2014 - 2017

Action Plan
for Critical Infrastructure

Public Safety Canada
Sécurité publique Canada

Canada

Cat. No.: PS4-66/2014E-PDF
ISBN: 978-1-100-23291-1

Table of contents

Renewing Canada's Action Plan for Critical Infrastructure

1. Introduction

The *National Strategy for Critical Infrastructure* and the supporting *Action Plan for Critical Infrastructure* were announced on May 28, 2010. Together, they established a collaborative federal, provincial, territorial and critical infrastructure sector approach to strengthening critical infrastructure resilience.

The National Strategy recognized that responsibilities for critical infrastructure in Canada are shared by federal, provincial and territorial governments, local authorities, and critical infrastructure owners and operators – who bear the primary responsibility for protecting their assets and services. It also recognized that critical infrastructure owners and operators have the expertise and information that governments need to develop comprehensive emergency management plans and, in turn, that governments have information on risks and threats relevant to owners and operators in carrying out their risk management activities.

Consistent with the National Strategy, as well as the *Emergency Management Framework for Canada,* these responsibilities (see Annex A) were further elaborated in the original Action Plan. National-level sector networks were established for each of the ten critical infrastructure sectors, with a lead federal department/agency responsible for each network (see Annex B). In addition, a National Cross Sector Forum was established to promote collaboration across sector networks, address interdependencies, and promote information sharing across sectors (see Annex C).

The National Strategy identified three strategic objectives for enhancing the resilience of critical infrastructure in Canada:

- Build partnerships;
- Share and protect information; and
- Implement an all-hazards risk management approach.

Building on the National Strategy, the original Action Plan set out action items for each of the three strategic objectives. Working together, governments (federal, provincial, territorial) and the private sector have made considerable progress in building partnerships (e.g. establishing sector networks and the National Cross Sector Forum), sharing and protecting information (e.g. creating the Critical Infrastructure Gateway and developing an information sharing framework), and implementing an all-hazards risk management approach (e.g. developing risk management tools and guidance). A summary of progress achieved is available in Annex D.

Recognizing the interconnected nature of critical infrastructure, the *Canada-United States Action Plan for Critical Infrastructure (2010)* established a coordinated, cross-border approach based on Canada's *National Strategy and Action Plan* and the United States' *National Infrastructure Protection Plan.* The Canada-U.S. Action Plan calls for joint sector meetings and collaborative risk management activities. The Canada-U.S. Action Plan also supports regional cross-border relations by promoting awareness of shared critical infrastructure issues, and encouraging cooperation among State, Provincial, and Territorial authorities.

What we have learned and what has changed

The risk environment exhibits both continuity and change. For instance, terrorism is a complex and evolving threat. Released in February 2012, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* outlines the Government of Canada's overall approach to protect

Canadians and Canadian interest from domestic and international terrorism. The Counter-Terrorism Strategy highlights the importance of cooperation with Canada's international partners, all levels of government, security intelligence and law enforcement agencies, industry stakeholders and civil society. The Government subsequently released the 2013 Public Report on the Terrorist Threat to Canada which provided additional detail on evolving trends in terrorism, with a focus on what they mean for Canadians.

Cyber security has become increasingly relevant for critical infrastructure sectors. Connectivity and the world's dependence on the internet continues to grow – as has the number and significance of cyber incidents. *Canada's Cyber Security Strategy*, announced in 2010, is the Government of Canada's plan for meeting the cyber threat. The Cyber Security Strategy commits the Government to engage public-private sector partners in a collaborative effort to enhance the security of Canada's cyberspace. The *Action Plan 2010-2015 for Canada's Cyber Security Strategy* outlines the Government's plan to implement the Strategy and meet the ultimate goal of securing our cyberspace for the benefit of Canadians and our economy. It identifies actions to help secure vital cyber systems outside the Government of Canada, including for Canada's critical infrastructure sectors. These cyber-specific activities reinforce Canada's overall approach to critical infrastructure resilience.

