National Cross Sector Forum

2018-2020 Action Plan for Critical Infrastructure

BUILDING A **SAFE** AND **RESILIENT CANADA**

Public Safety Canada Sécurité publique Canada

Canada

Cat. No.: PS4-66/2018E-PDF
ISBN: 978-0-660-26492-9

Table of Contents

Introduction

Canada's economic stability and national security depend on resilient critical infrastructure, such as banking, communications, and transportation. On a daily basis, Canadians count on critical infrastructure to provide safe food, clean water, reliable energy, and other essential services.

The resilience of Canada's critical infrastructure is dependent on the ability of owners and operators to respond to a rapidly-evolving risk landscape. These risks, as they relate, for example, to terrorism, natural disasters, and cyber attacks, can compromise the safety and security of communities and critical infrastructure, and by extension, have a significant impact on the well-being of Canadians. To address this evolving risk environment, the *National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure* (the Action Plan) sets out tangible initiatives that promote a collaborative approach among governments and critical infrastructure sectors to identify and manage risks before they lead to disruptions.

The Action Plan is a blueprint to implement Canada's *National Strategy for Critical Infrastructure* (the National Strategy). Approved by Federal/Provincial/Territorial Ministers responsible for Emergency Management in 2010, the National Strategy defines critical infrastructure as the 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.

The National Strategy is based on the principles outlined under the *Emergency Management Framework for Canada*, which recognizes the roles that various stakeholders must play in Canada's emergency management system to enhance the safety of Canadians. Similarly, the National Strategy highlights that the responsibility for protecting critical infrastructure in Canada is 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. The relationship is mutually beneficial: the National Strategy recognizes that critical infrastructure owners and operators have the expertise and information that governments need to develop meaningful plans/policies and implement effective programs/initiatives. In turn, governments play a key role in providing information on risks relevant to owners and operators to assist them in carrying out risk management activities.

Along with the National Strategy, the first *Action Plan for Critical Infrastructure (2010-2013)* defined areas of collaborative work for the federal government, provincial/territorial governments, and critical infrastructure owners and operators. It also established national-level sector networks for each of the ten critical infrastructure sectors, with a lead federal department/agency (LFD) responsible for each network (see Annex B). In addition, the National Strategy established the National Cross Sector Forum (NCSF) to promote collaboration across sector networks. The NCSF is a national-level consultation and outreach entity that brings together leaders from Canada's ten critical infrastructure sectors to identify priorities, and discuss cross-sector issues and initiatives to enhance the resilience of Canada's vital assets and systems (see Annex C).

Under the second *Action Plan for Critical Infrastructure (2014-2017)*, further progress was made to strengthen critical infrastructure and make it more resilient. For example, Public Safety Canada's *Regional Resilience Assessment Program* (RRAP) was implemented across Canada and expanded to include a cyber security assessment tool. At the same time, exercises were conducted and multisector network meetings were delivered to identify interdependencies and address cross-sector issues.

The 2018-2020 Action Plan continues to support the three strategic objectives identified in the National Strategy for enhancing the resilience of critical infrastructure in Canada:

- Building partnerships;
- Sharing and protecting information; and,
- Implementing an all-hazards risk management approach.

This renewed Action Plan sets out concrete activities under each of these three strategic objectives and takes a close look at the risks that the critical infrastructure community faces today, and those it might face in the coming years. It also considers accomplishments resulting from previous and ongoing collaborative efforts among all levels of government and critical infrastructure sectors.

2010-2017 Accomplishments

Since the publication of the National Strategy, governments (federal, provincial, territorial) and the private sector have worked together to achieve considerable progress in sustaining and enhancing partnerships. More specifically, since 2010, Public Safety Canada, along with LFDs, have established sector networks that meet on a regular basis, organized annual NCSF meetings, and convened well-attended multi-sector meetings to address issues of shared interest across the ten critical infrastructure sectors. Moreover, in the past few years, Public Safety Canada has worked closely with provinces and territories to strengthen partnerships between governments.

