearsafety.gc.ca.
[4] www.international.gc.ca.

relations, to encourage the country's international trade and to lead Canada's international development and humanitarian assistance.

- Department of National Defence – Directorate Nuclear Safety (DNSafe). DNSafe is the nuclear regulatory arm of DND. The exclusion of DND from the Nuclear Safety and Control Act (see CNSC above) is in recognition of its unique mandate and special requirements, such as the need to control operational readiness and national security.

- Environment Canada (EC)[1]. Environment Canada as a department is responsible for preserving and enhancing the quality of the natural environment, providing meteorological services, and coordinating policies and programs to achieve environmental objectives. One of the department missions is to protect Canadians and their environment from the effects of environmental emergencies through the provision of science-based expert advice and regulations.

- Health Canada (HC)[2]. HC is a science based department responsible for helping Canadians maintain and improve their health. Within HC, the Radiation Protection Bureau (RPB) *promotes and protects the health of Canadians by assessing and managing the risks posed by radiation exposure in living, working and recreational environments*[3]. The RPB also *leads the coordination of federal nuclear emergency preparedness and providing Health Canada's technical support to the Federal Nuclear Emergency Plan (FNEP)*.

- National Research Council (NRC)[4]. NRC is the Government of Canada's premier research and technology organization. Working with clients and partners, it provides innovation support, strategic research, scientific and technical services.

- Natural Resources Canada (NRCan)[5]. *NRCan has a responsibility to create a sustainable resource advantage for Canadians – now and in the future*. The department has a diverse portfolio that ranges from energy, mining, forestry, and environmental sciences and includes areas that intersects the threat landscape of the CSSP, such as natural hazards and explosives. The minister of Natural Resources is responsible for Atomic Energy of Canada Ltd.

- Public Safety Canada (PS Can)[6]. *Public Safety Canada was created in 2003 to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians.* The mandate of PS Can is *to keep Canadians safe from a range of risks such as natural disasters, crime and terrorism. Public Safety coordinates an integrated approach to emergency management, law enforcement, corrections, crime prevention and border security.*

---

[1] www.ec.gc.ca.
[2] http://www.hc-sc.gc.ca/.
[3] http://www.hc-sc.gc.ca/ahc-asc/branch-dirgen/hecs-dgsesc/sep-psm/rpb-br-eng.php.
[4] http://www.nrc-cnrc.gc.ca/ .
[5] http://www.nrcan.gc.ca/.
[6] http://www.publicsafety.gc.ca.

- Royal Canadian Mounted Police (RCMP)[1]. The RCMP is the Canadian national police service and an agency of the Ministry of Public Safety Canada. The mission of the RCMP is quite broad as it provides policing services at the national, territorial, provincial, municipal and aboriginal communities level. The RCMP's works to prevent, detect, deny and respond to criminal activity, including the threat of terrorism, one of its strategic priorities. The RCMP maintains CBRN response capability.

- Transport Canada (TC)[2]. TC *is committed to keeping Canada's air, marine, rail and road transportation systems among the safest in the world*. The department also develops the regulation on the transportation of dangerous goods and provides oversight during accidents involving the transportation of dangerous goods.

