Public Safety and Emergency Preparedness Canada
Sécurité publique et Protection civile Canada

Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection

November 2004

Canada

Table of Contents

1. Purpose **3**
2. Background **3**
3. Context **4**
4. Mission Statement **6**
5. Desired Outcomes **6**
6. Key Elements of a National Critical Infrastructure Protection Strategy **6**
6.1 Guiding Principles 6
6.2 Risk Management 7
6.3 Information Sharing 7
6.4 Inventory of Critical Infrastructure Assets 8
6.5 Threats and Warnings 9
6.6 Critical Infrastructure Interdependencies 9
6.7 Governance Mechanisms 10
6.8 Research and Development 11
6.9 International Cooperation 11
7. Next Steps **11**
Appendix A: Summary of Government of Canada Positions **12**
Appendix B: National Critical Infrastructure Sectors **13**
Appendix C: Stakeholder Roles **14**
References **18**

1. Purpose

This paper presents the Government of Canada's position on the development of a comprehensive national approach to critical infrastructure protection (CIP). It is intended to elicit feedback from stakeholder groups and to form the basis of a national strategy for critical infrastructure protection.

2. Background

Deputy Prime Minister Anne McLellan released Canada's first National Security Policy (NSP) in April 2004. Within the NSP, two interrelated initiatives focusing on CIP were announced. First, in order to establish a basis for the CIP challenge to be met by the federal, provincial and territorial governments as well as industry, the Government of Canada will release a position paper establishing the key elements of a proposed national CIP strategy. Second, with cyber security at the forefront of the transborder challenge to Canada's critical infrastructure (CI), the federal government will strengthen its capacity to predict and prevent cyber attacks. A high-level national task force with public and private representation is being established to develop the national cyber security strategy.

In addition to these two initiatives, the federal *Emergency Preparedness Act* is being reviewed to reflect the emerging requirements of emergency management. These requirements include mitigation programs, CIP, cyber security, information sharing between federal departments, agreements with international and private sector partners, and protection of sensitive private sector information.

Development of the CIP and cyber security strategies in addition to a comprehensive, modern legislative foundation are essential to providing national leadership to help reduce vulnerabilities, detect threats and risks more effectively, and improve response and recovery efforts and timing.

Figure 1 depicts the recommended strategic approach for the underlying policy framework for the successful development of a national CIP strategy for Canada.