The effects of climate change are better understood. The rate and severity of extreme weather events is expected to increase in the future. The trend of urbanization, and the growth of large cities, means that a natural disaster confined to a small area can have devastating consequences on large numbers of people and cascading effects across critical infrastructure sectors.

Globalization – as viewed through the lens of the production and trade of goods and services – has further contributed to our awareness of the role that interdependencies can play. For example, the 2011 flooding in Thailand disrupted a number of important electronics manufacturers, affecting the computer and automotive industries in particular, through their global supply chains.

At the same time, risks from purely natural hazards, such as earthquakes, persist and do not exhibit a long-term trend either upwards or downwards. As the earthquakes in Japan and New Zealand in 2011 show, losses can vary greatly in any given year. Awareness of the significance of these high-impact, low-frequency (including "black swan") events has increased. Individual events of this type are deemed improbable, yet have enormous consequences when they occur – as illustrated by earthquakes and flooding in 2011.

The *National Strategy for Critical Infrastructure* continues to provide the overarching vision for enhancing the resilience of Canada's critical infrastructure. Each of the strategic objectives of the National Strategy contribute to helping Canada better prepare and respond to these threats and hazards:

- Partnerships enhance collaboration among governments (federal, provincial, territorial) and critical infrastructure sectors. While different partners have different roles and responsibilities, effective action requires joint efforts, especially since disruptions to critical infrastructure can cross jurisdictions and affect multiple sectors.
- Multi-directional information sharing among critical infrastructure owners/operators, governments, and security and intelligence organizations (e.g. Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS), Canada Border Services Agency (CBSA), Canadian Cyber Incident Response Centre (CCIRC)) helps to inform risk management activities by keeping everyone aware of the evolving risk and threat environment.
- An all-hazards risk management approach helps prepare for a range of eventualities, whether from natural or accidental hazards, or intentional threats.

2. A Renewed Action Plan (2014-2017)

Improving the resilience of Canada's critical infrastructure will always be a work in progress. It will never be possible to protect against every threat or hazard and mitigate against every consequence; it is also important to improve the ability to respond to and recover from incidents when they occur.

The next phase of the Action Plan involves taking additional steps for each of the three strategic objectives outlined in the National Strategy, building on what has already been achieved under the original Action Plan and what the critical infrastructure community has learned since then. A table summarizing all of the action items can be found in Annex E. Taken together, the action items put forth in this renewed Action Plan will strengthen Canada's critical infrastructure resilience by helping to prevent, mitigate, prepare for, respond to, and recover from disruptions.

2.1 Sustain and Enhance Partnerships

Strengthening the resilience of critical infrastructure requires complementary and coherent action by all partners to promote effectiveness of action in a resource-efficient manner. The foundation for collaborative work and information sharing was established under the original Action Plan. The renewed Action Plan will build on these efforts by deepening existing partnerships and raising awareness of the need for collaborative action on critical infrastructure resilience. Key actions for this strategic objective are to:

- **Develop a call to action for critical infrastructure resilience:** Public Safety Canada and critical infrastructure stakeholders will clarify the rationale for critical infrastructure resilience activities and ensure the value proposition is understood by relevant audiences, including sector networks, governments, and the public.
  Timeline: Year 1 and ongoing.
- **Provide guidance to ensure appropriate representation on sector networks:** Sector networks provide standing fora for discussion and information sharing among sector-specific industry stakeholders and governments. Recognizing that each sector is unique and that representation is not expected to be uniform across each of the critical infrastructure sectors, Public Safety Canada will provide guidance to lead federal departments and agencies on appropriate coverage for sector networks. This guidance will be based on consultation and collaboration with lead federal departments and agencies, Public Safety portfolio agencies, and sector networks.
  Timeline: Year 1.
- **Address cross-sector issues through multi-sector meetings:** Multi-sector network meetings provide important opportunities for sector network members to engage directly on cross-sector issues, and share information and best practices. They also provide an additional opportunity for sector network members and Canada's security and intelligence community to share threat information. Public Safety Canada will continue to work with sector network members to co-host meetings on relevant topics.
  Timeline: Ongoing.
- **Strengthen public communications and awareness:** In collaboration with critical infrastructure partners, Public Safety Canada will promote public awareness and readiness to manage the impacts of disruptions when they occur.
  Timeline: Year 2 and ongoing.

