



Public Safety
Canada

Sécurité publique
Canada

Working Towards a National Strategy and Action Plan for **CRITICAL INFRASTRUCTURE**



© Her Majesty the Queen in Right of Canada, 2008

Paper Version:

Cat. No.: PS4-54/2008

ISBN: 978-0-662-05697-3

PDF Version:

Cat. No.: PS4-54/2008E-PDF

ISBN: 978-0-662-48600-8

Printed in Canada

Part I

Working Towards a National Strategy for

CRITICAL INFRASTRUCTURE:

Strategy

We are presenting *Working Towards a National Strategy and Action Plan for Critical Infrastructure* and asking members of the critical infrastructure sectors to provide feedback on this document.

We are asking you to submit your feedback by June 30, 2008, to:
Consultations.CHE@ps-sp.gc.ca or (613) 990-2649.

Table of contents

Working Towards a National Strategy for Critical Infrastructure: Strategy

Executive summary	2
1. Purpose	3
2. Strategic objectives	3
3. Context	3
4. The Strategy	4
4.1 Build trusted partnerships	4
4.2 Implement all-hazards risk management approach	6
4.3 Share and protect information.....	6
5. Review	7
Annex A: From strategy to action	8

Executive summary

Canada's critical infrastructure is vulnerable to disasters, whether natural (e.g., pandemic, floods, ice storms) or human-induced (e.g., terrorism, computer viruses). As the rate and severity of disasters increases, so does the possibility that disruption of critical infrastructure could result in widespread effects, cascading across borders and sectors, rapidly escalating from local to national levels and causing loss of life and economic damages.

Primary responsibility for protecting critical infrastructure rests with the private and public sector owners and operators. In many cases, they have already achieved significant progress. Federal, provincial and territorial levels of government are also working to protect their own critical infrastructure and to support owners and operators in addressing this challenge. The interconnected nature of critical infrastructure, however, demands an integrated approach across all levels of government and the private sector. These efforts need to be pulled together into a collaborative approach that will form the basis of an integrated action plan to enhance the resiliency of critical infrastructure across Canada.

To address the need for coordinated action, federal, provincial and territorial governments are developing a National Strategy and Action Plan that will enhance the resiliency of Canada's critical infrastructure. Its goal is to protect Canadians from disruptions to critical infrastructure.

Successful delivery of the Strategy is based on developing trusted partnerships across all levels of government and the private sector, committing to an all-hazards risk management approach, and improving information sharing and protection.

As the approach to enhancing the resiliency of critical infrastructure varies across jurisdictions, so too does the classification of critical infrastructure by sector. While recognizing that each province and territory structures its critical infrastructure program as it deems appropriate, the National Strategy classifies critical infrastructure within the 10 sectors listed below:

- Energy and utilities
- Finance
- Food
- Transportation
- Government
- Communications and information technology
- Health care
- Water
- Safety
- Manufacturing

Under the Strategy and Action Plan, critical infrastructure efforts will be aligned across these 10 sectors and also across federal, provincial, and territorial jurisdictions. The Action Plan guides the identification of risks, implementation of protective measures and effective response to disruptions of critical infrastructure.

1. Purpose

The purpose of the *National Strategy for Critical Infrastructure* (the Strategy) is to strengthen the resiliency of critical infrastructure in Canada. The Strategy works toward this goal by setting the direction for enhancing the resiliency of Canada's critical infrastructure against current and emerging hazards.

2. Strategic objectives

With a view to enhancing the resiliency of Canada's national critical infrastructure, the objectives of the Strategy are to:

- build trusted and sustainable partnerships;
- implement an all-hazards risk management approach; and,
- advance the timely sharing and protection of information among partners.

3. Context

An Emergency Management Framework for Canada defines critical infrastructure as the essential underlying systems and facilities upon which our standard of life relies. Critical infrastructure consists of the physical and information technology facilities, networks, services and assets essential to the health, safety, security or economic well-being of Canadians, and the effective functioning of government. Disruptions of this critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.

What are the risks to Canada's national critical infrastructure?

The risks are increasingly complex and frequent. They are both natural and human-induced hazards. Recent events illustrate the importance of protecting Canada's critical infrastructure from all types of hazards: the 1996 Saguenay Flood, the 1997 Red River Flood, the 1998 Ice Storm, the terrorist attacks of September 2001, the 2003 Power Blackout, the 2003 Severe Acute Respiratory Syndrome (SARS) outbreak, the 2005 London bombings and Hurricane Katrina.

As the rate and severity of natural disasters increases, so does the possibility that disruption of Canada's national critical infrastructure could result in prolonged loss of essential services. The risks and vulnerabilities are heightened by the complex system of interdependencies among critical infrastructure, which can lead to cascading effects expanding across borders and sectors. The implications of these interdependencies are compounded by society's increasing reliance on information technologies.

Why develop a National Strategy for Critical Infrastructure?

As the risks to critical infrastructure cut across jurisdictions and sectors, the Strategy will provide a comprehensive and collaborative pan-Canadian approach to enhancing the resiliency of critical infrastructure. This common approach will enable partners to respond collectively to risks and target resources to the most vulnerable areas of critical infrastructure.

4. The Strategy

The Strategy proposes that government and the private sector collaborate to protect Canada's critical infrastructure. This collaboration will require the development of trusted partnerships that respect jurisdictions and build upon existing mandates and responsibilities. To foster these partnerships, the Strategy outlines mechanisms for enhanced information sharing and information protection and it identifies the importance of a risk management approach to strengthen critical infrastructure in Canada.

The Strategy recognizes that primary responsibility for protecting critical infrastructure rests with the owners and operators. Federal, provincial and territorial levels of government are also working to protect their own critical infrastructure and to support owners and operators in addressing this challenge.

Enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address human induced intentional threats; business continuity practices to deal with disruptions and ensure the continuation of essential services; and emergency planning to ensure adequate response procedures are in place to deal with unforeseen disruptions to critical infrastructure.

As the approach to strengthening critical infrastructure resiliency varies across jurisdictions, so too does the classification of critical infrastructure by sector. While recognizing that each province and territory structures its critical infrastructure program as it deems appropriate, the National Strategy classifies critical infrastructure within the 10 sectors listed below:

- Energy and utilities
- Finance
- Food
- Transportation
- Government
- Communication and information technology
- Health care
- Water
- Safety
- Manufacturing

4.1 Build trusted partnerships

Strategic objective: Build trusted and sustainable partnerships to support critical infrastructure resiliency.

The Strategy recognizes that each responsible jurisdiction, department and agency, as well as private sector infrastructure owners and operators, will exercise their responsibilities as they deem appropriate for strengthening the resiliency of Canada's critical infrastructure. To be effective, however, implementation of the Strategy will require the collaboration of federal, provincial, territorial and private sector partners and the establishment of mechanisms to facilitate this collaboration.