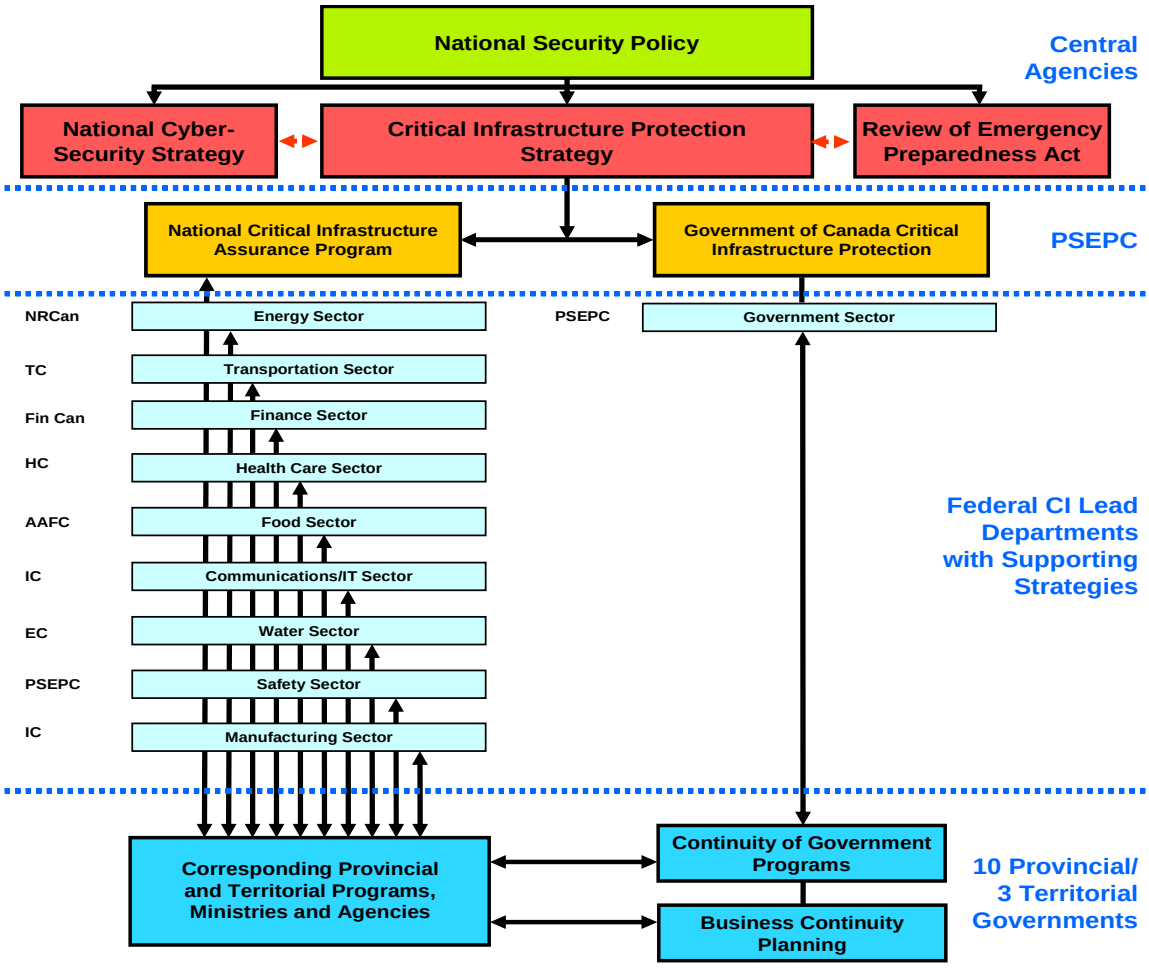

Figure 1 The recommended strategic approach for a national CIP strategy

3. Context

Canada and Canadians rely on infrastructures that are essential to their health, safety, security and economic well-being. These infrastructures are highly connected and highly interdependent. Corporate consolidation, industry rationalization, efficient business practices such as just-in-time manufacturing, and population concentration in urban areas have all contributed to this situation. Perhaps most importantly, over the past decade or so, the nation's critical infrastructures have become more dependent on common information technologies, including the Internet. Failure or disruption of even one infrastructure system can cascade through other systems, causing unexpected and increasingly more serious failures of essential services. Interconnectedness and interdependence also make these infrastructures more vulnerable to disruption or destruction.

At the same time as vulnerabilities are changing and increasing, so too are the threats. The frequency and impact of natural disasters that affect critical infrastructures are increasing. Infrastructures are also vulnerable to changing threat environments that include catastrophic terrorist attacks and destructive computer viruses and worms.

Canadians seek assurance that the country's infrastructures are viable and resilient. Since over 85 percent of Canada's infrastructure is owned and operated by the private sector and the provinces and territories, a national partnership based on a risk management framework is required to provide this assurance.

Canada defines its national critical infrastructure (NCI) as those "physical and information technology facilities, networks, services and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada." Critical infrastructures are found in 10 sectors: Energy and Utilities; Communications and Information Technology; Finance; Health Care; Food; Water; Transportation; Safety; Government; and Manufacturing. These 10 sectors are divided into sub-sectors that are further categorized to reflect and permit a more detailed analysis of the infrastructure. For example, the Energy and Utilities sector is divided into electrical power, natural gas and oil production, and transmission systems. Electrical power, in turn, is further divided into power generation plants, transmission stations, power line corridors (or transmission lines), distribution stations, control centres, and nuclear. (See Appendix B for a list of sample sub-sectors.)

