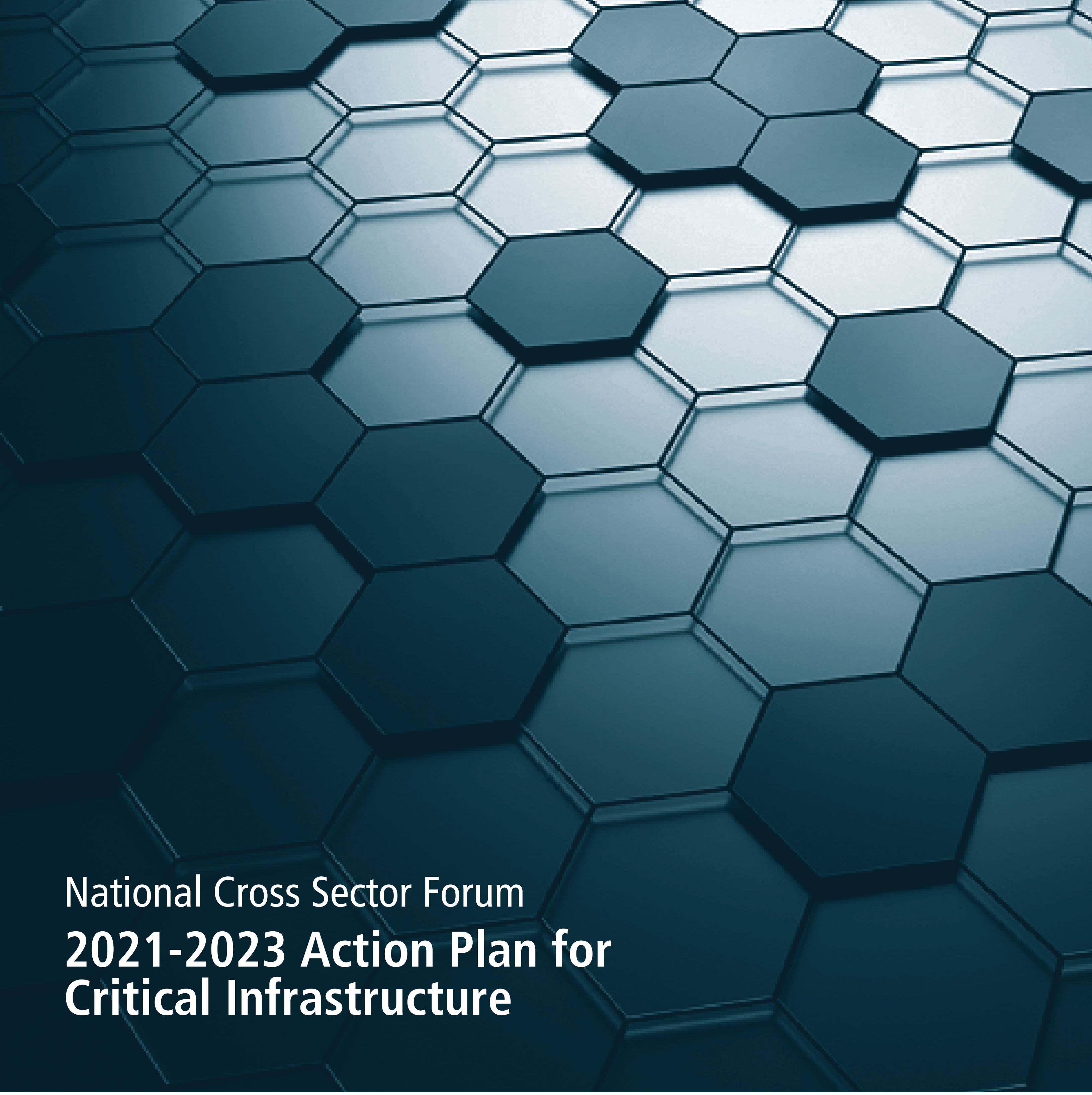


National Cross Sector Forum

2021-2023 Action Plan for Critical Infrastructure

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

Public Safety Canada Sécurité publique Canada

Canada

Cat. No.: PS4-66/2021E-PDF
ISBN: 978-0-660-38395-8

Table of Contents

Introduction

The *National Strategy for Critical Infrastructure* (the National Strategy) sets out Canada's approach to strengthening the resilience of critical infrastructure. 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. Canadians rely on critical infrastructure every day, from the infrastructure supporting transportation, to the food and water sectors. The National Strategy identifies three main objectives to strengthen critical infrastructure resilience: building partnerships, sharing and protecting information, and practicing an all-hazards risk approach. Since the publication of the National Strategy in 2010, three supporting action plans (2010-2013; 2014-2017; and 2018-2020) have been released to outline concrete steps towards advancing the objectives set out in the strategy.

