

ACTION PLAN

ActionPlan

for Critical Infrastructure



Government of Alberta



Manitoba



Newfoundland
Labrador



NOVA SCOTIA
NOUVELLE-ÉCOSSE



Ontario



Québec



Yukon
Government

Canada

© Her Majesty the Queen in Right of Canada, 2009

Cat. No.: PS4-66/2009
ISBN: 978-0-662-06347-6

Printed in Canada



Table of contents

| | |
|--|----|
| 1. Introduction | 2 |
| 2. Action Plan | 2 |
| 2.1 Build partnerships | 4 |
| 2.2 Share and protect information | 7 |
| 2.3 Implement all-hazards risk management approach | 8 |
| 3. Review | 11 |
| Annex A – Sector networks | 12 |
| Annex B – National Cross-Sector Forum | 14 |
| Annex C – Federal-Provincial-Territorial Critical Infrastructure Working Group | 16 |
| Annex D – Information sharing framework | 18 |
| Annex E – Risk management | 21 |





1. Introduction

The *National Strategy for Critical Infrastructure* and supporting Action Plan establish a collaborative federal, provincial, territorial and critical infrastructure sector approach that will be used to strengthen critical infrastructure resiliency.

To keep pace with the rapidly evolving risk environment, a key element of the national approach is an Action Plan that builds on the central themes of the National Strategy:

- sustainable partnerships with federal, provincial and territorial governments and critical infrastructure sectors;
- improved information sharing and protection; and
- a commitment to all-hazards risk management.

This Action Plan will be updated regularly to enable partners to anticipate and address new risks. The Strategy recognizes that each government, as well as infrastructure owners and operators, have major roles and responsibilities in strengthening the resiliency of critical infrastructure and will exercise their responsibilities as appropriate and according to the governments' respective jurisdictions. Provincial and territorial governments will also coordinate activities with their municipalities and local governments where it applies. Progress will be measured by national outcomes, including:

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



2. Action Plan

This Plan 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. The Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management have established priorities for the first and second years after release of the *National Strategy for Critical Infrastructure*.

Work will be undertaken across all three elements of the Strategy (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 National Cross-Sector Forum. During subsequent years, effective sector networks and improved information sharing will enable further risk management activities (e.g., development of sectoral risk profiles, guidelines for risk assessments), emergency management planning and exercises.

The Action Plan recognizes that, in an emergency, the first response is almost always by the municipalities and at the provincial and territorial level because disasters occur most often locally and because provincial and territorial governments have responsibility for emergency management within their respective jurisdiction. Should a provincial or territorial government require resources beyond their own in an emergency or critical infrastructure disruption, the federal government responds rapidly to any request for assistance.

Consistent with the *National Strategy for Critical Infrastructure* and the *Emergency Management Framework for Canada*, the following chart describes the roles and responsibilities for the Action Plan.

| | Roles | Responsibilities |
|---|---|---|
| Federal government | Lead federal activities | <ul style="list-style-type: none"> • Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure • Collaborate with provincial and territorial governments to achieve the objectives of the Strategy • Collaborate with national associations • Collaborate with critical infrastructure owners and operators within federal mandate in consultation with provinces and territories |
| Provincial / territorial governments | Lead provincial/ territorial activities | <ul style="list-style-type: none"> • Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure • Collaborate with federal, provincial and territorial governments to achieve the objectives of the Strategy • Coordinate activities with their stakeholders, including municipalities or local governments where it applies, associations and critical infrastructure owners and operators |
| Critical infrastructure owners/ operators | Collaboratively manage risks related to their critical infrastructure | <ul style="list-style-type: none"> • Manage risks to their own critical infrastructure • Participate in critical infrastructure identification, assessment, prevention, mitigation, preparedness, response and recovery activities |



2.1 Build partnerships



In year one, the building blocks for collaborative work and information sharing will be established. Year one will focus on the development of sector networks and a National Cross-Sector Forum. Renewal of the Federal-Provincial-Territorial Critical Infrastructure Working Group will be an integral part of this Action Plan and ongoing critical infrastructure initiatives across Canada.

The enormity and complexity of critical infrastructure, the interdependencies that cross sectors and jurisdictions, and the uncertain nature of risks and natural disasters make the effective implementation of protection efforts a great challenge. The coordination mechanisms described below establish linkages among federal, provincial and territorial governments and critical infrastructure sectors. They will all be invited to participate in the sector networks and will be represented at the National Cross-Sector Forum. In addition to direct coordination between critical infrastructure partners, the structures described below provide a national framework that fosters relationships and improves information sharing and risk management within and across critical infrastructure sectors.