2.2 Share and Protect Information

Information sharing and information protection are complementary elements of a strong foundation for collaborative efforts to strengthen critical infrastructure resilience. Timely information sharing across governments and critical infrastructure sectors is needed to promote effective risk management and to understand and address critical infrastructure interdependencies. At the same time, the inappropriate release of sensitive information also constitutes a risk for Canada. The sharing and disclosure of protected/classified information is governed by a range of existing federal, provincial and territorial legislation and policies.

Several information sharing arrangements were developed under the original Action Plan. The renewed Action Plan will build on these achievements by further expanding information sharing opportunities through various means, including formal agreements, virtual and physical mechanisms, and the creation and dissemination of information products. Key actions for this strategic objective are to:

- **Expand stakeholder membership and participation on the Canadian Critical Infrastructure Gateway and leverage the CI Gateway's capabilities to improve information sharing and collaboration on specific projects:** Public Safety Canada will build on the successful launch of the CI Gateway by ensuring that its membership spans the ten sectors and other key stakeholders, encouraging active membership participation, and promoting its use by sector networks and communities of practice to share information and best practices, and to work together on specific projects.
  Timeline: Year 1 and ongoing.
- **Sponsor security clearances among private sector stakeholders in order to enable increased sharing of sensitive information:** Some of the information gathered by Canada's security and intelligence community is sensitive and can only be shared with individuals with an appropriate security clearance. Public Safety Canada will work with lead federal departments and agencies to increase the number of security cleared stakeholders in the private sector.
  Timeline: Year 1 and ongoing.
- **Expand information sharing and investigate rationalization of existing information sharing arrangements:** Public Safety Canada will examine existing information sharing arrangements and consolidate where possible in order to simplify. Other opportunities to expand and rationalize information sharing will be explored, including through other *Action Plan* deliverables.
  Timeline: Year 2.
- **Provide impact assessments during unfolding events of national significance:** During an event, information and analysis are key inputs to decision-making. Dependencies and interdependencies are particular characteristics of critical infrastructure that can be difficult to take into account during an event. Alerting critical infrastructure stakeholders to potential cross-sectoral effects would help inform appropriate response measures. Public Safety Canada will monitor events of national significance and provide impact assessments as warranted.
  Timeline: Year 2 and ongoing.

2.3 Implement an All-Hazards Risk Management Approach

The original Action Plan set the foundation for a collaborative approach to risk management that takes into account accidental, intentional, and natural hazards. The renewed Action Plan will build on these achievements through various means, including: undertaking a broader range of assessments, developing risk profiles, promoting the use of appropriate standards, measuring progress toward resilience, and continuing to conduct exercises. Achieving this strategic objective will also provide greater clarity to critical infrastructure stakeholders about the identification of critical assets and systems and enable greater prioritization of activities and resources. Key actions for this strategic objective are to:

- **Implement the Regional Resilience Assessment Program (RRAP) across Canada:** The goal of the RRAP is to identify and analyze the resilience and interdependencies of critical infrastructure sectors using an all-hazards approach. The RRAP process involves site assessments, training, and exercises. Assessments can be conducted at the individual facility or regional (including cross-border) level. To conduct these assessments, Public Safety Canada will work with appropriate critical infrastructure stakeholders, including provinces/territories, local authorities, and other partners, which will vary from assessment to assessment. Public Safety Canada will consult sector networks to determine the best areas of focus.
  Timeline: Year 1 and ongoing.
- **Provide an overall description of key risks for critical infrastructure, including dependencies and emerging trends:** Public Safety Canada will work with sector networks to create a *National Risk Profile of Critical Infrastructure.* The National Risk Profile will provide an overview of the risk and threat environment for Canada's critical infrastructure, help identify cross sectoral dependencies and interdependencies, give an understanding of significant trends, and identify major cross cutting threats. This overview could be used by sectors to inform and prioritize their risk management activities.
  Timeline: Year 1 and ongoing.
- **Assess impacts of potential high impact/low frequency events on critical infrastructure sectors to increase awareness and understanding of risks to critical infrastructure:** High impact, low frequency (including "black swan") events are rare but devastating events that require special attention due to the potential for massive loss should they occur. Public Safety Canada will work with critical infrastructure sectors to prioritize scenarios and issues for assessment by subject matter experts.
  Timeline: Year 1 and ongoing.
- **Promote the adoption of existing standards and determine whether additional standards are needed to improve critical infrastructure resilience:** Standards provide a useful tool for owners/operators to incorporate good practice into their business activities. Public Safety Canada will work with sector networks to identify existing standards and potential gaps, as well as to determine the best way to promote adoption of existing standards and encourage the development of new standards where appropriate.
  Timeline: Year 1 and ongoing.