Between 2018 and 2020, an examination of the National Strategy was also conducted to determine if there was a need to update Canada's overall approach to critical infrastructure resilience. The examination's findings led to a recommendation that was given to the Deputy Minister of Public Safety for the Department to enter a renewal process, that will now take place over the next three years (2021-2023).

To continue supporting the advancement of the National Strategy objectives until the release of this renewed national approach to critical infrastructure resilience, Public Safety Canada (PS) has created the *National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure* (the Action Plan). The Action Plan reaffirms the Government of Canada's commitments to work closely with critical infrastructure sector partners, provinces and territories towards a more secure and resilient Canada. The Action Plan builds upon progress made through past action plans, identifies new activities based on the changing threat environment, and will support a collaborative approach to enhance the security and resilience of Canada's critical infrastructure. The 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.

2018-2020 Accomplishments

Under the *National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure*, PS completed an examination of the National Strategy and Canada's overall approach to critical infrastructure. This occurred through engagement with key national critical infrastructure stakeholders, including: the National Cross Sector Forum (NCSF), Lead Federal Departments (LFDs), the Federal/ Provincial/Territorial (FPT) Working Group for Critical Infrastructure, and limited one-on-one meetings with members of the broader critical infrastructure community, as well as academia.

During this period, PS continued to conduct all-hazards risk assessments through the Regional Resilience Assessment Program (RRAP). This included working with provinces and territories to determine priority sites for assessment, and to identify and implement measures to increase the impact and reach of the RRAP. Between 2018 and 2020, RRAP continued work on broader all-hazards regional assessments with the third cross-border RRAP project; maintained a high critical infrastructure owner/operator satisfaction rating; and created sector profiles by analyzing aggregate data from site assessments.

PS also worked closely with critical infrastructure stakeholders to expand the reach of its cyber engagement mechanisms, including through the Industrial Control System (ICS) Security Symposiums. ICS Security Symposiums brought together Canada's critical infrastructure owners and operators for briefings on the latest threats, hands-on development of incident handler skills, and information to increase the security of ICS. PS also launched a web conference series where industry experts provided briefings on topics related to ICS security. The inaugural meeting reached capacity and has allowed PS to expand its reach to stakeholders across the country.

Cross-sector tabletop exercises in coordination with LFDs, provinces and territories, municipalities and critical infrastructure owners and operators also continued through Nexus Vitalis 2019. These exercises brought together the critical infrastructure community to simulate responses to all-hazard attacks (e.g. cyber attacks), as well as to reinforce new and existing partnerships by sharing information and tackling shared problems. PS completed the Nexus Vitalis exercise series in three different regions (Saskatchewan, British Columbia, and Atlantic Canada) in spring 2019.

Given that private owners and operators of critical infrastructure depend on important event and steady state information from the Government of Canada, there was a call to improve PS-led forums (e.g. NCSF, LFDs, FPT Working Group for Critical Infrastructure, and Multi-Sector Network (MSN) meetings) to remove barriers to information, namely security clearances. In response, PS and security partners have begun to deliver unclassified panel discussions on emerging threats and mitigation measures, which will help improve overall situational awareness.

PS's Virtual Risk Analysis Cell (VRAC) also modified the development and distribution of impact assessment products to support critical infrastructure stakeholder decision-making and management actions. The VRAC provided expertise and analysis to identify the potential impacts of disruptive events, support improved planning, and swift response and recovery when incidents occurred. For instance, during flood and fire seasons, VRAC produced reports to highlight what impacts each sector may experience and what the cascading impacts to other sectors could be. These cyclical products were posted on the Critical Infrastructure Information Gateway.