The traditional approach to protecting the national infrastructure has been to identify specific physical assets of national importance and develop plans for their protection. Protection of assets, however, is just one of the strategies available to CI owners and operators to prevent the threat to, and reduce vulnerabilities of specific assets, thereby contributing to assurance.[1] Owing to the diverse nature of Canadian infrastructures, risk management actions must be undertaken with consideration for the continued operation of infrastructures across sectors, rather than individual facilities. Consequently, the Government of Canada focuses its efforts both on improving ways to provide protection where it is reasonable, and also on ways to assure the continued provision of essential services to Canadians. Protection and assurance can be achieved through better information collection, assessment and sharing, and through risk management. Both protection and assurance are ongoing objectives that the Government of Canada seeks to meet by building trusted partnerships.

The former Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), now Public Safety and Emergency Preparedness Canada (PSEPC), published a Discussion Paper in November 2002 to stimulate dialogue with stakeholders on concepts and issues surrounding the development of the National Critical Infrastructure Assurance Program (NCIAP). The provinces and territories, other federal departments, and industry associations shared their views on shaping the program and presented information about their existing CI programs and plans. NCIAP activities to date have focused on bringing organizations with a stake in national CI together, with the goal of building a national CIP strategy, partnerships, and methods of information exchange.

The national CIP strategy will be developed using the knowledge acquired during the development work on the NCIAP, and the stakeholder feedback obtained during consultations. This knowledge and shared understanding will serve as the focal point for national coordination, leading to the creation of a national CIP strategy. Within the federal government, PSEPC and the Treasury Board Secretariat (TBS) are collaborating on a joint project to identify, prioritize and work with other federal departments to protect the Government of Canada's CI.

[1] Other strategies include redundancy and back-up, distribution of operations, multiple sources of supply, mutual aid arrangements, early warning, rapid response, etc.

4. Mission Statement

To create an integrated and forward-looking National Critical Infrastructure Protection Strategy that will include voluntary participation from industry stakeholders as well as from federal, provincial and territorial governments by the fall of 2005.

5. Desired Outcomes

The ultimate outcome of the CIP strategy will be that CI is sufficiently resilient, thereby assuring the continued availability of essential services to Canadians. In the medium term, the CIP strategy will strive to achieve the following outcomes:

- CI sector owners and operators are aware of, accept and take action on the accountabilities, risks and vulnerabilities to their CI;
- The Government of Canada has an ongoing program to assure its physical and cyber infrastructures and thereby demonstrates leadership to other sectors; and
- New knowledge and tools for CIP are developed and shared.

6. Key Elements of a National Critical Infrastructure Protection Strategy

The following section outlines the key elements of a national CIP strategy. The elements include the desired outcomes of the national strategy as well as the processes that are necessary to achieve them.

6.1 Guiding Principles

- **Awareness:** The first step toward taking specific action is to raise awareness of CIP among senior managers in industry and all levels of government by presenting a compelling business case for corporate action (i.e., that industry has a fiduciary responsibility to mitigate risk for the benefit of corporate stakeholders, clients and the general public from both an economic and public safety perspective).

- **Integration:** CI assurance can be achieved by integrating physical and cyber security issues into emergency management programs, and encouraging the integration of CIP at the corporate level with good business practices (such as business continuity planning).

- **Participation:** Success of CI assurance will only be achieved through broad participation of industry stakeholders and federal, provincial and territorial governments. A national strategy must complement and build on current CIP activities and relationships, both those that are established as well as those that are in the formative stages. While the national strategy will focus on initiatives within Canada, it must also recognize cross-border and international activities.

- **Accountability:** CI partners are jointly accountable to Canadians (through legislation, regulation, policy, and due diligence) for safeguarding their own CI assets and ensuring the continued viability of their services.

- **All-hazards approach:** Canada's CI could be disrupted or destroyed as a result of deliberate attack, natural disaster, accident, computer virus or malfunction. CIP must be approached from an all-hazards perspective.