Annex B: 2012/13 and 2013/14 Investment Portfolio

CSSP-2014-CP-2020	Medical Countermeasures for Removing Insoluble Radioactive Materials in Lungs
CSSP-2013-CP-1029	Infrastructure mitigation for a rapid response after a radiological incident
CSSP-2013-CP-1011	The Application of Gravity Gradiometry for the Detection of Special Nuclear Material in Cargo Containers
CSSP-2013-CP-1010	Radiological/Nuclear Medical Emergency Preparedness and Response
CSSP-2013-CP-1013	High-fidelity, multi-scale atmospheric dispersion modeling of natural, accidental or malicious releases of toxic agents in the atmosphere
CSSP-2013-CP-1009	Early Triage for Radiological and Nuclear Events (ETRNE)
CSSP-2013-CD-1134	continuing RAP - Biomarkers of Alpha Particle Exposure
CSSP-2013-CD-1133	Field validation of novel algorithms for imaging
CSSP-2013-CD-1132	Bayesian Inference for Source Reconstruction Demo
CSSP-2013-CD-1131	Atmospheric Dispersion from RDDs
CSSP-2013-CD-1130	continuing RAP - Advanced Methods
CSSP-2013-CD-1129	Can US Interop for Airborne Gamma Surveying
CSSP-2013-CD-1128	Boron lined neutron detector evaluation for border security
CSSP-2013-CD-1127	FRAT Training (formerly FRAT Workshop)
CSSP-2012-TI-1119	Canadian National Nuclear Forensics Capability Pilot
CSSP-2012-CD-1115	RAP Student in Advanced Methods for Radioactive Source Localization and Characterization
09-0606TA	Compact OSL-Based Area Monitor (COSLAM)
09-0566TA	Upgrades to the Directional Gamma Ray / Sensitive Directional Gamma Ray Probes
09-0553TD	Children and Radiological/Nuclear Events
09-0511RD	Next Generation Stand-off radiation detection using nanosensors
09-0445TA	Actinide and Fission Fragment Measurements in Forensic Materials and Biological Samples by Accelerator Mass Spectrometry
08-0222RD	Stand-Off Radiation Detection by Air Radiolysis (SORDAR)

[1] http://www.rcmp-grc.gc.ca.
[2] http://www.tc.gc.ca.

This page intentionally left blank.

Annex L Surveillance, Intelligence, and Interdiction

Overview

The Surveillance, Intelligence and Interdiction portfolio was established to focus advanced science and technology and its application in intelligence and national security operations to strengthen Canada's ability to anticipate, prevent/mitigate, and prepare for acts of terrorism, espionage activities or other national security threats.

The Portfolio's two key sub-objectives are: (1) To enable the Government of Canada to develop, deploy and use S&T solutions in the broad subject areas of surveillance, intelligence and interdiction; and (2) To enable the Government of Canada to protect its assets and people through S&T solutions. The fields of science involved are diverse as solutions to surveillance, intelligence and interdiction problems may reside in the fields of physics, engineering, social sciences or any other relevant fields, or even be multidisciplinary.

Public Safety Canada, security and intelligence agencies (primarily CSIS and the RCMP), the Departmental Security Officers' (DSO) Readiness Committee (which reaches all departments and agencies), and the Global Navigation System Satellite (GNSS) Governance Working Group (7 member federal departments and agencies) are the portfolio's primary partners.

The Portfolio Manager represents DRDC CSS at the DSO Readiness Committee (six meetings a year) and attends the meetings of the Committee's Defence and S&T Cluster (also six meetings a year). He/she also attends monthly GNSS meetings chaired by Industry Canada and Public Safety Canada's meetings of relevance to the Portfolio. He/she maintains individual relationships with the project managers of CSSP-funded projects as well as working-level and supervisory officials within the portfolio's primary partner organizations. Finally, he/she attends ad hoc events of interest to the portfolio that are hosted by partner organizations (such as scientific meetings and academic presentations).

Policy and Operational Context

Several public documents provide strategic direction relevant to this Portfolio:

- **Action Plan - Air India Commission of Inquiry (2010).** In its Action Plan in response to the report of the Air India Commission of Inquiry, the Government said that it will: (1) enhance cooperation among Canada's law enforcement and intelligence agencies, in particular information sharing for national security purposes; (2) examine ways to improve how security intelligence is collected and retained; and (3) explore the process of disclosure and the obligations of security intelligence agencies. Each of these priorities is an important enabler to the Security & Intelligence community to fulfil its mandate.