With regard to sharing and protecting information, since the last Action Plan, Public Safety Canada has doubled the membership of the Critical Infrastructure Information Gateway (CI Gateway) while continuing to provide risk information to Canada's critical infrastructure community during a steady state and during disruptive events. Actions have also been taken to ensure that members of the critical infrastructure community have access to timely and actionable information, which include, for instance, facilitating security clearances for members of the NCSF. Additionally, the community continues to actively engage to share cyber security information with the purpose of protecting Canadian businesses and consumers, notably through the Canadian Cyber Threat Exchange (CCTX); an independent, not-for-profit organization, whose mission is to share threat information, conduct cyber threat analysis and recommend risk mitigation measures.

Public Safety Canada has also worked closely with all levels of government and private sector partners on a number of fronts to deliver risk management activities from an all-hazards perspective. For example, enhanced efforts under the RRAP have allowed departmental officials to work directly with owners and operators from across all ten critical infrastructure sectors to identify and mitigate their facilities' vulnerabilities. Working closely with the critical infrastructure community and international allies, Public Safety Canada has also strengthened the foundational role of the Virtual Risk Analysis Cell (VRAC), which provides expertise and analysis to identify the potential impacts of disruptive events and support improved planning and swift response and recovery when incidents occur. Public Safety Canada has also organized and participated in a number of exercises, bringing together communities of experts and addressing lessons learned. Finally, the Department has continued to deliver and expand its Industrial Control System (ICS) Cyber Security training and community building events, helping to build cyber security expertise and capacity among the critical infrastructure sectors across Canada.

In addition, as part of ongoing efforts to provide critical infrastructure sectors with tools/information to manage key risks, an industry-led working group under the NCSF developed the *Fundamentals of Cyber Security for Canada's CI Community*. This document, which endorses and promotes the adoption of the National Institute of Standards and Technology's Cybersecurity Framework, offers action-oriented guidance to aid organizations in achieving a baseline level of cyber security.

Finally, recognizing that critical infrastructure is interconnected not only within Canada but across borders, Public Safety Canada has also worked to promote a coordinated, global approach to critical infrastructure. For example, Canada and the United States have made great strides towards meeting shared objectives of enhancing the resilience of critical infrastructure of mutual interest, working across sectors and jurisdictions. Canada has also worked closely with the broader international community, including Five Eyes partners (United States; United Kingdom; Australia; New Zealand), to ensure that its approach to strengthening critical infrastructure resilience considers the global context and leverages best practices from trusted allies.

A summary of all completed activities under the *Action Plan for Critical Infrastructure (2014-2017)* is available in Annex D.

The Risk Landscape: What has changed

The 2018-2020 Action Plan is grounded in an all-hazards approach, acknowledging the new risk environment, and taking into account known vulnerabilities and potential mitigation strategies. The risk environment will inevitably continue to evolve, requiring Canada's approach to change and adapt accordingly.

The effects of climate change in Canada continue to be one of the main hazards that directly impacts critical infrastructure. Changing climate patterns have been associated with fluctuations in precipitation, sea level, inland water levels, sea ice, and permafrost, as well as an increased frequency of extreme weather events. Severe weather can have substantial impacts on infrastructure; not only can response and recovery require significant additional resources, but also cause potentially catastrophic cascading consequences throughout the supply chain. The development of adaptation strategies for infrastructure in regions exposed to more frequent and severe weather events will be crucial to reducing the negative social and economic impacts of climate change.

The deepening convergence of the cyber and physical domains also poses new challenges to Canada's critical infrastructure. The growth of connected public services, automation, artificial intelligence, and the multiplication of internet-connected devices has great potential for critical infrastructure sectors and Canada's economy, as technologies enable faster analytics and assist in running systems more effectively. Connected public services integrate cyber technologies and physical infrastructure to create environmental and economic efficiencies for urban centres and improve the movement of people and goods (e.g. interconnecting power grids to reduce waste; smarter and better timed transportation systems). However, the increased reliance of organizations on cyber systems and technologies creates exposure to new risks that could produce significant physical consequences. ICS are at the intersection of the cyber and physical security domains. These systems, many of which were developed prior to the internet era, are used in a variety of critical applications, including within the energy and utilities, transportation, health, manufacturing, food and water sectors. For a variety of reasons, including efforts to minimize costs and increase efficiencies, these systems are increasingly connected to the internet, which can result in exposure to more advanced threats than those considered at the time of their design.