Sector networks

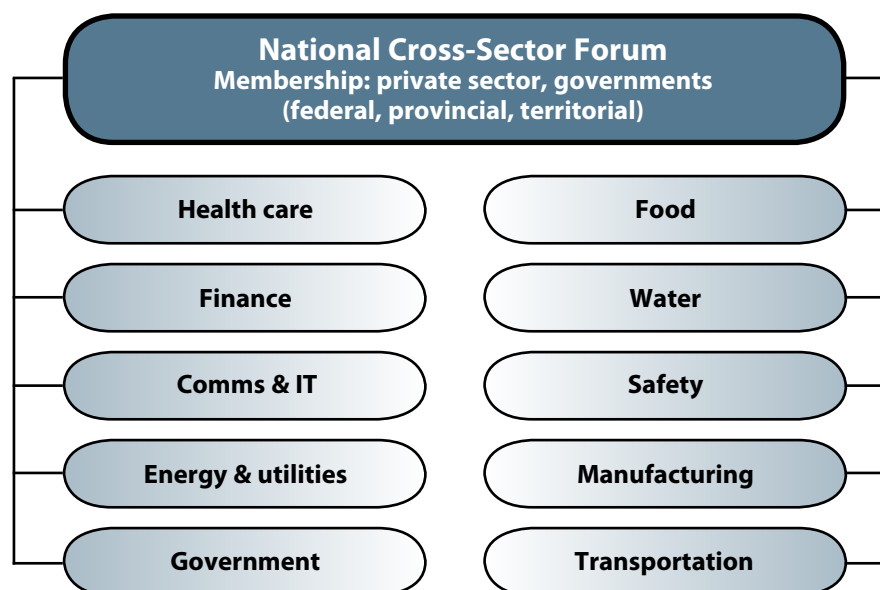
The Strategy proposes to establish a sector network for each of the critical infrastructure sectors. This approach would build to the fullest extent possible upon existing coordination and consultation mechanisms. In recognition of the unique characteristics of each sector, the Strategy does not prescribe the structure of each sector network. At a minimum, the sector networks should support critical infrastructure protection by providing standing fora for discussion and information exchange among partners.

Working with these critical infrastructure partners, each lead department would facilitate the development of sector networks to suit the needs of their stakeholders. The Strategy provides a framework for the possible functions of the sector networks, including:

- promotion of timely information sharing;
- identification of issues of national, regional or sectoral concern;
- use of subject-matter expertise from both the public and private sectors to provide guidance on current and future challenges; and
- development of tools and best practices for strengthening the resiliency of critical infrastructure across the full spectrum of prevention/mitigation, preparedness, response and recovery.

The sector networks will be composed of relevant federal departments and agencies, provinces, territories and key members of the private and public sectors. Participation in these networks will be voluntary. To facilitate the exchange of information, critical infrastructure partners will collaborate to develop a protocol to safeguard information shared through these networks.

To maintain a comprehensive and collaborative pan-Canadian approach to enhancing the resiliency of critical infrastructure, Public Safety Canada will establish the National Cross-Sector Forum. This Forum will promote information sharing across the sector networks and address cross-jurisdictional and cross-sectoral interdependencies. Specific membership will be drawn from the 10 sector networks and will be representative of a broad base of owners and operators, associations, and federal, provincial and territorial governments. Partnership through the National Cross-Sector Forum will form the basis for the implementation of the national approach to critical infrastructure resiliency.



4.2 Implement all-hazards risk management approach

Strategic objective: Implement an all-hazards approach to risk management.

The Strategy promotes the application of risk management and sound business continuity planning. While there are many acceptable approaches to the discipline of risk management, in the context of this Strategy, “risk management” refers to the continuous, proactive, and systematic process to understand, manage, and communicate threats, risks, vulnerabilities and interdependencies across the critical infrastructure community.

Having a strong situational awareness of the risks and interdependencies confronting critical infrastructure in Canada is the first step towards a comprehensive risk management process. As part of the development of emergency management plans and programs, lead federal departments and agencies for each sector are expected to work with provinces and territories and the private sector to acquire a greater understanding of these risks and interdependencies.

To move forward with this comprehensive risk management process, federal, provincial and territorial governments will collaborate with their critical infrastructure partners to develop all-hazards risk analyses. While the Government of Canada will promote a common approach to critical infrastructure protection, and will share tools, lessons learned and best practices, stakeholders are ultimately responsible for implementing a risk management approach appropriate to their situation.

As part of the implementation of the Strategy, federal, provincial and territorial governments intend to conduct exercises and assist in the coordination of regional exercise planning across jurisdictions and with the private sector. The goal is to support a common approach to critical infrastructure protection. These exercises will assist partners to assess and recommend improvements to their protection plans, which will help assure Canadians of a swift and effective response and recovery in the face of a critical infrastructure disruption.

4.3 Share and protect information

Strategic objective: Advance the timely sharing and protection of information among partners and key stakeholders.

Information sharing and information protection are complementary elements of a strong foundation for collaborative efforts to strengthen the resiliency of critical infrastructure. Timely information sharing across governments and the public and private sectors is needed to promote effective risk management and to understand and address critical infrastructure interdependencies. As requested by critical infrastructure stakeholders, improvements in information sharing will include:

- a wider range of information products (e.g. risk assessments, incident reports, best practices, lessons learned, assessment tools);
- improved delivery mechanisms (e.g. web-based critical infrastructure information);
- improved protection of shared information from unauthorized disclosure; and
- expanded production of all-hazards risk information products.

Information protection

In light of the many interdependencies in Canadian critical infrastructure, the inappropriate release of sensitive information that poses a risk for a province, territory or local authority would often also constitute a risk for Canada. Exemptions from disclosure for reasons of national security and public safety already exist under federal, provincial and territorial access to and freedom of information legislation.

These information protection measures notwithstanding, more work should be done to protect information to foster an environment of mutual trust. Governments will work towards providing an appropriate level of protection to emergency management and critical infrastructure information based on sensitivity. A common information sharing protocol to support the trusted sharing of information provided in confidence will be developed through a collaborative approach, including all levels of government. In addition, federal, provincial and territorial governments are encouraged to collaborate to share best practices on information protection. The end result of these efforts will be the development of a more coherent approach to information sharing and information protection in Canada.

5. Review

Federal, provincial and territorial governments will work together to monitor the implementation of the Strategy and support the assessment of programs and activities targeted at enhancing the resiliency of Canada's critical infrastructure.

The Action Plan will be reviewed three years after launch and every five years thereafter.

ANNEX A

From strategy to action: Key priorities for enhancing the resiliency of critical infrastructure

The Strategy will be intentionally positioned as a high-level, principles-based document to accommodate the broad needs of all 10 critical infrastructure sectors while also addressing the unique challenges faced by each sector and jurisdiction.