The Government of Canada position is that these five guiding principles will influence the development of the national CIP strategy.

6.2 Risk Management

The assurance actions of CI partners and the priorities of those actions are based on risk management principles that employ common criteria where appropriate.[2] CI partners should use a consistent set of criteria to identify and rank their CI and to determine the relative level of risk. The relative criticality and priority of CI assets are identified by assessing the *impac*t of their loss on the operation of the sector and other sectors, and the *consequence* of their loss. Owners and operators make decisions about safeguarding and assuring their own CI assets. Governments use established risk management approaches to fulfil their responsibilities for CI assurance to Canadians.

Components of a risk management framework for CIP include the following:

- Understanding and creating awareness of CI, and its interdependencies;
- Assuring CI through threat and vulnerability assessments, mitigation and preparation, and research and development; and
- Managing response and recovery through facilitating cross-sector coordination, response planning, and education.

The Government of Canada position is to use the integrated risk management (IRM) framework as a starting point when developing the national CIP strategy.

6.3 Information Sharing

Because Canada's CI is owned or operated by thousands of different organizations – both public and private – it is essential that the conditions for effective information sharing exist. Such conditions must exist not only among organizations, but within a national coordinating body at the federal level.

Stakeholders must have relevant information in order to fulfill their CI assurance role. Specifically:

- CI owners and operators should possess information about the critical infrastructures of others on which they depend, and the threats to their own infrastructures to carry out their business continuity activities;
- Emergency managers and first responders should possess sufficient CI information to plan and carry out their emergency management roles; and
- Public authorities with protection responsibilities should possess information about those critical infrastructures within their jurisdictions that must be protected.

[2] A common approach to identifying and prioritizing CI is proposed in *Selection Criteria to Identify and Rank Critical Infrastructure Assets,* January 2004. See http://www.ocipep.gc.ca/critical/nciap/nci_criteria_e.asp. A risk management framework such as that tabled by the Treasury Board of Canada Secretariat provides an organization with a mechanism to develop an overall approach to manage strategic risk by creating the means to discuss, compare, and evaluate substantially different risks. See http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

The more information available to organizations about potential threats and vulnerabilities, the better able they will be to understand the risk and assure the continuity of essential services. Information that should be shared includes information about threats, vulnerabilities, incidents, protection and mitigation measures, and best practices. Information sharing can be viewed as a means by which to better manage risk and, in turn, help deter, prevent, mitigate, and respond to threats.

It is recognized that information sharing needs to take place in an environment of trust and confidentiality. Existing fora and mechanisms should be used for information exchange as far as possible. New governance mechanisms, information integration centres and modernizing legislation – in particular the *Emergency Preparedness Act* – will be studied.

The Government of Canada position is to promote and support timely and accurate information sharing across jurisdictions and CI sectors. This will require establishing working groups with participants at all levels and conducting stakeholder consultations, including with international partners, to determine: the nature of the information required; the most appropriate vehicles to exchange the information; and to increase interoperability.

6.4 Inventory of Critical Infrastructure Assets

In order to take the required actions to protect CI and assure its reliability, the critical components in each sector must be identified. By identifying and prioritizing CI components, governments, and owners and operators can better allocate resources to the most vulnerable and high-risk areas, develop and exercise plans, improve response capacity, and apply mitigative and preventative measures.

Identifying specific infrastructure components as critical also creates its own set of challenges. For instance, such information can be an attractive target to malicious actors. Therefore, information related to critical infrastructure must be protected for reasons of national security and public safety, in addition to competitive and economic interests.

The Government of Canada will use all of its available legislative and statutory instruments to appropriately protect CI information.

The Government of Canada position is that it will identify and assess its own CI. In addition, the Government of Canada will work with other levels of government and the private sector to ensure that processes are in place to identify their critical infrastructures (or components thereof) as a measure to strengthen public safety and as part of good business practices, and that all associated information be protected to the fullest extent of the law.

6.5 Threats and Warnings

CI stakeholders require clear and timely warning of threats to CI in order to implement risk management strategies.