Another complex and evolving threat to Canada's critical infrastructure is terrorism. The Government of Canada continues to adapt its overall approach to protect Canadians, following the release of *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (2012). The Counter-Terrorism Strategy highlights the importance of cooperation with Canada's international partners, all levels of government, intelligence and law enforcement agencies, industry stakeholders, and civil society. The Government of Canada has also released the *2017 Public Report on the Terrorist Threat to Canada*, which provides additional details on trends on terrorism and what they mean to Canada. To this end, Public Safety Canada continues to work closely with critical infrastructure stakeholders, governments, and security and intelligence organizations [e.g. Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS), Canadian Border Services Agency (CBSA), and the Canadian Cyber Incident Response Centre (CCIRC)] to assess the evolving threat environment and provide relevant information to the critical infrastructure community.

Finally, aging infrastructure is also emerging as a key risk. Many infrastructure assets are approaching, or have exceeded, the end of their designed life spans, which can lead to rising maintenance costs and increased risk of disruption. Identifying strategies to reduce risks related to aging infrastructure will be essential to mitigating the potentially significant impacts of infrastructure failure on our national security, our economy, and the well-being of Canadians.

Community Engagement: **How we work together**

In addition to looking at current and emerging hazards and threats to critical infrastructure, this Action Plan takes into consideration feedback received through consultations and numerous engagement events. In 2016, Public Safety Canada conducted a cyber security consultation to review existing measures to protect Canadians and our critical infrastructure from cyber threats. The results of these consultations pointed to the importance of digital technologies for critical infrastructure, while recognizing the emergence of new vulnerabilities.

More recently, Public Safety Canada engaged with the federal community, provinces and territories, and owners and operators of critical infrastructure to seek feedback on information sharing mechanisms and key resilience-building programs, including the Regional Resilience Assessment Program (RRAP) and the Virtual Risk Analysis Cell (VRAC). Public Safety Canada also obtained feedback from critical infrastructure stakeholders through a variety of other engagement initiatives, such as sector networks meetings and other community-building events. Feedback and comments obtained from all ten sectors through these various engagements have informed the development of this Action Plan.

Under the 2014-2017 Action Plan, Public Safety Canada renewed its emphasis on collaboration through the Federal/Provincial/Territorial Critical Infrastructure Working Group. Moving forward, this renewed approach will allow all levels of government to work together in a complementary manner to achieve shared critical infrastructure resilience objectives. It will also allow the critical infrastructure community to effectively support existing intergovernmental governance mechanisms, (such as the Federal/Provincial/Territorial Senior Officials Responsible for Emergency Management and the Federal/Provincial/Territorial Ministers Responsible for Emergency Management) while complementing standing public-private sector engagement fora, such as the sector networks, multi-sector networks, and National Cross Sector Forum.

2018-2020 Action Items

This Action Plan supports the risk management principles outlined in the *National Strategy*. The following section outlines action items across each of the National Strategy's strategic objectives, which build on past achievements and lessons learned. The activities are intended to strengthen Canada's critical infrastructure resilience by helping to prevent, mitigate, prepare for, respond to, and recover from disruptions. It is designed to help foster collaboration and information sharing among all levels of government and private sector partners, with a focus on delivering tangible risk management initiatives. A table summarizing the action items and associated implementation timelines can be found in Annex E.

BUILDING PARTNERSHIPS

Strengthening the resilience of critical infrastructure requires collaborative work among all partners and stakeholders. Public Safety Canada works closely with federal departments and agencies, provinces and territories, private sector, and international counterparts to build partnerships and advance mutual goals. The action items below are focused on building, sustaining, and enhancing collaboration with all partners within the critical infrastructure community. They also aim at establishing or maintaining structures and mechanisms to facilitate cooperation and information sharing.

1. Address cross-sector issues through multi-sector meetings

Multi-sector meetings have proven to be an effective way to address cross-sector issues. Senior leaders across the 10 critical infrastructure sectors are engaged via the National Cross Sector Forum (NCSF) on Critical infrastructure, co-chaired by the Deputy Minister of Public Safety Canada (PS), and supported by operational level discussions at meetings of the Multi-Sector Network (MSN). In addition to the NCSF and MSN, Public Safety Canada will provide leadership in coordinating ad-hoc cross-sector meetings to address issues of shared interest.