The implementation of the Strategy will build upon federal, provincial, territorial and public and private sector capabilities, programs and agreements currently in place. The alignment of these activities into a coherent approach is fundamental to developing a national critical infrastructure program.

To implement a cohesive national approach, federal, provincial and territorial partners will continue to work together and collaborate with the private sector to develop a national implementation plan (e.g. risk assessments of national critical infrastructure, all-hazards analyses) that will help form a common operating picture for critical infrastructure across the country.

The participation of federal departments and agencies with responsibilities for critical infrastructure will be essential for collaborating on risk assessments and information exchange. Ultimately, this enhanced situational awareness of Canadian critical infrastructure will be the basis for the actions of governments and the private sector and will help target limited resources to the highest priority areas.

Federal departments and agencies will also collaborate to fulfill Canada's commitments under the *Security and Prosperity Partnership*, including the development and implementation of compatible Canada-U.S. critical infrastructure programs.

The following provides an overview of the initial priorities in the areas of partnerships, risk management and information sharing. These priorities are reflected in the Action Plan required to implement the Strategy.

Partnerships

Develop sector networks so that each of the critical infrastructure sectors will have a forum for discussion and information exchange. At a minimum, the sector networks should support critical infrastructure protection by providing a permanent mechanism for discussion, information exchange and cooperation.

Establish the National Cross-Sector Forum to coordinate the efforts of these sector networks and address cross-sectoral interdependencies. Partnership through the Forum will form the basis for implementing the national approach to critical infrastructure.

Conduct research and development by supporting academia and members of the private sector, thereby helping to anticipate new risks and promote a shared understanding of how research and development can enhance the resiliency of critical infrastructure.

Develop joint initiatives to support cross-jurisdictional efforts to enhance the resiliency of critical infrastructure.

Risk Management

Undertake risk assessments of Canada's critical infrastructure at federal, provincial, territorial and sectoral levels. Public Safety Canada will coordinate the undertaking of these assessments in cooperation with sector networks, key federal departments and agencies, provinces, territories and the private sector.

Develop emergency programs and plans through collaboration between lead federal departments and agencies for each sector, provinces and territories and the private sector.

Conduct exercises and assist in the coordination of regional exercise planning across jurisdictions and with the private sector. This will support a common approach to enhancing the resiliency of critical infrastructure.

Information Sharing

Develop a common information protection protocol to support the trusted sharing of information provided in confidence. This protocol will be developed through a collaborative approach, including all levels of government.

Produce and exchange information products, thereby supporting comprehensive risk/threat assessments, leading to improved coordination of rapid and effective response to disruptions.

Part 2

Working Towards a National Strategy for

CRITICAL INFRASTRUCTURE:

Action Plan

Table of contents

Working Towards a National Strategy for Critical Infrastructure: Action Plan

1. Introduction	14
2. Action Plan	14
2.1 Build trusted partnerships	15
2.2 Share and protect information	18
2.3 Implement all-hazards risk management approach	19
3. Review	22
Annex A: Sector networks	23
Annex B: National Cross-Sector Forum	25
Annex C: Federal-Provincial-Territorial CI Working Group	27
Annex D: Information sharing framework	29
Annex E: Risk management	32

1. Introduction

The *National Strategy and Action Plan for Critical Infrastructure* and supporting Action Plan establish a collective federal, provincial, territorial and private sector approach that will be used to set national priorities and requirements for critical infrastructure resiliency.

In order to keep pace with the rapidly evolving threat environment a key element of Canada's national approach is the Action Plan that builds on the central themes of the National Strategy:

- sustainable partnerships with federal, provincial and territorial governments and the private sector;
- improved information sharing and protection; and
- a commitment to all-hazards risk management.

The Action Plan will be updated regularly to enable partners to anticipate and address new risks. The Strategy recognizes that each province and territory, as well as infrastructure owners and operators, have major roles and responsibilities in critical infrastructure protection and will exercise their responsibilities as appropriate. Progress will be measured by national outcomes, including:

- strengthened resiliency of Canada's critical infrastructure;
- a better understanding of the risks and threats to critical infrastructure; and
- swift and effective response and recovery when disruptions occur.

2. Action Plan

This document sets out action items in the areas of partnerships, risk management and information sharing. Given the range, complexity and linked nature of these action items, a critical path is also detailed. Priorities have been established for the first and second years after release of the National Strategy and Action Plan.

Work will be undertaken across all three themes (partnerships, risk management and information sharing). Within years one and two, partners will focus primarily on the development of sector networks and the National Cross-Sector Forum, as well as improved information sharing. Initial activities in support of risk management will also be undertaken at this time. Their completion is tied to the establishment of the sector networks and the National Cross-Sector Forum. During subsequent years, effective sector networks and improved information sharing will enable further risk management (e.g., development of sectoral risk profiles, guidelines for risk assessments), emergency management planning and exercises.

Actor	Roles	Responsibilities
Federal	Lead national activities	<ul style="list-style-type: none"> - Advance collective national approach to protecting critical infrastructure (CI) - Collaborate with national associations - Collaborate with CI owners and operators within federal mandate in consultation with provinces and territories
Provincial/Territorial	Lead provincial/territorial activities	<ul style="list-style-type: none"> - Collaborate with federal, provincial and territorial (FPT) governments to achieve the objectives of the National Strategy - Coordinate activities with other levels of government, including local governments, associations and CI owners and operators
Critical Infrastructure Owner/Operator	Collaboratively manage risks related to their critical infrastructure	<ul style="list-style-type: none"> - Responsible for risk management - Participate in CI identification, assessment, prevention/mitigation, preparedness, response and recovery activities

2.1 Build trusted partnerships

In year one, Canada’s approach to critical infrastructure will establish the building blocks for collaborative work and information sharing. Year one will feature the development of sector networks and the National Cross-Sector Forum. Renewal of the Federal-Provincial-Territorial Critical Infrastructure (FPT CI) Working Group will be an integral part of the Action Plan and ongoing critical infrastructure initiatives across Canada.

Sector networks will be established, building on existing consultation mechanisms.