The National Security Policy outlined the requirement of the Government of Canada to provide greater security for Canadians by building a fully integrated security system that will ensure a more effective response to existing threats and quickly adapt to new ones. This system will be fully connected to key partners – provinces, territories, communities, first line responders, the private sector and Canadians.

The system begins with a comprehensive assessment of threats to Canada. The threat assessment is used to trigger a proportionate and integrated response to prevent or mitigate the effects of the threat. When an event occurs, an integrated system for managing its consequences is triggered.

The Government of Canada created the Integrated Threat Assessment Centre (ITAC) to facilitate the integration of intelligence into a comprehensive threat assessment, which will be made available to those who require it. The integrated approach that the Government is taking ensures that information will be provided in a timely fashion to those who need it.

To provide more comprehensive threat assessments and warnings to CI stakeholders, this process will require information from CI stakeholders, including information on threats, vulnerabilities, incidents, protection and mitigation measures, and best practices.

The Government of Canada position is to continue to improve mechanisms to quickly and effectively communicate relevant information and intelligence on threats to CI to stakeholders.

6.6 Critical Infrastructure Interdependencies

Each infrastructure is a complex and sophisticated system in its own right, but more complex still are the various interconnections and interdependencies amongst these infrastructures, and between them and society. Interdependencies leave infrastructures vulnerable to disruption or events in others sectors, causing hard-to-predict cascading effects that can intensify the impacts of specific failures and the consequences to society. Compounding this interdependence is the increasing reliance on information technologies.

The August 2003 blackout provided an object lesson in infrastructure interdependencies by demonstrating how a disruption in one infrastructure can cascade across others. This was the largest blackout ever in North America, leaving 50 million people from New York to Toronto without power for up to two days. Ontario's public health infrastructure was stressed due to hospitals operating on emergency generators. Food and water supplies were put at risk. Grocery stores were forced to discard thousands of dollars worth of food and water treatment plants operated on emergency power. Thousands of Ontarians felt a cash crunch due to closed banks and disabled bank and debit machines. Transportation and commuting were disrupted when gas stations were unable to pump gasoline (pumps require electricity to be able to operate). Flights were cancelled at both international airports in Ontario (Toronto and Ottawa). An extraordinary volume of calls created tremendous backlogs on 911 systems, and cellular transmitter stations failed when their battery back-up power was exhausted.

In the past, initiatives to protect CI have been sector- or industry-specific, pursued by companies, sector associations, or government departments acting largely independently. This approach has not explicitly addressed cross-infrastructure concerns. A holistic systems-based approach is needed to properly address the issue of interdependencies.

The Government of Canada position is that interdependency analysis must be integrated into risk management decisions, mitigation and preparation strategies, and response and recovery activities. In addition, the Government of Canada will coordinate national efforts in interdependency research and development, which is essential to understanding this issue.

6.7 Governance Mechanisms

A study of CIP governance models in other countries reveals the importance of establishing formalized partnerships among CI owners, operators and governments to provide national direction and coordination of CIP.[3] To this end, the Government of Canada proposes to work with each sector in order to develop appropriate mechanisms for governance where required. It recognizes that suitable mechanisms may already exist within certain sectors, while others will have to be developed, taking into account existing legislative and regulatory environments. These governance mechanisms are to be inclusive in nature and will recognize the regional dimension of CI, thus allowing government and the private sector to maximize coordination and integration of efforts.

Horizontal issues such as interdependency analysis, information sharing and cyber security impact all sectors. These horizontal issues may require separate governance mechanisms, such as the cyber security task force proposed in the NSP.

Implementation of a national CIP strategy comprises a continuum of activities. It includes a national-level capacity to guide and integrate the efforts of national and international governing structures with those of private industry and the provincial and territorial governments. The provinces and territories, with the collaboration of federal departments in the regions, will guide and integrate the interests of private industry within the jurisdictions of the province and territories; particularly during declared provincial and territorial emergencies.