Deliverables

1.1 NCSF to meet face-to-face and participate in ad-hoc teleconferences. PS will coordinate and organize all meetings.
Timeline: Ongoing

1.2 MSN to meet in person annually. PS to provide leadership in coordinating additional ad-hoc multi-sector meetings.
Timeline: Ongoing

2. Engage with provinces and territories to strengthen critical infrastructure resilience

PS will continue to collaborate with other levels of government, primarily through the Federal/Provincial/Territorial (FPT) Critical Infrastructure Working Group (FPT CI WG), engaging on current and emerging issues facing critical infrastructure sectors, including as it relates to the nexus with emergency management, national security, and cyber security. PS and provinces/territories (P/Ts) will work together to identify opportunities for P/Ts to leverage federal critical infrastructure programs , such as the Regional Resilience Assessment Program (RRAP), to support jurisdictional efforts to build resilience.

Deliverables

2.1 PS to coordinate and chair meetings of the FPT CI WG.
Timeline: Ongoing

2.2 The FPT CI WG to develop and implement a Work Plan to outline and direct its work.
Timeline: Ongoing

2.3 PS to engage with P/Ts to identify ways to collaborate more effectively in the delivery of critical infrastructure programs, particularly the RRAP.
Timeline: Year 1

3. Ongoing collaboration with LFDs

PS will continue to provide leadership and support to the federal critical infrastructure community, including its coordination role with respect to the Lead Federal Department Critical Infrastructure Network (LFD CI Network). This Network brings together federal departments/agencies responsible for the 10 critical infrastructure sectors to support information sharing and collaboration. In addition, PS plans to build a community of federal cyber security experts from across the 10 sectors to address cyber security risks to critical infrastructure. PS will also continue to work closely with other government organizations and regional offices.

Deliverables

3.1 LFD CI Network to meet at the director-level on a regular basis. PS to chair and coordinate meetings.
Timeline: Ongoing

3.2 PS to work with LFDs to strengthen partnerships in the area of cyber security by leading the creation of a community of critical infrastructure cyber security experts.
Timeline: Year 1 & Ongoing

4. Expand regional outreach of critical infrastructure programs

To improve the reach and impact of PS programs, the Department will develop an outreach strategy for key resilience enhancement programs. This will be achieved by building partnerships with other levels of government, Indigenous communities, critical infrastructure owners/operators, academia, as well as federal and international partners.

Deliverables

4.1 PS to develop and implement an outreach strategy for key resilience enhancement programs.
Timeline: Year 1

5. Engage with various international fora to address critical infrastructure issues

PS will continue to participate in a number of international groups, such as the Critical Five. These groups have been formed to provide a forum for the discussion of critical infrastructure resilience issues of mutual interest.

Deliverables

5.1 PS to lead Canada's participation in international groups to advance a collaborative approach to strengthening the resilience of globally interconnected assets and systems, and to share best practices.
Timeline: Ongoing

SHARING AND PROTECTING INFORMATION

Sharing and protecting information is essential to strengthening critical infrastructure resilience. Timely information sharing across governments and critical infrastructure sectors is needed to promote effective risk management. The action items described below are designed to help ensure that stakeholders have access to the right information at the right time to support planning and decision-making, during both steady state and disruptive events. These initiatives feature a collaborative approach to assess what type of information is produced, who it is shared with, and how it is shared.

6. Modernization and promotion of the Critical Infrastructure Information Gateway

PS will work to modernize the Critical Infrastructure Information Gateway (CI Gateway) to improve user experience and functionality. This modernization initiative will also include a review of existing publications and tools to ensure their continued relevance. PS will also focus on expanding the Gateway membership, particularly targeting regions and sectors with less participation.

Deliverables

6.1 PS will modernize the CI Information Gateway to update information and improve user experience.
Timeline: Year 1

6.2 PS will actively promote the use of the CI Gateway to include greater regional and sectoral representation.
Timeline: Year 1 & Ongoing

7. Conduct an environmental scan on information sharing

Building on the existing Critical Infrastructure Information Sharing Framework, PS will conduct an environmental scan to identify gaps in current information sharing mechanisms. This initiative will also explore mechanisms to improve how information is delivered to ensure it is timely and accessible to the CI community. Part of the objective is to assess protocols on how/what/when/with whom to share information when an incident occurs.