And finally, in 2019, PS published the Enhancing Canada's Critical Infrastructure Resilience to Insider Risk. This document provided Canadian critical infrastructure organizations with guidance on what constitutes insider risk and recommendations on how to monitor, respond to, and mitigate insider risk . This guide assists organizations in developing their insider risk programs to defend against human and technical vulnerabilities, including those related to their partners, service providers, and associates. The document was praised by both public and private sector partners as providing useful and sound advice in an area of increasing concern.

In 2019, PS published the Enhancing Canada's Critical Infrastructure Resilience to Insider Risk. This document provided Canadian critical infrastructure organizations with guidance on what constitutes insider risk and recommendations on how to monitor, respond to, and mitigate insider risk.

The Risk Landscape:
Driving Change

As we look forward into another decade, a world of uncertainty persists. The risk landscape facing the Canadian critical infrastructure community continues to be a complex one, including a range of environmental threats, cyber security threats, foreign interference, economic pressures, and most notably, a health crisis that has highlighted the need for greater focus on preparedness and risks posed by the globally distributed supply chains that support critical infrastructure.

Canada's climate is changing. The effects of widespread warming are evident in many parts of Canada and are projected to intensify in the future. These shifts are increasingly affecting Canada's natural environment, economy, and the health of Canadians. Extreme weather events, such as floods and fires, continue to threaten the ability of critical infrastructure to deliver services. For example, a severe blizzard in 2020 caused St. John's, Newfoundland and Labrador, to experience a disruption in its transportation systems, telecommunications networks and just-in-time supply chains.

Canada's climate is changing. The effects of widespread warming are evident in many parts of Canada and are projected to intensify in the future.

> The digitalization of systems and processes, and the ability to control critical infrastructure operations remotely, also continues to present new cyber security challenges.

While the growing adoption of digital infrastructure systems alongside traditional physical infrastructure has improved overall connectivity, communications, and service delivery to Canadians, the use of internet enabled systems increases the probability and scale of both intentional and unintentional disruptions.

Canada's critical infrastructure remains a high value target for foreign interference, including for the purposes of intentional service disruptions and intellectual property theft. The high level of interconnectedness across Canada's critical infrastructure sectors creates a multiplying effect of a disruption on a single sector. The compromise of an operator in one sector, such as an electricity provider in the Energy and Utilities Sector, can have cascading impacts on other sectors.

Canada's critical infrastructure remains a high value target for foreign interference, including for the purposes of intentional service disruptions and intellectual property theft.

And let's not forget that the development of the Action Plan (2021-2023) comes during unprecedented circumstances surrounding the spread of the novel coronavirus (COVID-19), which was declared a global pandemic in March 2020 by the World Health Organization. From the onset of the pandemic, Canada's critical infrastructure owners and operators faced challenges as governments mandated the closure of non-essential businesses and restricted the movement of people and goods, and shortages of medical supplies including personal protective equipment persisted.

The pandemic highlighted various critical infrastructure vulnerabilities, such as the reliance on globally distributed supply chains for essential goods. For example, Canada now relies on only a handful of meat processing facilities in Canada and the U.S. for the supply of meat to Canadians. Many of these facilities were forced to temporarily close and reduce capacity due to health risks, thereby undermining our food security. Another concern is that most of Canada's pharmaceuticals are sourced from a single country, which leaves little recourse in the case of a disruption. All of our critical infrastructure sectors rely on goods and services produced by supply chains based around the world, beyond Canada's purview, which can present certain risks. The pandemic has challenged norms and should shape Canada's approach to resilience long after vaccines have been developed.

Community Engagement: **How we work together**

In addition to looking at current and emerging hazards and threats to critical infrastructure, the Action Plan takes into consideration feedback received through consultations and numerous engagement events. Most recently, PS brought the critical infrastructure community together during the COVID-19 pandemic through the Extended NCSF (E-NCSF).

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. At the outset of the COVID-19 pandemic, NCSF meetings were expanded to include hundreds of new participants across all ten critical infrastructure sectors. This forum was rebranded as the E-NCSF in order to differentiate its activities from the core NCSF. The critical infrastructure community used this outlet as events unfolded early in the pandemic as a means to give and receive valuable information, guidance and planning to ensure resilience, and E-NCSF meetings continue to be held on a monthly basis while the pandemic situation continues to evolve. The pandemic reaffirmed multi-sector network meetings such as the NCSF and the E-NCSF as a primary medium for effective collaboration between the critical infrastructure community and the federal government.