Year 1

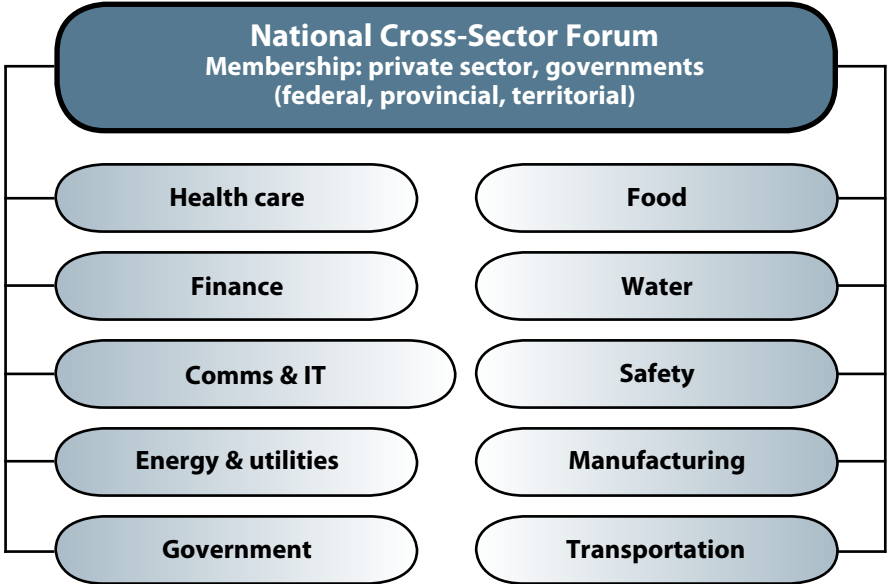
A collective, national approach to critical infrastructure requires the collaboration of federal, provincial, territorial and private sector partners. As a starting point, sector networks will be established, both within and across the critical infrastructure sectors.

The sector networks will provide standing fora for discussion and information exchange among sector-specific industry and government stakeholders. Each sector network will also develop sector risk profiles, support the development of tools and best practices, and lead implementation of the Strategy within their sector.

All 10 critical infrastructure sectors are dependent on communications and information technology. Cyber security requires integrated and focused effort from all levels of government and the private sector. Cyber incidents are not localized events. Responding to a cyber incident cannot be undertaken in isolation of other jurisdictions and sectors. Therefore, in addition to creating a sector network for Communications and Information Technology, each sector network will address cyber risks and interdependencies.

Key Action: Sector networks will be established for each of the 10 critical infrastructure sectors. Members of the sector network (e.g., private sector, federal government, provincial and territorial governments) will set priorities and direct sector-specific work plans. Responsible federal departments and agencies (identified in Annex A) will support these sector networks. Development of the sector networks will build on existing consultation mechanisms. Additional details are provided in Annex A.

Timeline: Sector networks for each critical infrastructure sector will be established in Year 1.



National Cross-Sector Forum: Public Safety Canada will establish the National Cross-Sector Forum to promote collaboration across the sector networks, address interdependencies and promote information sharing across sectors. **Year 1**

To support a pan-Canadian approach to critical infrastructure, the National Cross-Sector Forum will be established to promote collaboration across the sector networks and address cross-jurisdictional and cross-sectoral interdependencies. More specifically, the role of the National Cross-Sector Forum is to:

- provide advice and recommendations to FPT Ministers Responsible for Emergency Management and the FPT Justice Ministers regarding policy and activities relating to critical infrastructure resiliency;
- support the implementation of a risk management approach across sectors;
- review the Strategy and its supporting Action Plan to ensure consistency with the needs of provinces and territories, critical infrastructure owners and operators, and other stakeholders;

- provide feedback and recommendations on the implementation of programs related to the Strategy; and
- facilitate a broad exchange of information between federal, provincial and territorial governments and owners and operators in critical infrastructure issues.

The National Cross-Sector Forum will also establish special working groups, as appropriate, to deal with high priority or emerging issues.

Key action: Public Safety Canada will develop the National Cross-Sector Forum, drawing membership from the chairs of the 10 sector networks and provinces/territories. Additional details are available in Annex B.

Timeline: The National Cross-Sector Forum will be established in Year 1.

FPT CI Working Group will be the standing forum for federal, provincial and territorial government collaboration on CI resiliency matters.

Year 1

As the primary conduit for federal, provincial and territorial government collaboration on CI matters, key roles of the Federal/Provincial/Territorial (FPT) Critical Infrastructure (CI) Working Group include to:

- supporting the implementation of the *National Strategy and Action Plan for Critical Infrastructure* within federal, provincial and territorial jurisdictions;
- facilitating a federal/provincial/territorial network to support critical infrastructure-related information sharing, risk management, planning and exercises;
- cooperating with the sector networks to facilitate private sector initiatives within federal, provincial and territorial jurisdictions;
- providing advice and recommendations to the FPT Senior Officials Responsible for Emergency Management;
- advancing a common understanding of risks and interdependencies; and
- identifying linkages among federal, provincial and territorial programs and initiatives and facilitating an exchange of information and best practices.

Key action: Seek approval of FPT Ministers for the FPT CI Working Group to serve as a standing forum for FPT collaboration on CI matters, including the implementation of the *National Strategy and Action Plan for Critical Infrastructure*. Additional details are available in Annex C.

Timeline: Renewal of the FPT CI Working Group will occur in January 2009.

2.2 Share and protect information

Building on the sector networks, partners will turn their attention towards the development of an information sharing framework that will enable federal, provincial and territorial governments and the private sector to produce and share a wider range of information products in a timely manner. Ultimately, these improvements in information sharing will assist federal, provincial and territorial governments, and the private sector, with risk management.

Establish an information sharing framework to accelerate sharing, improve quality and better protect critical infrastructure information.

Year 2

To facilitate information sharing among critical infrastructure partners, it is proposed that an information sharing framework be established to (i) accelerate dissemination of critical infrastructure information, (ii) improve the quality of information, and (iii) better protect information. The framework will include the following elements:

- identification of existing processes for sharing and protecting critical infrastructure information;
- a plan to address gaps and anticipate new pressures and requirements;
- identification of key points of contact to improve government-to-government and government-to-sector communications;
- enhanced process for disseminating information;
- information protection protocol, including common indicators of the level of sensitivity of the information; and
- address legal and policy barriers to sharing information.

Better information products

Due to the complex jurisdictional issues associated with critical infrastructure, and because information is not readily available on vulnerabilities or protective measures, an accurate assessment of the state of readiness of each sector is difficult. This problem is exacerbated by the uneven quantity and quality of critical infrastructure information across federal departments and agencies, provinces, territories and critical infrastructure sectors.

To improve the quality of information products, federal, provincial and territorial government partners will work directly with sector experts to produce more targeted information (e.g., better threat and risk information), in a Canadian context. Owners and operators can then use that information to protect their assets and essential services.

Information sharing and protection protocol

To facilitate the responsible sharing of sensitive information, an information protection protocol will be developed to establish mechanisms to protect sensitive information from inappropriate disclosure, and ultimately foster an environment of trust among critical infrastructure partners. The protocol will serve as the basis for the development of information sharing agreements. The protocol will also recognize that the sharing and disclosure of protected / classified information is governed by existing federal, provincial and territorial legislation and policies. Development of this protocol will include efforts to address related federal/provincial/territorial policy and legal barriers as well as actual or perceived gaps.