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

Year 1

A collaborative, national approach to critical infrastructure requires the collaboration of federal, provincial, territorial and critical infrastructure sector partners. As a starting point, at the national level, sector networks will be established, for each of the critical infrastructure sectors.

The sector networks will provide standing fora for discussion and information exchange among sector-specific industry stakeholders and governments. The sector networks reflect a partnership model that will enable governments and critical infrastructure sectors to undertake a range of activities (e.g. risk assessments, plans to address risks, exercises) unique to each sector. These sector networks will also enable improved collaboration among critical infrastructure partners in the development and execution of risk management and information sharing activities. Each sector network will also develop sector risk profiles, support the development of tools and best practices, and advance implementation of the Strategy within their sector.

Recognizing the interconnected nature of critical infrastructure, all critical infrastructure sectors are confronted with the challenge of addressing interdependencies. Responding to a disruption in one critical infrastructure sector cannot be undertaken in isolation of other sectors. For example, all critical infrastructure sectors are dependent on human resources, government services and cyber systems. Therefore, each sector network will adopt a comprehensive approach to strengthening the resiliency of critical infrastructure, based on an integrated, all-hazards risk management approach.

In collaboration with federal, provincial and territorial governments, each sector network will also establish an approach to identifying and addressing international critical infrastructure issues. To support these efforts, each sector network will be provided with a methodology and template incorporating international factors into their sector risk profile.

Key Action: Sector networks will be established for each of the 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. 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: A National Cross-Sector Forum will be established to promote collaboration across the sector networks, address interdependencies and promote information sharing across sectors.

Year 1

To support a collaborative approach to critical infrastructure, a 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 the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management 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, and with those of critical infrastructure owners and operators, and other stakeholders;
- provide feedback and recommendations on the implementation of actions related to the Strategy; and
- facilitate a broad exchange of information between federal, provincial and territorial governments and owners and operators on critical infrastructure issues.

The National Cross-Sector Forum will also identify high priority and emerging issues and make relevant recommendations to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management to address these issues.

Key action: The Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management will develop the National Cross-Sector Forum, drawing membership from the chairs of each sector network. Additional details are available in Annex B.

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

Federal-Provincial-Territorial Critical Infrastructure Working Group

will be the standing forum for federal, provincial and territorial government collaboration on critical infrastructure resiliency matters.

Year 1

As the primary conduit for federal, provincial and territorial government collaboration on critical infrastructure matters, key roles of the Federal-Provincial-Territorial Critical Infrastructure Working Group include:

- supporting the implementation of the *National Strategy for Critical Infrastructure* and Action Plan within federal, provincial and territorial governments;
- 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 Federal-Provincial-Territorial 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: Renewal of the Federal-Provincial-Territorial Critical Infrastructure Working Group. Additional details are available in Annex C.

Timeline: January 2010.





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 critical infrastructure sectors to produce and share a wider and more timely range of information products, in full respect of existing federal, provincial and territorial legislation and policies. Ultimately, these improvements in information sharing will assist federal, provincial and territorial governments, and the critical infrastructure sectors, 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;
- addressing 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, provincial and territorial governments, and critical infrastructure sectors.

To improve the quality of information products, federal, provincial and territorial governments will work directly with their sector experts to produce more targeted information (e.g., better risk information), in a Canadian context. The sector networks will identify areas of emerging concern and identify priority areas for information products. Owners and operators can then use that information to improve the resiliency of their assets and essential services.

Information sharing and protection protocol

To facilitate the responsible sharing of sensitive information, the Federal-Provincial-Territorial Critical Infrastructure Working Group will lead the development of a coherent approach to information protection among governments. 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 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 critical infrastructure sectors, taking into account the communication protocols and policies already established by the governments. Federal, provincial and territorial governments and critical infrastructure sectors will develop this process to enable timely information exchange to deal with real or potential disruptions that threaten the integrity of critical infrastructure in Canada.

Key action: Federal, provincial and territorial governments will collaborate to develop an information sharing framework. Additional detail is available in Annex D.

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

2.3 Implement all-hazards risk management approach



While partnerships and enhanced information sharing represent the building blocks of the Canadian 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.