Deliverables

7.1 Review the existing CI Information Sharing Framework and conduct an environmental scan of the processes currently in place to share information and assess potential gaps.
Timeline: Year 2

7.2 Identify barriers and mechanisms to improve information sharing between the federal government and PTs and owners and operators.
Timeline: Year 2

8. Develop and distribute risk information during steady state and disruptive events

PS, through the Virtual Risk Analysis Cell (VRAC), provides information to government and private sector partners during steady state and during an unfolding event. VRAC will continue to provide risk information, including: threat and impact assessments; relevant emergency management and business continuity information; analysis of critical infrastructure dependencies and interdependencies; geospatial products; supply chain modelling; as well as relevant statistical information. By continuing to develop these types of products, and informed by industry practices such as the Canadian Cyber Threat Exchange (CCTX), PS will support the risk management efforts of critical infrastructure stakeholders.

Deliverables

8.1 PS to develop and share analytical material and information products to support critical infrastructure stakeholders' risk management action.
Timeline: Ongoing

8.2 PS to advance modelling tools to support dependency and interdependency analysis.
Timeline: Ongoing

9. Support the acquisition of security clearances among private sector stakeholders

PS will work collaboratively with LFDs to increase the number of secret-level cleared stakeholders. This will ensure that sensitive information can be shared with appropriate individuals.

Deliverables

9.1 LFDs and PS will work together to identify ways to increase access to security clearances for critical infrastructure sectors, and explore mechanisms to streamline the acquisition process (e.g. length of time to obtain clearance; transferability of clearances).
Timeline: Ongoing

9.2 PS to work with LFDs and Portfolio partners to promote the use of declassified, or partially declassified, information to support situational awareness.
Timeline: Year 1 & Ongoing

IMPLEMENTING AN ALL-HAZARDS RISK MANAGEMENT APPROACH

The National Strategy promotes the application of risk management and sound business continuity planning to strengthen critical infrastructure resilience. By adopting a risk-based approach, governments and the private sector can assess the likelihood and the impact of a potential disruption, and allocate resources based on their risk tolerance. Risk assessments can assist in developing a strong situational awareness of the challenges posed by the convergence of hazards, threats, and vulnerabilities to critical infrastructure assets in Canada. With this in mind, Public Safety Canada and sector-specific federal departments and agencies work closely with PTs and critical infrastructure stakeholders to acquire a greater understanding of these risks. The items below are aimed at helping to ensure that the critical infrastructure community has the tools and information needed to take meaningful risk management action from an all-hazards perspective.

10. Increase impact of resilience assessments

To bolster the program's impact, the RRAP will work towards a collaborative partnership with P/Ts, while maintaining a national leadership role. The RRAP will also look at including additional modules within the current assessment tools to increase the depth of the assessment in particular areas. Lastly, as part of RRAP, the Canadian Cyber Resilience Review (CCRR) will continue to assess facilities across Canada to increase the resilience of owners and operators to cyber threats, while exploring additional tools to increase the depth of CCRR assessments.

Deliverables

10.1 PS to work with Provinces and Territories in identifying and implementing measures to increase the impact and the reach of the RRAP.
Timeline: Year 1

10.2 PS to continue to deliver the CCRR across Canada and explore possibilities for adding other tools to support and complement the CCRR.
Timeline: Year 1

10.3 Assess needs and feasibility of adding modules to RRAP assessment tools to increase the depth of analysis on specific topics.
Timeline: Year 2

11. Implement a risk-based approach to identify key assets and infrastructure of significance

PS will work with LFDs to review and update the Canadian Critical Infrastructure Asset List (CI Asset List), and explore opportunities to refine the methodology for identifying assets of national significance. The list will be used, among other things, to inform the RRAP site selection process. The site selection process, and resulting annual assessment plan, will be further informed by input from PTs and LFDs, as well as an objective assessment of each facility's criticality.