Information dissemination

A single framework is needed to enable quick exchange of information among key points of contact across the 10 critical infrastructure sectors. Federal, provincial and territorial governments and the private sector will develop this process to enable timely information exchange to deal with real or potential disruptions that threaten the integrity of Canada's critical infrastructure.

Key action: Federal, provincial and territorial government partners will collaborate to develop an information sharing framework. Additional details are available in Annex D.

Timelines: An information sharing framework will be completed in Year 2.

2.3 Implement all-hazards risk management approach

While trusted partnerships and enhanced information sharing represent the building blocks of Canada's approach to enhancing the resiliency of critical infrastructure, these cannot be undertaken in isolation of risk management and the development of plans and exercises to address these risks.

Risk assessments of Canada's critical infrastructure: Sector risk profiles will be developed through sector networks, in cooperation with federal departments and agencies, provinces, territories and the private sector.

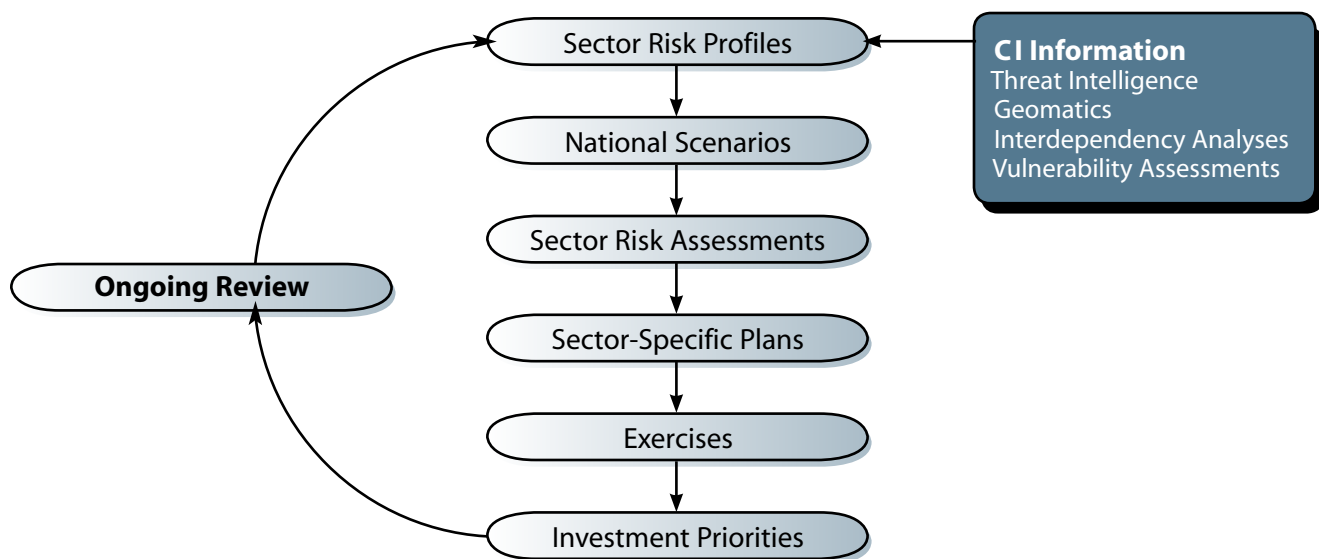
Year 2 and ongoing

Although the Strategy promotes a common approach to enhancing the resiliency of critical infrastructure, owners and operators and all jurisdictions are ultimately responsible for implementing a risk management approach appropriate to their situation. Implementation of a risk management approach to Canada's critical infrastructure will include the development of three different types of products:

1. Sector risk profiles at the national level;
2. Risk assessments; and
3. Risk management tools and guidance.

The success of these efforts, in particular the sector risk profiles, is dependent on other elements of the Action Plan, such as the development of sector networks and improved information sharing. Information will be drawn from provincial/territorial sector risk profiles, as appropriate, to support and validate the sector risk profiles at the national level.

The sector risk profiles will be useful to each sector network in identifying priority areas of sectoral concern, research and planning, development of a sector-specific plan and assessing the effectiveness of critical infrastructure programs and activities. Each sector risk profile will be combined to provide a consolidated overview of the risks across all sectors to critical infrastructure in Canada.



As illustrated in the flow chart above, the sector risk profiles will enable the development of scenarios (e.g., regional, national, international). Scenario-driven models will, in turn, facilitate the development of more precise sector risk assessments and sector-specific plans to address these risks. Ultimately, these risk assessments will guide investment priorities for each sector.

Key action: The undertaking of sector risk profiles will be managed through each sector network.

Timelines: Sector risk profiles will be completed in Year 2. Tools and guidance will be shared on an ongoing basis. Owner/operator risk assessments will be an ongoing activity.

Sector-specific work plans will be developed and shared among federal, provincial and territorial partners and owners and operators to address risks to critical infrastructure.

Year 3 and ongoing

Sector-specific work plans will be useful to each sector network in addressing all hazards and interdependencies confronting their critical infrastructure. Although each plan will be tailored to the structures and challenges of its sector, the FPT CI Working Group will provide support to each sector network by developing a sector-specific plan model.

Characteristics of effective sector-specific work plans include, but are not limited to, the following:

- *Comprehensive:* Effective plans and programs must address physical, cyber and human elements of critical infrastructure. In addition to the all-hazards component of these plans and programs, analysis should be undertaken to identify and address interdependencies within and across sectors.

- *Integrated:* In light of the shared responsibility for addressing risks to critical infrastructure, and given the widespread implications of critical infrastructure interdependencies, sector-specific work plans need to be complementary across federal, provincial and territorial governments and sectors.
- *Risk-based:* Sector-specific work plans should be based on an understanding of the risk environment and designed to allow measurement, evaluation and feedback on the effectiveness of mitigation efforts. This allows owners, operators and governments to reevaluate risk levels after the program has been implemented.

Key Action: To address the risks identified in the sector risk profiles, sector-specific work plans will be developed through the sector networks. These plans will be complementary across federal, provincial and territorial governments and sectors.

Timelines: Sector-specific work plans will be completed in Year 3. These work plans are living documents and will be updated on an ongoing basis. Owner/operator critical infrastructure plans will be an ongoing activity.

Exercises: Federal, provincial and territorial governments, in collaboration with the private sector, will conduct national exercises in support of a common approach to enhancing the resiliency of critical infrastructure.

Ongoing

Exercises provide:

- an efficient means to test, evaluate and improve planning;
- training in a lower-risk environment for responders, emergency managers and senior officials at all levels; and
- quality assurance for response to disruptions.