- **Perimeter Security & Economic Competitiveness Action Plan (2011).** In its Action Plan on Perimeter Security & Economic Competitiveness, the Government said that it will: (1) Develop a common approach to assessing threats and identifying those who pose a risk; (2) Enhance our shared understanding of the threat environment through joint,

integrated threat assessments, improving our intelligence and national-security information sharing; (3) Share information and intelligence in support of law enforcement and national security. In its December 2012 implementation report, the Government of Canada noted that it had worked closely with its U.S. counterpart and met each of these three objectives. Taken together, they speak to the necessity for intelligence analysts, this time across our southern border, to work closely together and share intelligence assessments that are timely and relevant.

- **Canada's Counter-Terrorism Strategy (2011).** Canada's Counter-Terrorism Strategy emphasizes that it will operate through four mutually reinforcing elements: (1) Prevent: Addressing the factors that may motivate individuals to engage in terrorist activities (2) Detect: Identifying terrorists, terrorist organizations and their supporters, their capabilities and the nature of their plans through investigation, intelligence operations and analysis. Strong intelligence capabilities and a solid understanding of the changing threat environment is key. This involves extensive collaboration and information sharing with domestic and international partners (3) Deny: Denying terrorists the means and opportunities to pursue terrorist activities through mitigating vulnerabilities and aggressively intervening in terrorist planning, and making Canada and Canadian interests a more difficult target for would-be terrorists, and (4) Respond: Developing Canada's capacities to respond proportionately, rapidly and in an organized manner to terrorist activities and to mitigate their effects. To succeed, the implementation of the "prevent," "deny" and "respond" pillars depends on the "detect" pillar; that is, on the capabilities and abilities of intelligence analysts to provide, from both a domestic and an international perspective, that "solid understanding of the changing threat."

- **Action Plan 2010-2015 for Canada's Cyber Security Strategy (2013).** Quite simply, the Action Plan noted that starting in 2012 the Government of Canada will: Increase capacity to collect and analyze intelligence.

The Portfolio Manager also refers to priorities established by the portfolio's primary partners. These include the S&T priorities established by the DSO Readiness Committee in its *Annual Report 2013-2014*, the priorities for 2014-2017 developed by the GNSS Governance Working Group and those priorities highlighted by specific partners in public documents such as their Reports to the Treasury Board on Plans and Priorities of web pages (for example, CSIS's priority areas listed at http://www.csis-scrs.gc.ca/prrts/index-eng.asp).

Finally, the Portfolio's focus is also informed by analyses of S&T problems produced by government departments and agencies and the academic community. This large body of work is used to identify issues of concerns and new avenues of scientific research that could assist government departments and agencies in meeting their respective objectives.

The following sources are illustrative of the several thousand sources available:

- *Intelligence and Security Informatics* International Workshops proceedings, released annually as part of the Lecture Notes in Computer Science published by Springer-Verlag in Berlin;
- Valérie Lavigne and Denis Gouin, "Visual Analytics for cyber security and intelligence," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, Vol. 11, 2014;
- Proceedings material from the conference on "Understanding and Improving Intelligence Analysis: Learning from other Disciplines," London, 12-13 July 2012;
- Kevin S. Ni, Daniel Faissol, Thomas Edmunds and Richard Wheeler, "Exploitation of Ambiguous Cues to Infer Terrorist Activity," *Decision Analysis*, Vol. 10, No. 1, March 2013;
- Baruch Fischhoff and Cherie Chauvin, eds, *Intelligence Analysis*, Behavioral and Social Scientific Foundations, National Research Council of the Academies, Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security, Washington, D.C. National Academies Press, 2011;
- The Royal Academy of Engineering, *Global Navigation Space Systems: Reliance and Vulnerabilities*, London, 2011.