Deliverables

11.1 PS to work with LFDs to review and update the CI Asset List.
Timeline: Year 1 (and ongoing)

11.2 PS to develop risk-based criteria for objectively assessing facilities for criticality (Criticality Exposure Index).
Timeline: Year 1

11.3 PS to develop and implement an annual RRAP site assessment plan.
Timeline: Year 1 (and ongoing)

12. Identify ways to support the critical infrastructure community in taking action to address risks

PS will explore ways to promote risk mitigation action after resilience assessments have been conducted. The objective is to find mechanisms to encourage stakeholders to take action to address identified issues and/or systemic vulnerabilities. In addition, PS will seek to identify emerging risks to critical infrastructure and explore opportunities to work with sector partners to raise awareness of, and address identified risks.

Deliverables

12.1 PS to work with critical infrastructure stakeholders to identify effective ways to support owners and operators to take action to address risks.
Timeline: Ongoing

12.2 PS to work with the sector partners to identify and raise awareness of emerging risks to critical infrastructure (e.g. aging infrastructure, climate change, artificial intelligence, drones).
Timeline: Year 2 (and ongoing)

13. Conduct cross-sector exercises to strengthen preparedness and response

The critical infrastructure community has identified exercises as an effective means to test, evaluate, and improve event management. In support of a common approach to enhancing resilience, and working in collaboration with LFDs, P/Ts, and critical infrastructure owners and operators, PS will continue to conduct cross-sector exercises. As a means to encourage organizational learning, PS will share observations and best practices from exercises to improve systemic issues common to the critical infrastructure community.

Deliverables

13.1 PS to continue to conduct physical and cyber-focused cross-sector exercises, in collaboration with LFDs, P/Ts, and critical infrastructure owners and operators.
Timeline: Ongoing

13.2 PS to share observations and best practices from exercises.
Timeline: Ongoing

14. Assess the health of the ten critical infrastructure sector networks

PS will develop and implement a process to measure and improve the "health" of the 10 sector networks, consulting with the LFDs and industry representatives. PS will develop a report which will identify strengths and areas to be enhanced both across and within the sector networks in order to support the development of tools and best practices, strengthen partnerships, and improve the collective focus on critical infrastructure priority issues.

Deliverables

14.1 PS to work collaboratively with LFDs to develop a process to assess the health of the CI sector networks.
Timeline: Year 1

14.2 PS to work with NCSF members and LFDs to identify next steps for improving sector network health.
Timeline: Ongoing

15. Support the community in addressing risks associated with the convergence of physical and cyber critical infrastructure systems

Canada's critical infrastructure is increasingly reliant on cyber-based assets and systems. To address risks associated with the convergence of physical and cyber critical infrastructure systems, PS will continue to provide training sessions on how to protect ICS and bring together stakeholders to share their knowledge and experience on mitigating cyber threats. Working closely with LFDs and critical infrastructure owners and operators, PS will work to expand its reach across the ten critical infrastructure sectors.

Deliverables

15.1 PS to host annual Industrial Control Systems (ICS) security symposiums in various cities across Canada.
Timeline: Ongoing

15.2 PS to work closely with critical infrastructure stakeholders to expand the reach of cyber engagement mechanisms, such as ICS security symposiums.
Timeline: Year 1

16. Examine the *National Strategy for Critical Infrastructure* (2010) to determine if there is a need to update Canada's overall approach to critical infrastructure resilience

The *National Strategy for Critical Infrastructure* (the Strategy) was published in 2010, and continues to guide the overall approach to critical infrastructure resilience in Canada. To ensure the continued relevance of our resilience efforts, PS will review the National Strategy to determine whether there is a need for it to be renewed or updated, working closely with PTs, the federal community, and the private sector.

Deliverables

16.1 PS to examine the *National Strategy for Critical Infrastructure*, working closely with P/Ts, the federal community, and the private sector, to ensure its continued relevance.
Timeline: Year 3

17. Develop a tracking mechanism to assess the progress of activities in the Action Plan

PS will track progress of the activities outlined in this Action Plan. It will adjust items if needed, to ensure they achieve their primary goal. To this end, PS will develop a tracking tool, which will establish the expected outcome of each deliverable, and report regularly on progress.