7

- **Conduct exercises to strengthen readiness and response efforts:** Exercises provide an efficient means to test, evaluate, and improve planning; allow for practice in a low risk environment for responders, emergency managers and senior officials at all levels of government; and are a means to conduct quality assurance of the response to disruptions. Public Safety Canada will take advantage of existing planned exercises to enable inclusion of critical infrastructure-related content and participation of critical infrastructure stakeholders. Public Safety Canada will also consider whether additional exercises are needed – both discussion-based and physical – to complement already existing exercises.
  Timeline: Year 1 and ongoing.
- **Develop targeted risk assessment products in response to emerging critical infrastructure issues:** Public Safety Canada will produce additional information products to support the risk management efforts of critical infrastructure stakeholders. Products could be scenario-based or focus on the implications of emerging issues. These products would be validated with stakeholders to ensure relevance and inclusion of key considerations.
  Timeline: Year 2 and ongoing.
- **Finalize national application of an interdependencies model:** Public Safety Canada will work with the critical infrastructure sector networks to model dependencies within and across sectors at the national level. Public Safety Canada will also work with interested provincial and territorial counterparts to implement the model at the provincial and territorial level.
  Timeline: Year 2.
- **Measure progress toward resilience to demonstrate results and monitor progress:** Establishing resilience goals and measuring progress will enable critical infrastructure stakeholders to demonstrate results from their resilience activities – both within and across sectors. In addition, measuring changes in critical infrastructure resilience at the owner/operator level will allow for critical infrastructure sectors to monitor their progress toward improving resilience. Public Safety Canada will work with sector networks to establish resilience goals at the national and sector network levels, put in place a regular progress reporting process, and generate regular reports showing progress achieved toward these goals.
  Timeline: Year 2 and ongoing.

3. Strengthening Critical Infrastructure Resilience Efforts Across Canada

The *National Strategy for Critical Infrastructure* continues to define the overall approach to enhancing critical infrastructure resilience in Canada and support the coherence of government (federal, provincial, territorial) and private sector plans and activities. Among other partnership activities, coherence of activity across critical infrastructure sectors and federal/provincial/territorial governments is achieved through the National Cross Sector Forum and the Federal-Provincial-Territorial Critical Infrastructure (FPT CI) Working Group:

- The National Cross Sector Forum includes representatives from each of the ten critical infrastructure sectors. The annual meeting is co-chaired by the Deputy Minister of Public Safety Canada and a provincial/territorial representative.
- The FPT CI Working Group is the standing forum and primary conduit for federal/provincial/territorial government collaboration on critical infrastructure matters. Meetings are co-chaired by Public Safety Canada and a provincial/territorial representative.