In February 2020, PS also hosted an in-person FPT Working Group for Critical Infrastructure meeting and a MSN meeting. These events included face-to-face facilitated discussions on the National Strategy examination, and lessons learned from the Nexus Vitalis exercise series. These consultations pointed to the importance of strengthening integrated emergency response while raising awareness of new threats and vulnerabilities.

2021-2023 Action Plan Activities

The following section outlines activities and action items that support the risk management principles outlined in the National Strategy's strategic objectives. The activities are intended to strengthen Canada's critical infrastructure resilience by helping to prevent, mitigate, prepare for, respond to, and recover from disruptions.

These activities are designed to foster collaboration and information sharing among all levels of government, private sector partners, and allied countries, with a focus on delivering concrete risk management initiatives. A summary of activities and associated implementation timelines can be found in Annex E.

Acknowledging the rapidly changing operating environment as a result on the COVID-19 pandemic, Action Plan activities and deliverables will be reviewed on an annual basis, to determine if new activities or deliverables should be added, or existing ones removed.

BUILDING PARTNERSHIPS

Strengthening the resilience of critical infrastructure requires collaborative efforts among all partners and stakeholders. To build effective partnerships and advance mutual objectives, PS works closely with federal departments and agencies, provinces and territories, private sector, and international counterparts. The activities and deliverables below are focused on building, sustaining, and enhancing collaboration with all partners within the critical infrastructure community, including mechanisms to facilitate cooperation and information sharing.

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

Multi-sector meetings continue to be an effective way to share information and address cross-sector issues and concerns. Senior representatives from across the ten critical infrastructure sectors are engaged via the NCSF, co-chaired by the Deputy Minister of PS, and supported by operational level discussions at multi-sector network (MSN) meetings such as the E-NCSF. In addition to the NCSF and MSN meetings, PS will provide leadership in coordinating ad-hoc cross-sector meetings to address issues of shared interest.

Deliverables

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

1.2 NCSF to meet in person or virtually, and participate in ad-hoc teleconferences. PS will coordinate and organize all meetings
Timeline: Ongoing

1.3 PS to reassess NCSF membership and terms of reference
Timeline: Year 1

1.4 PS to build on the E-NCSF to strengthen public-private sector collaboration through MSN engagement during event-state and steady-state operations
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 COVID-19 response efforts. PS and provinces/territories (P/Ts) will work together to identify opportunities for P/Ts to leverage federal critical infrastructure programs 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 via the FPT CI WG to identify changes, needs and priorities as a result of COVID-19
Timeline: Year 1

2.4 PS to work with P/Ts to determine needs of municipal governments and identify opportunities to support municipal initiatives
Timeline: Ongoing

3. Continuing collaboration with Lead Federal Departments (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 ten critical infrastructure sectors to support information sharing and collaboration. PS will also continue to work closely with other government organizations, including the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS) and PS 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 continuing to support the community of critical infrastructure cyber security experts
Timeline: Ongoing

3.3 PS to provide direct support on intergovernmental efforts in support of Canada's COVID-19 response
Timeline: Ongoing

3.4 PS to work with LFDs to update sector profiles and fact-sheets
Timeline: Ongoing

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

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

Deliverables

4.1 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

4.2 PS to support various Organization for Economic Cooperation and Development (OECD) initiatives related to critical infrastructure
Timeline: Ongoing

5. Engage with public and private sector stakeholders on the renewal of Canada's strategy and approach to critical infrastructure

PS will leverage existing partnerships, and create new mechanisms to support the renewal of Canada's strategy and approach to critical infrastructure, to ensure it is reflective of Canada's broader critical infrastructure community and the challenges and issues that they will face resulting from an evolving threat and risk landscape.

Deliverables

5.1 PS to establish a Critical Infrastructure Experts Working Group (CIEWG) consisting of public and private sector stakeholders, academics, and select subject matter experts to act as consultative body for the critical infrastructure strategy and approach renewal process
Timeline: Year 1

SHARING AND PROTECTING INFORMATION

The sharing and protection of information is a key component in strengthening the resilience of Canada's critical infrastructure community. Timely information sharing, within and across the critical infrastructure sectors and all levels of government, is needed to promote effective risk management. The activities and deliverables described below are curated to ensure stakeholders have timely access to relevant information to support planning and decision-making. 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 to continue efforts to modernize the CI Gateway to meet the changing needs of the critical infrastructure community, and promote the use of the CI Gateway to increase the number of users and site visits.