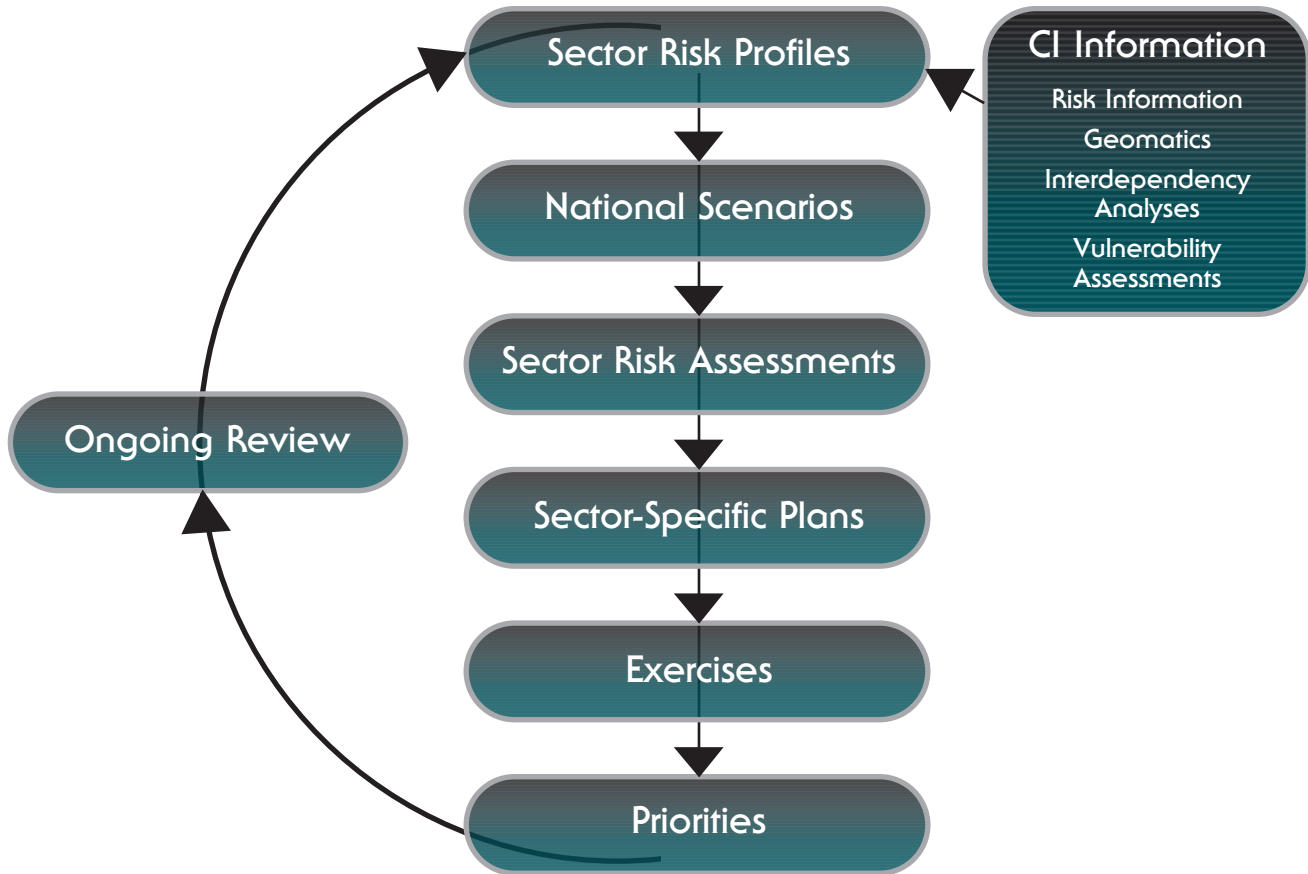
Risk assessments of critical infrastructure in Canada: Sector networks will develop risk profiles in cooperation with governments and the private sector. ***Year 2 and ongoing***

Although the Strategy promotes a common approach to enhancing the resiliency of critical infrastructure, owners and operators and all governments are ultimately responsible for implementing a risk management approach appropriate to their situation. Implementation of a risk management approach to 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 governmental 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, developing 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 to critical infrastructure across all sectors in Canada.



As illustrated in the flow chart above, the sector risk profiles will enable the development of scenarios. 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 would guide 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 governments, 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, tools will be made available to help each sector network identify critical assets within the sector, assess risks from an all hazards perspective, and develop measures to address risks for the sector. These tools are to be developed by the designated federal sector-specific departments and agencies in coordination with relevant government and private-sector representatives. These tools will be used by the Federal-Provincial-Territorial Critical Infrastructure Working Group to evaluate whether any gaps exist in the protection of critical infrastructure on a national level and, if so, to work with the sectors to address them. It is anticipated that the sector-specific plans will continue to evolve as the critical infrastructure, threats against them, and strategies for protecting against and responding to these threats and incidents evolve.