Exercises are underway across Canada on an ongoing basis (e.g., through federal, provincial and territorial emergency managers and owners and operators). Through these exercises, federal, provincial and territorial governments cooperate with the sectors to assess capabilities for responding to disruptions of critical infrastructure. The purpose of these exercises is to clarify roles and responsibilities, address interdependencies and raise awareness of the risks to critical infrastructure.

Key action: Federal, provincial and territorial governments will conduct exercises and assist in the integration of regional exercise planning across jurisdictions and with the private sector to support a common approach to enhancing the resiliency of critical infrastructure.

Timelines: Exercises will be an ongoing activity.

3. Review

Federal, provincial and territorial governments and the private sector will work together to monitor the implementation of the Strategy and support the assessment of programs and activities targeted at enhancing the resiliency of Canada's critical infrastructure.

The Action Plan will be reviewed, in collaboration with the sector networks, the National Cross-Sector Forum and the FPT CI Working Group three years after launch and every five years thereafter.

Annex A

Sector networks

Purpose

The purpose of the sector networks is to develop national sector-specific standing fora to address cross-sector and regional issues, and enable information sharing on critical infrastructure.

Recognizing the unique structures and challenges faced by each sector, the following should be considered as guidelines for the development and role of the sector networks. The sector networks will:

- promote timely information sharing;
- identify issues of national, regional or sectoral concern, such as cyber security;
- advance a common understanding of risks and interdependencies, and conduct sector-specific all-hazards risk analyses;
- support the development of sector-specific work plans to address risks and interdependencies;
- participate in exercises to test sector-specific work plans and identify new risks;
- provide guidance on current and future challenges related to the sector; and
- promote the development of tools and best practices for enhancing the resiliency of critical infrastructure.

It is expected that a sector network will be developed for each of the 10 critical infrastructure sectors. Where appropriate, sub-sector networks may also be established to reflect the diversity of a particular sector. The critical infrastructure sectors and the responsible federal government departments/agencies are set out in the table below. As required, supporting federal departments will also participate in the sector networks.

Sectors	Responsible federal department
Energy and utilities	Natural Resources Canada
Communications and Information Technology	Industry Canada
Finance	Finance Canada
Health care	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

Membership

Participation in these networks is voluntary. Each sector network will develop governance processes and roles appropriate to the sector. In most cases, the sector networks will be composed of owners and operators from the sector (with a focus on national industry associations), relevant federal departments and agencies, provinces and territories. Involvement of associations will be valuable in achieving effective outreach and gaining buy-in from the sector.

To facilitate the exchange of information, members of the sector network will collaborate to develop guidelines to safeguard information being shared through their network. It is also expected that each member will sign a non-disclosure agreement.

The Chair of each sector network will represent the sector at the National Cross-Sector Forum.

Role of federal government departments

In recognition of the unique characteristics of each sector, and building upon existing consultation mechanisms, each responsible federal department will work together with its private sector partners, other federal departments and provinces and territories to facilitate the development of individual sector networks.

More specifically, the role of the responsible federal departments and agencies will be to:

- develop and maintain sector networks;
- encourage and facilitate collaboration among sector partners;
- enable information sharing within and between sectors and governments;
- support the development of sector risk profiles;
- provide secretariat support and guidance to the sector network; and
- support the development and implementation of sector-specific work plans.

Public Safety Canada will work with its partners and support sector networks through each lead federal department and agency in the areas of information sharing, threat assessments and analysis, integration of strategic issues, development of sector-specific work plans, identification of interdependencies, tools and guidelines, and other pertinent issues as necessary.

Annex B

National Cross-Sector Forum

Purpose

Establish a National Cross-Sector Forum to maintain a comprehensive and collaborative pan-Canadian approach to critical infrastructure by providing a standing mechanism for discussion and information exchange within and between the federal, provincial and territorial governments as well as with the private sector.

The role of the National Cross-Sector Forum is to:

- provide advice and recommendations to standing fora relating to emergency management;
- foster a coherent approach to critical infrastructure at all levels and address cross-jurisdictional and cross-sectoral interdependencies;
- recommend actions regarding research priorities, the sharing of information, the development of CI plans and exercises;
- establish special working groups, if necessary, to deal with high priority or emerging issues;
- review the Strategy and supporting Action Plan to ensure consistency with the needs of the federal, provincial and territorial governments, owners and operators, and other stakeholders; and
- facilitate information sharing between federal, provincial and territorial governments and owners and operators on physical and cyber security.

Regular reports on the work of the Forum will be provided to the Assistant Deputy Ministers Committee for Emergency Management (federal government), the FPT Deputy Ministers Responsible for Emergency Management and the FPT Senior Officials Responsible for Emergency Management. Formally, the Forum will report to the FPT Ministers Responsible for Emergency Management (and the FPT Justice Ministers, as appropriate).

As the primary conduit for federal, provincial and territorial government collaboration on CI matters, the Federal/Provincial/Territorial (FPT) CI Working Group supports the implementation of the *National Strategy for Critical Infrastructure* within federal, provincial and territorial jurisdictions. The FPT CI Working Group Co-Chairs will report to the FPT Senior Officials Responsible for Emergency Management on CI matters.

Membership

Membership will be drawn from the sector networks and will be representative of a broad base of owners and operators, associations, and federal, provincial and territorial governments. Membership will develop the terms of reference for the National Cross-Sector Forum, including designation of chair(s).

The chair(s) will work with the members to set agendas, determine the frequency of meetings and to manage the business of the Forum.

Procedures

- To facilitate the exchange of information, the members will sign a non-disclosure agreement and the Forum will adopt information sharing guidelines to protect information from inappropriate disclosure.
- The Forum may hold open or closed meetings.
- The Forum may invite senior federal government officials and other experts to participate in its meetings and to act as subject matter experts.

Secretariat

The Critical Infrastructure Policy Division, Public Safety Canada, will serve as the Forum's secretariat. The Division's staff will provide strategic advice, support information sharing, develop the cross-sector risk profile and provide general support to the Forum. Division staff members will also manage the preparation of documents for the meetings and prepare meeting summaries and reports.

Remuneration

The Forum members serve without remuneration, but members from outside the National Capital Region may be reimbursed for travel and living expenses associated with the meetings according to the Treasury Board of Canada guidelines.

Annex C

Federal/Provincial/Territorial CI Working Group

Purpose

The purpose of the FPT CI Working Group is to be the standing forum and primary conduit for federal/provincial/territorial government collaboration on CI matters.