The Government of Canada proposes to establish a national body, such as a national advisory council on CIP, composed of representatives from all levels of government and industry sectors. Such a body would evolve from sector-level governance mechanisms and the collaborative efforts of government and industry in regional CIP structures. One of the most important tasks of such a body would be to raise awareness of CIP issues through contacts with senior-level industry and government representatives, and to provide support for horizontal coordination and management of international, national, and regional CIP initiatives.

[3] For a discussion of governance options see Edlund & Associates*, Establishment of a National Advisory Council on Critical Infrastructure Protection (CIP)*, prepared for Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, July 14, 2003 and The Zeta Group, *NCIAP Governance Paper*, prepared for Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, March 2003.

The Government of Canada position is to establish a governance architecture that will result in national direction and coordination of CIP activities. To this end, it will establish a CIP national body, and where appropriate mechanisms within sectors and to address horizontal and regional issues.

6.8 Research and Development

Through outreach, coordination, and promotion activities Canada must continue the work to leverage the considerable expertise and innovation in its research communities. These communities are contributing both new knowledge and new technologies to CIP and cyber security efforts.

The Government of Canada position is to conduct targeted research projects and leverage Canadian and international science and technology capabilities in order to address gaps in knowledge, build national capacity and to create innovative solutions for CIP.

6.9 International Cooperation

Governments around the world are engaged in the challenge of protecting CI. There is the opportunity to learn from and participate with other countries on CIP issues and initiatives. This is particularly true for the United States with whom Canada shares critical cross-border infrastructure.

The Government of Canada position is to participate in international CIP initiatives and to strengthen information-sharing mechanisms and operational linkages with other countries and international organizations.

7. Next Steps

Overall, Canada's national critical infrastructure protection strategy will:

- Recognize the important steps underway or already taken to assure CI;
- Present and establish priorities and timelines for initiatives that will be undertaken by governments and the private sector, individually and in partnership;
- Outline the principles and objectives of protection and assurance initiatives; and
- Provide direction to the CI partners and propose roles and responsibilities as well as governance mechanisms to foster trust and build the partnership.

The next step for the Government of Canada is to consult with senior provincial and territorial government leaders, industry representatives, and key international partners on development and implementation of an integrated and forward-looking National Critical Infrastructure Protection Strategy that will include voluntary participation from industry stakeholders as well as from federal, provincial and territorial governments by the fall of 2005.

Appendix A:
Summary of Government of Canada Positions

1. **Guiding Principles:** five guiding principles (awareness, integration, participation, accountability, and all-hazards) will influence the development of the national CIP strategy.

2. **Risk Management:** use the integrated risk management (IRM) framework as a starting point when developing the national CIP strategy.

3. **Information Sharing:** promote and support timely and accurate information sharing across jurisdictions and CI sectors. This will require establishing working groups with participants at all levels and conducting stakeholder consultations, including with international partners, to determine: the nature of the information required; the most appropriate vehicles to exchange the information; and to increase interoperability.

4. **Inventory of CI Assets:** identify and assess its own CI. In addition, the Government of Canada will work with other levels of government and the private sector to ensure that processes are in place to identify their critical infrastructures (or components thereof) as a measure to strengthen public safety and as part of good business practices, and that all associated information be protected to the fullest extent of the law.

5. **Threats and Warnings:** continue to improve mechanisms to quickly and effectively communicate relevant information and intelligence on threats to CI to stakeholders.

6. **CI Interdependencies:** interdependency analysis must be integrated into risk management decisions, mitigation and preparation strategies, and response and recovery activities. In addition, the Government of Canada will coordinate national efforts in interdependency research and development, which is essential to understanding this issue.

7. **Governance Mechanisms:** establish a governance architecture that will result in national direction and coordination of CIP activities. To this end, the Government of Canada will establish a CIP national body, and where appropriate mechanisms within sectors and to address horizontal and regional issues.