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 plan 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 of the 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 sectors to assess capabilities for responding to disruptions of critical infrastructure. The purpose of these exercises is to clarify the understanding of 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 critical infrastructure sectors 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 critical infrastructure sectors will work together to monitor the implementation of the Strategy and support the assessment of programs and activities of the Strategy targeted at enhancing the resiliency of critical infrastructure in Canada.

The Action Plan will be reviewed, in collaboration with the sector networks, the National Cross-Sector Forum and the Federal-Provincial-Territorial Critical Infrastructure 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 sectoral 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;
- advance a common understanding of risks and interdependencies, and implement 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 ten critical infrastructure sectors. Where appropriate, sub-sector networks may also be established to reflect the diversity of a particular sector. Recognizing that Public Safety Canada is responsible for leading the overall federal effort to strengthen the resiliency of critical infrastructure, the sector-specific federal government departments and agencies are set out in the table below. As required, supporting federal departments will also participate in the sector networks.

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

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), and of relevant federal, provincial and territorial departments and agencies. 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.



Annex B – National Cross-Sector Forum

Purpose

The purpose of the National Cross-Sector Forum is to maintain a comprehensive and collaborative Canadian approach to critical infrastructure by providing a standing mechanism for discussion and information exchange within and between the federal, provincial and territorial governments and the critical infrastructure sectors.

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

- provide advice and recommendations to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management;
- foster a complementary 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 sector-specific plans and exercises;
- facilitate information sharing between federal, provincial and territorial governments, and owners and operators on physical and cyber security.

The National Cross-Sector Forum will provide advice and recommendations to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management, which manages federal, provincial and territorial government collaboration on critical infrastructure matters. In turn, Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management Co-Chairs will report to the Federal-Provincial-Territorial Deputy Ministers responsible for emergency management on critical infrastructure 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. Where potential members fall under a specific jurisdiction (e.g. health care institutions, municipalities, some energy providers), the responsible government will proceed with invitations, as deemed appropriate. 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 National Cross-Sector Forum.

Procedures

- To facilitate the exchange of information, the members will sign a non-disclosure agreement and the National Cross-Sector Forum will adopt information sharing guidelines to protect information from inappropriate disclosure.
- The National Cross-Sector Forum may hold open or closed meetings.
- The National Cross-Sector Forum may invite government or private sector 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 National Cross-Sector 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 National Cross-Sector Forum. Division staff members will also manage the preparation of documents for the meetings and prepare meeting summaries and reports.

Remuneration

The National Cross-Sector 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 in accordance with Treasury Board of Canada guidelines.



Annex C – Federal-Provincial-Territorial Critical Infrastructure Working Group



Purpose

The purpose of the Federal-Provincial-Territorial Critical Infrastructure Working Group is to be the standing forum and primary conduit for federal/provincial/territorial government collaboration on critical infrastructure matters.

Objectives/Priorities

- Support the implementation of the Strategy within federal, provincial and territorial jurisdictions;
- Provide guidance and participate in the evolution and implementation of the Action Plan;
- Act as a clearinghouse for governments on critical infrastructure related issues to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management;
- Facilitate federal/provincial/territorial networking to support critical infrastructure information sharing, risk management, critical infrastructure planning and exercises;
- Identify critical infrastructure issues of regional or jurisdictional concern;
- Advance a common understanding of critical infrastructure risks and interdependencies;
- Encourage participation in exercises to test sector-specific work plans and identify new risks;
- Provide guidance on current and future challenges related to critical infrastructure; 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 is open to all governments for participation in accordance with their needs and as their resources permit. All governments are members of the Federal-Provincial-Territorial Critical Infrastructure Working Group regardless of their presence at meetings; no decision will be made without the sharing of information and the opportunity for all members to comment.

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

The Working Group will be co-chaired by a representative from the Emergency Management and National Security Branch of Public Safety Canada and a provincial/territorial representative determined by group consensus.

Reporting

The Co-Chairs (Public Safety Canada and a provincial/territorial representative) will report to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management on critical infrastructure matters.

Working Group Secretariat

Public Safety Canada will serve as the secretariat for the Federal-Provincial-Territorial Critical Infrastructure Working Group 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 for 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 risks and vulnerabilities, (ii) insufficient sharing of information and (iii) limited integration of existing information into coherent situational awareness.

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. In respect of existing federal, provincial and territorial legislation and policies, three key features of this framework are: 1) the information protection protocol, 2) development of better information products and 3) information dissemination.