Annex A – Roles and Responsibilities

Actor	Role	Responsibilities
Federal government	Lead federal activities	• Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure • Collaborate with provincial and territorial governments to achieve the objectives of the Strategy • Collaborate with national associations • Collaborate with critical infrastructure owners and operators within federal mandate in consultation with provinces and territories
Provincial/ territorial governments	Lead provincial/ territorial activities	• Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure • Collaborate with federal, provincial and territorial governments to achieve the objectives of the Strategy • Coordinate activities with their stakeholders, including municipalities or local governments where it applies, associations and critical infrastructure owners and operators
Critical infrastructure owners/operators	Collaboratively manage risks related to their critical infrastructure	• Manage risks to their own critical infrastructure • Participate in critical infrastructure identification, assessment, prevention, mitigation, preparedness, response and recovery activities

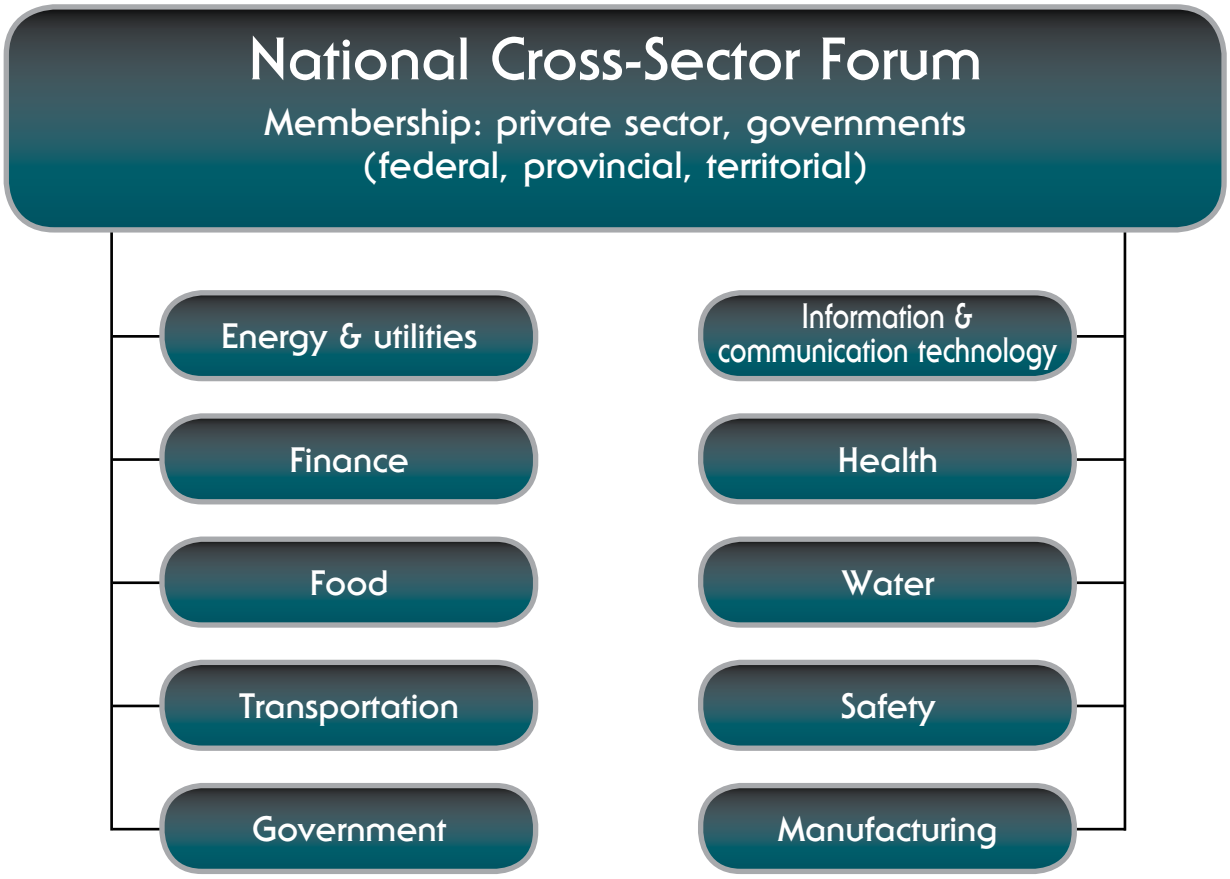
Source: Action Plan for Critical Infrastructure (2010)