Deliverables

17.1 PS to develop a mechanism to ensure that the progress of action items is tracked and that there is regular reporting on the achievement of objectives.
Timeline: Year 1 & Ongoing

Conclusion

The *National Strategy for Critical Infrastructure* will continue to guide Canada's overall approach to strengthening critical infrastructure. This updated Action Plan provides a blueprint for working collaboratively with other federal departments and agencies, provinces and territories, and critical infrastructure stakeholders. The actions outlined for the next three years will continue to build on success achieved to date under previous action plans, by addressing lessons learned, continuously improving existing products, and exploring emerging opportunities.

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:

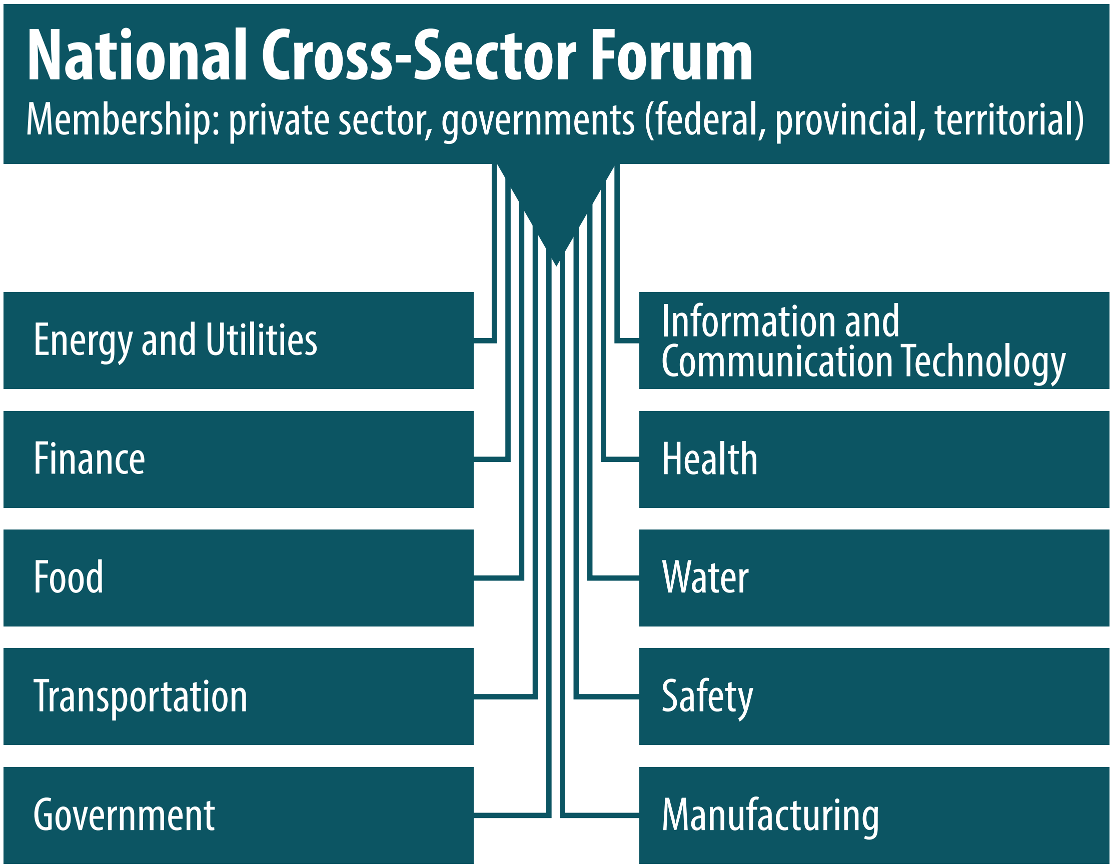
Critical Infrastructure Sectors and Lead Federal Departments/Agencies

Sector	Sector-specific federal department/agency
Energy and utilities	Natural Resources Canada
Information and communication technology	Innovation, Science and Economic Development Canada
Finance	Finance Canada
Health	Public Health Agency of Canada
Food	Agriculture and Agri-Food Canada
Water	Environment and Climate Change Canada
Transportation	Transport Canada
Safety	Public Safety Canada
Government	Public Safety Canada
Manufacturing	Innovation, Science and Economic Development Canada; Department of National Defence