1. Information Protection Protocol

As a starting point, an information protection protocol is needed to facilitate sharing of sensitive critical infrastructure information between governments and critical infrastructure 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 that 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 critical infrastructure information may be used

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

- managing response to an emergency;
- establishing policies and programs respecting emergency management and critical infrastructure in both physical and cyber dimensions;
- conducting exercises and providing training related to critical infrastructure;
- 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 critical infrastructure 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 and usefulness of the information products, members of the sector networks will identify areas of emerging concern and identify priority areas for information products. It is expected that these information products will be used by critical infrastructure partners to improve the resiliency of their key assets and services.

The sector networks will advise the National Cross-Sector Forum on areas of emerging concern and identify priority areas for information products. For example, it is expected that the National Cross-Sector Forum will recommend to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management areas that require new or updated information products.

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, quick exchange of information among key points of contact across the critical infrastructure sectors is needed. To accomplish this, connections between federal, provincial and territorial points of contact and with owners and operators under their respective jurisdiction 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 critical infrastructure.

Regular situations

The federal government currently sponsors security clearances for key stakeholders in some critical infrastructure sectors who require access to information related to the resiliency of their critical infrastructure. On an ongoing basis, Public Safety Canada, its portfolio partners and sector-specific federal departments will examine the need to expand the availability of these security clearances for each of the critical infrastructure sectors. In addition, the Federal-Provincial-Territorial Critical Infrastructure Working Group will consider other options for improved information dissemination (e.g., scrubbing sensitive information to allow for regular unclassified distribution).

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

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

Initially, the 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 Strategy approval.

The goal of the second phase is to begin populating the portal with information related to all aspects of critical infrastructure. This second phase will reflect the Strategy’s all-hazards approach and will include adding information products such as physical and cyber threat assessments, 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 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 critical infrastructure stakeholders.

Timeline: *Information sharing framework*

| Action | Lead |
|--|---|
| Year 1 | |
| Establish information sharing protocol | Federal-Provincial-Territorial Critical Infrastructure Working Group |
| Compile inventory of information currently being shared | Special Working Group of the Federal-Provincial-Territorial Critical Infrastructure Working Group |
| Identify information gaps and anticipate new requirements | Special Working Group of the Federal-Provincial-Territorial Critical Infrastructure Working Group |
| Develop statement of requirements for the information sharing portal | Public Safety Canada |
| Year 2 | |
| Establish the Public Layer of the information sharing portal | Public Safety Canada |
| Develop and test secure, web-based user authentication | Public Safety Canada |
| Implement the Secure Layer of the information sharing portal | Public Safety Canada |
| Ongoing | |
| Enhance information dissemination | Federal-Provincial-Territorial partners, sector networks |
| Populate Public and Secure Layers of the information sharing portal | Federal-Provincial-Territorial partners, sector networks |



Annex E – Risk management

Managing risk is a shared responsibility of all critical infrastructure 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 critical infrastructure 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 provided as soon as sector networks are established and new tools will be developed on an ongoing basis. Owner/operator risk assessments, where they exist, should be an ongoing activity.

Sector risk profiles

It is essential that all of the key critical infrastructure 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 risks 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 concern to particular sectors, priorities for research, development of a sector-specific work plan and assessing the effectiveness of critical infrastructure 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.

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 critical infrastructure asset, site or system. These assessments will provide a detailed and specific understanding to each critical infrastructure site owner/operator of their particular risk environment. Though considered an important activity to enhance the resiliency of critical infrastructure, the Strategy does not impose a requirement on owners and operators to undertake risk assessments.

Risk assessments can be used by owners and operators to support the development of sector-specific work plans to address the 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 critical infrastructure partners. There are a number of respected assessment methodologies and the needs and capabilities of each sector and critical infrastructure 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 risks (natural, intentional and accidental);
- an assessment of vulnerabilities;
- an assessment of the impacts of disruptions to critical infrastructure; 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 risk information will be provided to each sector network for distribution to its members. It is expected that most 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 critical infrastructure has been subject to a risk assessment by its owners/operators.

Risk assessments for assets, sites or systems 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 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 owners/operators to support broader risk assessment and emergency planning activities.

Timelines

As the Strategy does not impose a requirement on owners/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, tools, guidelines, methodologies and plans will be made available. Public Safety Canada, with the support of sector networks and of the National Cross-Sector Forum and the Federal-Provincial-Territorial Critical Infrastructure Working Group, will provide these tools.

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.

It is expected that these tools will be distributed through each sector network and via the web-based critical infrastructure information sharing portal (see Annex D).

Timelines

The development and dissemination of risk management tools will be an ongoing process.