Deliverables

6.1 PS will modernize the CI Gateway in order to increase functionality and improve overall user experience
Timeline: Ongoing

6.2 PS to conduct a review of existing publications and tools to ensure their continued relevance
Timeline: Year 2

6.3 PS will actively promote the use of the CI Gateway to include greater regional and sectoral representation
Timeline: Ongoing

7. Develop and distribute impact assessment products during both steady and event states

PS to provide timely and relevant information to public and private sector partners during steady and event states. PS will enhance the situational awareness of critical infrastructure stakeholders through the development of critical infrastructure focused resilience analysis by distributing: threat and impact assessments; relevant emergency management and business continuity information; analysis of critical infrastructure dependencies and interdependencies; geospatial products; as well as relevant statistical information.

Deliverables

7.1 PS to develop and share analytical material and information products to support critical infrastructure stakeholders' risk management actions
Timeline: Ongoing

7.2 PS to continue to utilize RRAP assessment data and other data sources to create trend reports, sector overviews, and other analytical products to support critical infrastructure partners
Timeline: Ongoing

7.3 PS to collaborate with public and private sector stakeholders to expand the reach of trusted information products to critical infrastructure partners and communities in Canada
Timeline: Ongoing

IMPLEMENTING AN ALL-HAZARDS RISK MANAGEMENT APPROACH

The best way to minimize impacts to critical infrastructure, citizens, economic prosperity, and security, is to implement an all-hazards approach to address critical infrastructure risks and interdependencies. The National Strategy promotes the application of risk management and sound business continuity planning to strengthen critical infrastructure resilience. By embracing a risk-based approach, governments and industry can assess the likelihood and impact of a potential disruption and allocate resources based on their risk tolerance. With this in mind, PS and other federal departments and agencies work closely with other levels of government and critical infrastructure stakeholders to obtain a greater understanding of these risks. The activities and deliverables listed below are aimed at helping to ensure that Canada's critical infrastructure community has the tools and information needed to take meaningful risk management action from an all-hazards perspective.

8. Support sectoral and cross-sectoral exercises to strengthen the preparedness and response abilities of Canada's critical infrastructure

Exercises are an effective means to test, evaluate, and improve event management across the critical infrastructure community. PS continues to work in collaboration with LFDs, P/Ts, and critical infrastructure owners and operators to support sectoral and cross-sectoral exercises in an effort to strengthen the ability of stakeholders to mitigate impacts of disruptive events.

Deliverables

8.1 PS to continue to support physical and cyber-focused sectoral and cross-sectoral exercises, in collaboration with LFDs, P/Ts, and critical infrastructure owners and operators
Timeline: Ongoing

8.2 PS to share observations and best practices from exercises and events
Timeline: Ongoing

8.3 PS will explore opportunities for various exercise delivery models and platforms
Timeline: Ongoing

9. Utilize existing assessment tools to assess the resilience of critical infrastructure

PS will work with appropriate critical infrastructure stakeholders, including P/Ts, local authorities, and other partners, in order to assess the resilience of Canada's critical infrastructure. This work will be primarily led through the RRAP.

PS, in collaboration with the CCCS, provides the Canadian Cyber Security Tool for organizations to self-assess their organizational resilience and cyber security posture. The tool provides cyber focused advice and guidance, and presents the results as a comparative overview of an organization's cyber security posture. It will assist PS and CCCS in developing the next generation of products and services to address the cyber security needs of Canada's critical infrastructure community.

Deliverables

9.1 PS to continue to utilize the Critical Infrastructure Resilience Tool (CIRT) and Critical Infrastructure Multimedia Tool (CIMT) in conducting RRAP assessments throughout Canada
Timeline: Ongoing

9.2 PS to continue to deliver the Canadian Cyber Resilience Review (CCRR) across Canada, including usage of the Network Security Resilience Analysis tool (NSRA)
Timeline: Ongoing

9.3 PS to conduct research into additional assessment tools and delivery methods
Timeline: Year 2

9.4 PS to deliver the Canadian Cyber Security Tool to the critical infrastructure community
Timeline: Ongoing

10. Enhance the security of Industrial Control Systems for Canada's critical infrastructure community

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. PS will work closely with LFDs and critical infrastructure owners and operators to expand its reach across the ten critical infrastructure sectors.