Annex B – Sector Networks and Federal Departments/Agencies

Sector	Sector-specific federal department/agency
Energy and utilities	Natural Resources Canada
Information and communication technology	Industry Canada
Finance	Finance Canada
Health	Public Health Agency of Canada
Food	Agriculture and Agri-Food Canada
Water	Environment Canada
Transportation	Transport Canada
Safety	Public Safety Canada
Government	Public Safety Canada
Manufacturing	Industry Canada Department of National Defence

Source: Action Plan for Critical Infrastructure (2010)

Annex C – Sector Networks and the National Cross Sector Forum



Source: National Strategy for Critical Infrastructure (2010)

Annex D – Achievements under Phase One of the *Action Plan for Critical Infrastructure* (2010-2013)

Strategic Objective	Action Item	Year	Status
Build Partnerships	Establish sector networks	1	Completed
	Establish National Cross Sector Forum	1	Completed
	Renew FPT CI Working Group	1	Completed
Share and Protect Information	Establish an information sharing framework	2	Completed
	Develop statement of requirements for the information sharing portal	1	Completed
	Establish the Public Layer of the information sharing portal	2	Completed
	Develop and test secure, web-based user authentication	2	Completed
	Implement the Secure Layer of the information sharing portal	2	Completed
	Enhance information dissemination	Ongoing	Ongoing
	Populate Public and Secure Layers of the information sharing portal	Ongoing	Ongoing
Implement an All-Hazards Risk Management Approach	Develop risk assessments of CI in Canada	2 and ongoing	Ongoing
	Develop and share sector-specific work plans	3 and ongoing	In progress
	Conduct national exercises	Ongoing	Ongoing

Annex E – Action Plan (2014-2017) Summary Table

Strategic Objective	Action Item	Year to Achieve
Sustain and Enhance Partnerships	Develop a call to action for critical infrastructure resilience	1 and ongoing
	Provide guidance to ensure appropriate representation on sector networks	1
	Address cross-sector issues through multi-sector meetings	Ongoing
	Strengthen public communications and awareness	2 and ongoing
Share and Protect Information	Expand stakeholder membership and participation on the *Canadian Critical Infrastructure Gateway* and leverage the CI Gateway's capabilities to improve information sharing and collaboration on specific projects	1 and ongoing
	Sponsor security clearances among private sector stakeholders in order to enable increased sharing of sensitive information	1 and ongoing
	Expand information sharing and investigate rationalization of existing information sharing arrangements	2
	Provide impact assessments during unfolding events of national significance	2 and ongoing
Implement an All-Hazards Risk Management Approach	Implement the Regional Resilience Assessment Program (RRAP) across Canada	1 and ongoing
	Provide an overall description of key risks for critical infrastructure, including dependencies and emerging trends	1 and ongoing
	Assess impacts of potential high impact / low frequency events on critical infrastructure sectors to increase awareness and understanding of risks to critical infrastructure	1 and ongoing
	Promote the adoption of existing standards and determine whether additional standards are needed to improve critical infrastructure resilience	1 and ongoing
	Conduct exercises to strengthen readiness and response efforts	1 and ongoing
	Develop targeted risk assessment products in response to emerging critical infrastructure issues	2 and ongoing
	Finalize national application of an interdependencies model	2
	Measure progress toward resilience to demonstrate results and monitor progress	2 and ongoing

Annex F – Resources

The following websites contain useful information relating to the resilience of Canada's critical infrastructure:

National Strategy for Critical Infrastructure:
http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

Public Safety Canada/Critical Infrastructure:
http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx

Canadian Critical Infrastructure Gateway (CI Gateway):
http://cigateway.ps.gc.ca

Royal Canadian Mounted Police (RCMP):
http://www.rcmp-grc.gc.ca/index-eng.htm

Canadian Security Intelligence Service (CSIS):
http://www.csis-scrs.gc.ca/index-eng.asp

Canadian Cyber Incident Response Centre (CCIRC):
http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

Canada's Cyber Security Strategy:
http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Action Plan 2010-2015 for Canada's Cyber Security Strategy:
http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy:
http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-trrrsm-strtg-eng.aspx

The Canadian Disaster Database:
http://www.publicsafety.gc.ca/prg/em/cdd/index-eng.aspx