Program of Work

The projects currently within the Portfolio (listed below) do not form a coherent whole given how broad the remit of the portfolio is. Each, however, reflects the priorities of partner organizations and can be linked to higher-level strategic direction as follow:

National Strategies	Priorities/ Recommendations	Project#/Name
Action Plan – Air India Commission of Inquiry (2010) CSIS Priority Areas	Enhance cooperation among Canada's law enforcement and intelligence agencies, in particular information sharing for national security purposes	CSSP-2013-TI-1054 DSO Security Commons CSSP-2013-CD-1095 Geomatics in Support of DSO Community
	Examine ways to improve how security intelligence is collected and retained	CSSP-2014-TI-2056 Project ZIZEL
Canada's Counter-Terrorism Strategy (2011)	Prevent: Addressing the factors that may motivate individuals to engage in terrorist activities	CSSP-2014-CP-2018 Countering Violent Radicalization

	Detect: Identifying terrorists, terrorist organizations and their supporters, their capabilities and the nature of their plans through investigation, intelligence operations and analysis. Strong intelligence capabilities and a solid understanding of the changing threat environment is key. This involves extensive collaboration and information sharing with domestic and international partners	CSSP-2014-TI-2056 Project ZIZEL CSSP-2014-TI-2037 Structured Analytic Techniques (SAT) Validation Study
	Deny: Denying terrorists the means and opportunities to pursue terrorist activities through mitigating vulnerabilities and aggressively intervening in terrorist planning, and making Canada and Canadian interests a more difficult target for would-be terrorists	CSSP-2013-CP-1025 Detection and Geo-Location of Low-cost Jammers
DSO Readiness Committee Priorities	To enable the Government of Canada to protect its assets and people through S&T solutions	CSSP-2013-TI-1054 DSO Security Commons CSSP-2013-CD-1095 Geomatics in Support of DSO Community

The S&T components of these projects are helping the Portfolio meet its objectives through the

- development and testing of tools for improving the analysis of security and intelligence problems across government;
- development, testing and deployment of solutions to counter the ability of adversaries (i.e., terrorists and spies) to evade detection and surveillance; and
- mitigating government of Canada vulnerabilities in the protection of its people and assets

For the foreseeable future, it is assumed that:

- Protecting Government of Canada assets and people and countering the Insider Threat will continue to be a very high priority of government;
- Improving intelligence analysis has been a constant since 2001 and will continue to require S&T investments; and
- As the ability of terrorists and spies to evade surveillance constantly improves, surveillance countermeasures will be a high priority.

In order to build upon the work presently being conducted, next steps would logically include partner proposals to

- improve intelligence analysis across government (such as the testing and validation of the existing structured analytic techniques for intelligence analysis; or the development of new structured analytic techniques for intelligence analysis);
- foster horizontal solutions to surveillance and interdiction problems (these might include, but are not limited to: the development, testing and validation of new surveillance and interdiction technologies related to the fields of communications, biometrics and imagery that would assist national security and intelligence agencies in identifying terrorists,

terrorist organizations and their supporters, their capabilities and the nature of their plans); and

- increase the capability of the Government of Canada to protect its people and assets (these might include, but are not limited to: building entry/exit technologies; detecting, reporting and analyzing suspicious activities on government premises).

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Developing the CSSP Planning Process

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Greene, B.W.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
March 2017	98	2

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Reference Document

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2017-D018	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This Reference Document describes and captures work carried out between 2012 and 2015 in support of the effort to establish a strategic policy planning framework for the Canadian Safety and Security Program (CSSP), including the first group of Portfolio Narratives written in support of the initiative. It also includes a diagrammatic representation of the overall process.

Le présent document de référence énonce et décrit les travaux effectués entre 2012 et 2015 à l'appui de l'établissement d'un cadre de planification d'une politique stratégique pour le Programme canadien pour la sûreté et la sécurité (PCSS), ce qui comprend le premier groupe de descriptions de portefeuilles rédigées pour les besoins de cette initiative. Il comporte par ailleurs un diagramme représentant l'ensemble du processus.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

CSSP; Strategic Planning; Portfolio Narratives; Environmental Scan; Strategic Assessment