Objectives/Priorities

- Support the implementation of the National Strategy within federal, provincial and territorial jurisdictions;
- Participate in the evolution and implementation of the Action Plan;
- Act as a clearinghouse for the provinces and territories on CI related issues with a direct input to Public Safety Canada through the FPT Senior Officials Responsible for Emergency Management;
- Facilitate federal/provincial/territorial networking to support CI information sharing, risk management, CI planning and exercises;
- Cooperate with the sector networks to facilitate private sector CI initiatives within provincial and territorial jurisdictions;
- Identify CI issues of regional or jurisdictional concern;
- Advance a common understanding of CI risks and interdependencies;
- Participate in exercises to test sector-specific work plans and identify new risks;
- Provide guidance on current and future challenges related to CI; and,
- Identify linkages among federal, provincial and territorial programs and initiatives and facilitate sharing of information and best practices.

Membership

Membership in the Working Group (WG) is open to all provinces and territories to participate in accordance with their needs and as their resources permit. All provinces and territories are members of the FPT CI Working Group regardless of their presence at meetings; no decision will be made without the sharing of information and the opportunity to comment by all provinces and territories.

The Emergency Management and National Security (EMNS) Branch, Public Safety Canada will be the federal government lead.

It has been agreed that all decisions would be made by consensus.

The WG will be co-chaired by a representative from EMNS Branch, Public Safety Canada and a provincial/territorial representative determined by group consensus.

Other participants (may include, but are not exclusive to private sector representatives and other federal government departments) may be invited on an ad-hoc basis as determined by the subject-matter being discussed.

Terms of reference

Policy and planning basis

- *Emergency Management Act*
- *Department of Public Safety and Emergency Preparedness Act*
- *National Security Policy*
- *An Emergency Management Framework for Canada*
- *National Strategy and Action Plan for Critical Infrastructure*
- *Government Security Policy*
- Provincial/territorial equivalent (legislation, programs, plans, policies, strategies, initiatives or their equivalents, etc.)
- MOUs and Agreements between applicable orders of government
- FPT CI Working Group terms of reference

Reporting

The WG Co-Chairs (EMNS Branch, Public Safety Canada and a provincial/territorial representative) will report to the FPT Senior Officials Responsible for Emergency Management on CI matters. At the National Cross-Sector Forum the provincial and territorial governments will be represented by the provincial/territorial Co-Chair of the FPT CI Working Group.

Working Group Secretariat

Public Safety Canada will serve as the secretariat for the FPT CI WG by organizing meetings, as identified by the co-chairs, and will be responsible for preparing and distributing material.

Annex D

Information sharing framework

Purpose

The following outlines a way forward to producing a wider range of relevant critical infrastructure information products and sharing them in a timely manner.

Challenges

Currently, critical infrastructure protection is hampered by (i) uneven understanding of threats and vulnerabilities, (ii) insufficient sharing of information and (iii) limited integration of existing information into coherent situational awareness. While the development and exchange of information is often characterized as a problem for the federal government to resolve, all stakeholders must play an active role.

Information sharing framework

To facilitate information sharing among critical infrastructure partners, the Action Plan proposes that an information sharing framework be established to provide a clear structure for the process of establishing information sharing relationships. Three key features of this framework are the information protection protocol, development of better information products and information dissemination:

1. Information protection protocol

As a starting point, an information protection protocol is needed to facilitate sharing of sensitive CI information between the Government of Canada, provincial and territorial governments and private sector owners and operators. It will provide guidance for the protection of sensitive information in support of more accurate and timely information sharing between organizations by setting out the principles which underpin information protection. It will also assist organizations in the development of information sharing agreements or memoranda of understanding on information sharing and protection. Development of this protocol will include efforts to address federal, provincial and territorial policy and legal barriers on protected/classified material.

Purposes for which shared CI information may be used

The protocol will apply to the exchange of CI information that is shared in confidence by private sector CI owner and operators. Examples of uses of CI information include but are not limited to:

- managing response to an emergency;
- establishing policies and programs relating to emergency management and critical infrastructure (CI) in both physical and cyber dimensions;
- conducting exercises and providing training related to CI;
- developing information products and tools to support national-level, sectoral and cross-sectoral initiatives (e.g., all-hazards risk assessments, high-level risk profiles);
- developing all-hazards risk and vulnerability management tools; and
- analyzing interdependencies between CI sectors.

2. Better information products

Due to the complex jurisdictional issues associated with critical infrastructure, and the lack of information on interdependencies, vulnerabilities or protective measures, it is difficult to develop accurate assessments of the state of readiness of each sector. This problem is exacerbated by the uneven quantity and quality of critical infrastructure information across federal departments and agencies, provinces, territories and critical infrastructure sectors.

To improve the quality of information products, Public Safety Canada (in partnership with the Integrated Threat Assessment Centre and the Royal Canadian Mounted Police) will work directly with industry experts to produce more targeted information (e.g., better threat and risk information), in a Canadian context, that owners and operators can use to protect their assets and essential services and develop comprehensive emergency management plans.

3. Information dissemination

As a starting point in the development of the information sharing framework, information dissemination will be improved for (i) emergency situations and (ii) regular situations.

Emergency situations

During an emergency, a single structure is needed to enable quick exchange of information among key points of contact across the 10 critical infrastructure sectors. To accomplish this, connections between federal, provincial and territorial points of contact and with owners and operators need to be strengthened. Federal, provincial and territorial governments will collaborate to develop this process to enable timely information exchange to deal with disruptions – real or perceived, imminent or actual, a natural disaster or terrorist activity – that threaten the integrity of Canada's critical infrastructure.

Regular situations

The federal government currently sponsors security clearances for key private sector stakeholders in some critical infrastructure sectors who require information related to the protection of their critical infrastructure. On an ongoing basis, Public Safety Canada will examine the need to expand the availability of these security clearances for each of the 10 critical infrastructure sectors. In addition, the FPT CI Working Group will consider other options for improved information dissemination (e.g., scrubbing sensitive information to allow for regular unclassified distribution).

For lower sensitive information, a secure web-based CI information sharing portal will also be developed. Development of this CI portal will leverage existing mechanisms, where appropriate, to reduce duplication and streamline processes. Creation of this CI portal will be an iterative process and three general development phases can be outlined.

The first development phase will involve:

- establishing the overall governance framework;
- consulting with stakeholders to determine their CI information sharing needs;
- constructing the CI information sharing portal to support sharing of unclassified CI information; and
- initially populating the portal with unclassified information.

Initially, the CI information sharing portal will only support the sharing of public, unclassified information (Public Layer). The first phase of development will be completed within one year of approval of the National Strategy.

The goal of the second phase is to begin populating the portal with information related to all aspects of CI. This second phase will reflect the Strategy’s all-hazards approach and will include adding information products such as physical and cyber threats, tools for risk assessments, interdependency assessments and other unclassified information products.

The final phase of development will involve implementing the secure, web-based user authentication and information sharing system (Secure Layer). The Secure Layer will support two-way information sharing of classified information, including threat and risk assessments. The Secure Layer will include discussion forums, workspaces, exercise calendars, and other information sharing tools. This Layer will facilitate communication between sector network members, National Cross-Sector Forum members and other CI stakeholders.