Deliverables

10.1 PS to host annual ICS security symposiums in person or virtually
Timeline: Ongoing

10.2 PS to host ICS security technical workshops for the critical infrastructure community
Timeline: Ongoing

10.3 PS to host ICS security webinars to expand the reach and number of individuals able to participate
Timeline: Ongoing

11. Renew Canada's strategy and approach to critical infrastructure resilience

PS will undertake a project to renew Canada's strategy and approach to critical infrastructure, which will include extensive research, analysis, and consultation across the broader critical infrastructure community. This renewal project will look at fundamental definitions and concepts; roles and responsibilities; legislative authorities and regulations, and overall program delivery. The outcome will be a forward facing strategy and approach to guide critical infrastructure resilience efforts in a rapidly changing threat and risk environment.

Deliverables

11.1 PS to work closely with P/Ts, the federal community, and the private sector, to develop a new strategy and approach to critical infrastructure resilience
Timeline: Year 3

12. Utilize a tracking mechanism to assess 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 be updated and reported on annually to the NCSF and PS senior management.

Deliverables

12.1 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 (and ongoing)

Annex A: Roles and Responsibilities

Actor	Role	Responsibilities
Federal government	Lead federal activities	- Advance a collaborative federal, provincial, and territorial approach to strengthening the resilience 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 resilience 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:

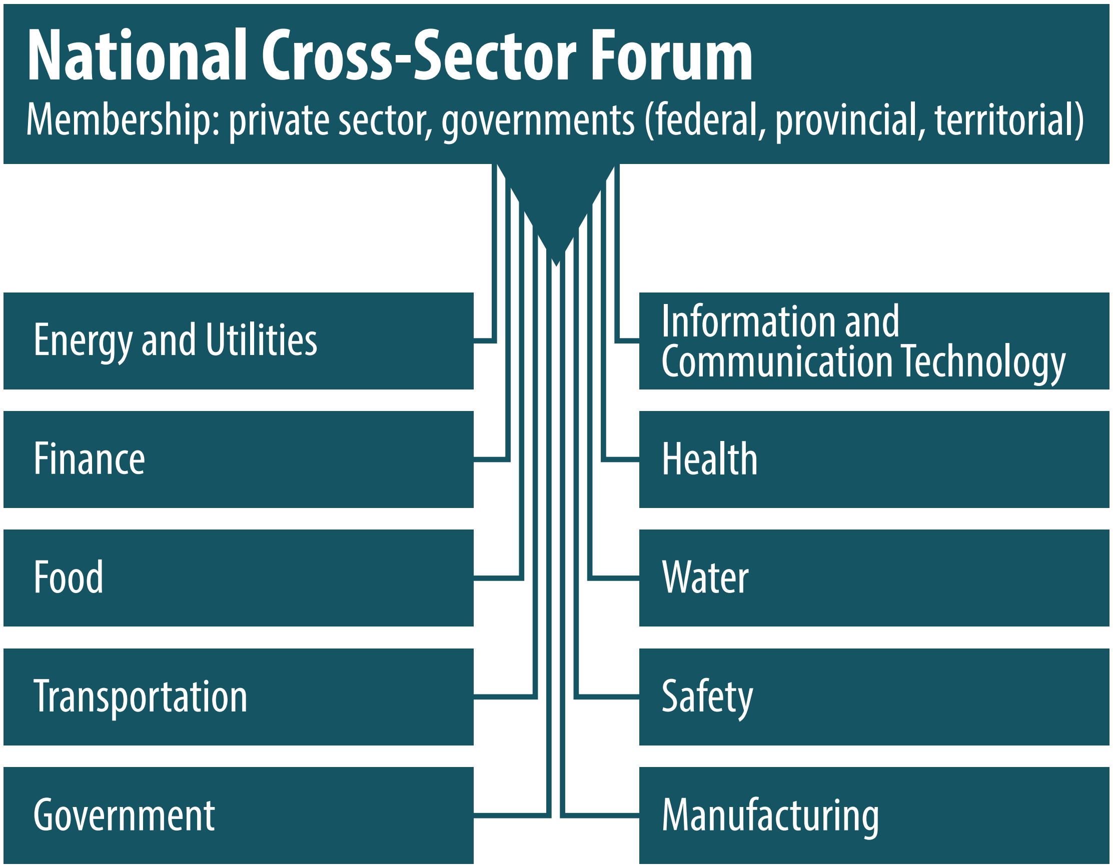
Critical Infrastructure Sectors and Lead Federal Departments/Agencies