Source: *Action Plan for Critical Infrastructure* (2010)

Annex C:

Sector Networks and the National Cross Sector Forum



National Cross-Sector Forum

Membership: private sector, governments (federal, provincial, territorial)

Energy and Utilities

Finance

Food

Transportation

Government

Information and Communication Technology

Health

Water

Safety

Manufacturing

Source: *National Strategy for Critical Infrastructure* (2010)

Annex D:

Achievements under the *Action Plan for Critical Infrastructure (2014-2017)*

Strategic Objective:

SUSTAIN AND ENHANCE PARTNERSHIPS

Deliverable	Current Status
Develop a call to action for critical infrastructure resilience	Completed
Provide guidance to ensure appropriate representation on sector networks	Completed
Address cross-sector issues through multi-sector meetings	Completed (and ongoing)
Strengthen public communications and awareness	Completed (and ongoing)

Strategic Objective:

SHARE AND PROTECT INFORMATION

Deliverable	Current Status
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	Completed (and ongoing)
Sponsor security clearances among private sector stakeholders in order to enable increased sharing of sensitive information	Completed (and ongoing)
Expand information sharing and investigate rationalization of existing information sharing arrangements	Completed
Provide impact assessments during unfolding events of national significance	Completed (and ongoing)

Strategic Objective:

IMPLEMENT AN ALL-HAZARDS RISK MANAGEMENT APPROACH

Deliverable	Current Status
Implement the Regional Resilience Assessment Program (RRAP) across Canada	Completed (and ongoing)
Provide an overall description of key risks for critical infrastructure, including dependencies and emerging trends	Completed (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	Completed (and ongoing)
Promote the adoption of existing standards and determine whether additional standards are needed to improve critical infrastructure resilience	Completed (and ongoing)
Conduct exercises to strengthen readiness and response efforts	Completed (and ongoing)
Develop targeted risk assessment products in response to emerging critical infrastructure issues	Completed (and ongoing)
Finalize national application of an interdependencies model	Ongoing
Measure progress toward resilience to demonstrate results and monitor progress	Completed (and ongoing)

Annex E: *2018-2020 Action Plan*: Summary Table

BUILDING AND ENHANCING PARTNERSHIPS

Deliverable	Timeline
Address cross-sector issues through multi-sector meetings	Ongoing
Engage with provinces and territories to strengthen critical infrastructure resilience	Ongoing
Ongoing collaboration with Lead Federal departments	Ongoing
Expand regional outreach of critical infrastructure programs	Year 1
Engage with various international fora to address critical infrastructure issues	Ongoing

SHARING AND PROTECTING INFORMATION

Deliverable	Timeline
Modernization and promotion of the Critical Infrastructure Information Gateway	Ongoing
Conduct an environmental scan on information sharing	Year 2
Develop and distribute risk information during a steady state and during disruptive events	Ongoing
Support the acquisition of security clearances among private sector stakeholders	Ongoing

IMPLEMENT AN ALL-HAZARDS RISK MANAGEMENT APPROACH

Deliverable	Timeline
Increase impact of resilience assessments	Year 2
Implement a risk-based approach to identify key assets and infrastructure of significance	Year 2
Identify ways to support the critical infrastructure community in taking action to address risks	Year 2
Conduct cross-sector exercises to strengthen preparedness and response	Ongoing
Assess the health of the ten critical infrastructure sector networks	Ongoing
Support the community in addressing risks associated with the convergence of physical and cyber critical infrastructure systems	Ongoing
Examine the *National Strategy for Critical Infrastructure* (2010) to determine if there is a need to update Canada's overall approach to critical infrastructure resilience	Year 3
Develop a tracking mechanism to assess the progress of activities in the *Action Plan*	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 Information Gateway (CI Gateway):
http://cigateway.ps.gc.ca

Royal Canadian Mounted Police (RCMP):
http://www.rcmp.gc.ca/en

Canadian Security Intelligence Service (CSIS):
https://csis.gc.ca/index-en.php

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

***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

***Cyber Review Consultations Report*:**
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/index-en.aspx

Canadian Cyber Threat Exchange (CCTX):
https://cctx.ca/