Timeline: *Information sharing framework*

Action	Lead
Year 1	
Establish information sharing protocol	Public Safety Canada
Define roles and responsibilities of key information sharing partners	Special Working Group of the National Cross-Sector Forum
Compile inventory of information currently being shared	Special Working Group of the National Cross-Sector Forum
Identify information gaps and anticipate new requirements	Special Working Group of the National Cross-Sector Forum
Develop statement of requirements for the CI Information Sharing Portal	Public Safety Canada
Year 2	
Establish the Public Layer of the CI Information Sharing Portal	Public Safety Canada
Develop and test secure, web-based user authentication	Public Safety Canada
Implement the Secure Layer of the CI Information Sharing Portal	Public Safety Canada
Ongoing	
Enhance information dissemination	FPT partners, private sector and sector networks
Populate Public and Secure Layers of the Portal	FPT partners, private sector and sector networks

Annex E

Risk management

Managing risk is a shared responsibility of all critical infrastructure (CI) stakeholders to continuously, proactively and systematically understand, manage, and communicate risks and interdependencies across the critical infrastructure community. Moving forward with this comprehensive risk management process requires federal, provincial and territorial governments to collaborate with their critical infrastructure partners.

While the Strategy promotes a common approach to enhancing the resiliency of critical infrastructure, and the sharing of tools and best practices, owners and operators and each jurisdiction are ultimately responsible for implementing a risk management approach appropriate to their situation.

Implementation of a risk management approach to Canada's CI will require the development of three different types of products:

1. Sector risk profiles at the national level;
2. Risk assessments; and
3. Risk management tools and guidance.

The success of these efforts, in particular the sector risk profiles, is dependent upon other elements of the Action Plan such as the successful establishment of the sector networks and improved information sharing and development.

Timelines: Sector risk profiles should be completed in Year 2. Tools and guidance will be disseminated as soon as sector networks are established and new tools will be developed on an ongoing basis. Owner/operator risk assessments, where they exist, will be an ongoing activity.

Sector risk profiles

It is essential that all of the key CI partners within a sector have an accurate and common understanding of their risk environment. These sector risk profiles will provide a global understanding of this risk environment through an analysis of:

- existing practices;
- key threats to each sector;
- common vulnerabilities within a sector;
- key interdependencies; and
- the risk tolerance of each sector.

Depending upon the nature of each sector and the structure of its sector network, sub-sector risk profiles may also be undertaken. These in turn will be incorporated within the broader sector risk profile.

The profiles will be useful to each sector network in identifying priority areas for collective action, issues of sectoral concern, priorities for research, development of a sector-specific work plan and assessing the effectiveness of CI programs and activities.

Once completed, each network will provide its profile to the National Cross-Sector Forum. Each sector or sub-sector profile will be combined to provide a consolidated overview of the risks across all sectors. This consolidated profile will support interdependencies analysis and also be made available to each sector network.

The undertaking of sector risk profiles at the national level will be managed through each sector network and led by the responsible federal department with the active support of sector network members. Public Safety Canada and Defence Research and Development Canada will provide support to each sector network, including a sector risk profile model.

Defence Research and Development Canada will develop sector-specific strategic risk assessments to support each sector network. These will not look at individual assets, sites or systems but will include a priority ranking of generic threats to particular CI sectors and elements within specific sectors, and the probable impacts of these threats. This information will be used to improve upon future iterations of the sector risk profiles.

Timelines: The sector risk profiles will be living documents. Each sector risk profile should be completed in Year 2 and revised on an ongoing basis. To ensure the most up-to-date information is available to each sector network, sector risk profiles should be submitted to the National Cross-Sector Forum annually.

Risk assessments

A risk assessment is a detailed analysis of threats, vulnerabilities and impacts to a particular CI asset, site or system. These assessments will provide a detailed and specific understanding to each CI site owner/operator of their particular risk environment. Though considered an important activity to ensure the protection of CI, the Strategy does not impose a requirement on owner and operators to undertake risk assessments.

Risk assessments can be used by owner and operators to support the development of sector-specific work plans to address highest risks on a priority basis as well as to develop and implement site-specific emergency plans, such as business continuity plans.

The Strategy does not impose a single risk assessment methodology on CI partners. There are a number of respected assessment methodologies and the needs and capabilities of each sector and CI owner/operator are diverse. Nevertheless, some consistency is needed to ensure that, at minimum, assessments have certain commonalities to support comparison within and across sectors. It is expected, therefore, that each owner/operator's risk assessment will contain at least:

- identification of the critical assets and systems to be covered by the risk assessment;
- an assessment of threats (natural, deliberate and accidental);
- an assessment of vulnerabilities;
- an assessment of the impacts of disruptions to the CI; and
- an assessment of interdependencies.

Undertaking risk assessments is the responsibility of the owner/operator. To support the assessment process, and as part of improving information development and sharing, sector-specific threat information will be provided to each sector network for distribution to its members. Public Safety Canada will work with its CI partners such as Defence Research and Development Canada, the Integrated Threat Assessment Centre and the Royal Canadian Mounted Police to provide tools and guidance for the development of risk assessments (see 'Risk Management Tools' below).

It is expected that most CI owners/operators will have already undertaken risk assessments to some degree. As part of the sector risk profile development process, each sector network will assess the degree to which its CI has been subject to a risk assessment by its owner/operator.

CI asset, site or system risk assessments will neither be shared broadly across the sector network nor used to create a central inventory of critical infrastructure. A trusted information sharing environment, supported by the CI Information Protection Protocol, will be created (see Annex D). It is expected that owners/operators will share risk-related information with relevant government officials and other CI owner/operators to support broader risk assessment and emergency planning activities.

Timelines: As the Strategy does not impose a requirement on CI owner/operators to undertake assessments, there is no deadline for the completion of risk assessments. Each sector network may, however, establish recommendations for risk assessments as it deems appropriate.

Risk management tools and guidance

To improve collective understanding of risk management, common tools, guidelines, methodologies and plans will be made available. Public Safety Canada, with the support of sector networks, the National Cross-Sector Forum and the FPT CI Working Group, will lead this process.

It is expected that these tools will include a common lexicon of risk management concepts, risk assessment methodologies, educational and awareness materials, and guidelines for implementing a risk management program.

The development of the risk management "tool box" will begin with a survey of available materials. Where no suitable materials have been found to address an identified need, new tools will be developed in priority order as decided by the National Cross-Sector Forum.

It is expected that these tools will be distributed through each sector network as well as via the common web-based Information Sharing Portal (see Annex D).

Timelines: The development and dissemination of risk management tools will be an ongoing process but it is expected that the needs identification and survey of available materials will be initiated within nine months of establishing a sector network.