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)

This chart outlines NCSF membership, which includes representation from the private sector and federal, provincial and territorial governments. It shows the ten sectors: Energy and Utilities, Finance, Food, Transportation, Government, Information and Communications Technology, Health, Water, Safety and Manufacturing.

Annex D:

Achievements under the National Cross Sector Forum Action Plan for Critical Infrastructure (2018-2020)

BUILDING AND ENHANCING PARTNERSHIPS

Deliverable	Current Status
Address cross-sector issues through multi-sector meetings	Completed (and ongoing)
Engage with provinces and territories to strengthen critical infrastructure resilience	Completed (and ongoing)
Ongoing collaboration with Lead Federal Departments	Completed (and ongoing)
Expand regional outreach of critical infrastructure programs	Completed (and ongoing)
Engage with various international fora to address critical infrastructure issues	Completed (and ongoing)

SHARING AND PROTECTING INFORMATION

Deliverable	Current Status
Modernization and promotion of the Critical Infrastructure Information Gateway	Completed (and ongoing)
Conduct an environmental scan on information sharing	Ongoing
Develop and distribution risk information during a steady state and during disruptive events	Completed (and ongoing)
Support the acquisition of security clearances among private sector stakeholders	Completed (and ongoing)

IMPLEMENT AN ALL-HAZARDS RISK MANAGEMENT APPROACH

Deliverable	Current Status
Increase impact of resilience assessments	Completed (and ongoing)
Implement a risk-based approach to identify key assets and infrastructure of significance	Completed (and ongoing)
Identify ways to support the critical infrastructure community in taking action to address risks	Ongoing
Conduct cross-sector exercises to strengthen preparedness and response	Completed (and ongoing)
Assess the health of the ten critical infrastructure sector networks	Completed (and ongoing)
Support the community in addressing risks associated with the convergence of physical and cyber critical infrastructure systems	Completed (and 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	Completed
Develop a tracking mechanism to assess the progress of activities in the Action Plan	Completed

Annex E:
2021-2023 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
Continuing collaboration with Lead Federal Departments (LFDs)	Ongoing
Engage with various international fora to address critical infrastructure issues	Ongoing
Engage with public and private sector stakeholders on the renewal of Canada's strategy and approach to critical infrastructure	Ongoing

SHARING AND PROTECTING INFORMATION

Deliverable	Timeline
Modernize and promote the Critical Infrastructure Information Gateway (CI Gateway)	Ongoing
Develop and distribute impact assessment products during both steady and event states	Ongoing

IMPLEMENTING AN ALL-HAZARDS RISK MANAGEMENT APPROACH

Deliverable	Timeline
Support sectoral and cross-sectoral exercises to strengthen the preparedness and response abilities of Canada's critical infrastructure	Ongoing
Utilize existing assessment tools to assess the resilience of critical infrastructure	Ongoing
Enhance the security of Industrial Control Systems for Canada's critical infrastructure community	Ongoing
Renew Canada's strategy and approach to critical infrastructure resilience	Year 3
Utilize a tracking mechanism to assess 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
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

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

Canadian Critical Infrastructure Information Gateway
https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx

Enhancing Canada's Critical Infrastructure Resilience to Insider Risk
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx

Royal Canadian Mounted Police
https://www.rcmp-grc.gc.ca/en

Canadian Security Intelligence Service
https://www.canada.ca/en/security-intelligence-service.html

Canadian Centre for Cyber Security
https://cyber.gc.ca/en/

National Cyber Security Strategy
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

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

The Canadian Disaster Database
https://www.publicsafety.gc.ca/cnt/rsrcs/cndn-dsstr-dtbs/index-en.aspx

Emergency Management Strategy for Canada
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-en.aspx