8. **Research and Development:** conduct targeted research projects and leverage Canadian and international science and technology capabilities in order to address gaps in knowledge, build national capacity, and to create innovative solutions for CIP.

9. **International Cooperation:** participate in international CIP initiatives and to strengthen information-sharing mechanisms and operational linkages with other countries and international organizations.

Appendix B:
National Critical Infrastructure Sectors

PSEPC has identified 10 sectors that form the basis of the NCIAP. The table below lists these sectors and provides sample sub-sectors for each sector.

Sector		Sample Sub-Sectors
1.	Energy and Utilities	Electrical power (generation, transmission, nuclear) Natural gas Oil production and transmission systems
2.	Communications and Information Technology	Telecommunications (phone, fax, cable, satellites) Broadcasting systems Software Hardware Networks (internet)
3.	Finance	Banking Securities Payments System
4.	Health Care	Hospitals Health-care facilities Blood-supply facilities Laboratories Pharmaceuticals
5.	Food	Food safety Agriculture and food industry Food distribution
6.	Water	Drinking water Wastewater management
7.	Transportation	Air Rail Marine Surface
8.	Safety	Chemical, biological, radiological, and nuclear safety Hazardous materials Search and rescue Emergency services (police, fire, ambulance and others) Dams[4]
9.	Government	Government facilities Government services (for example meteorological services) Government information networks Government assets Key national symbols (cultural institutions and national sites and monuments)
10.	Manufacturing	Chemical industry Defence industrial base

[4] Dams can be critical to a number of sectors (Water, Transportation, and Energy and Utilities) depending on their purpose. While different sectors need to assure continuation of the services dams provide, a crosscutting concern is dam safety. Recognizing the interdependency between the service dams provide and dam safety, the services should be incorporated in the appropriate sectors; however, the safety of dams should be dealt with in the Safety sector.

Appendix C: Stakeholder Roles

Canadian federal and provincial/territorial governments and Canadian industry are CI partners. The following table lists the roles of these partners and of Canadians.

Stakeholder	Roles
All Partners	• Develop, lead, and manage risk management strategies and programs • Develop and lead awareness, training and education programs • Develop multi-jurisdictional partnerships and share information • Collaborate on exercises and R&D efforts • Develop and share best practices and lessons learned
Federal and Provincial/ Territorial Governments	• Provide leadership and guidance (e.g., analyzing interdependencies, developing tools, assessing and reporting on progress, and addressing issues) • Establish CI assurance/protection programs for government services within their jurisdiction • Participate with industry owners/operators in CI assurance programs within sectors (including where the government is also an owner/operator) • Share threat, vulnerability, and other relevant information on subjects where government has unique information or access to information, subject to applicable laws and policies • Issue guidelines and direction within government regulated sectors • Develop and implement regulations and standards • Develop public alerting initiatives
Owners/Operators[5]	• Strengthen partnerships among owners/operators and with governments • Participate in sector- or sub-sector-wide risk management and CI assurance/protection programs • Share threat and vulnerability information on subjects where the owner/operator has unique information or access to information
Citizens	• Become aware of CI issues • Take basic steps toward actions to secure infrastructures such as IT (i.e., safe computing) • Take precautions for temporary disruption of critical products and services

[5] Including federal, provincial, and municipal governments in their role as owner/operator.

Government of Canada's Responsibilities

The Government of Canada has a unique role to play in raising awareness and leadership at the national level, and international collaboration (e.g., U.S. Department of Homeland Security, NATO, and G8). In addition, the Government of Canada will protect its own CI, support provincial/territorial programs and provide consistent, consolidated threat and vulnerability information nationally. The federal government's sector lead departments and agencies represent the federal government in sector CI assurance/protection initiatives and carry out other roles in CI assurance, including:

- Encouraging collaboration among partners,
- Supporting and contributing to NCI assurance initiatives, and
- Enabling information sharing with interdependent sectors and all levels of government.

The following table lists the Government of Canada's sector lead departments and agencies.

Sector		Department/Agency
1.	Energy and Utilities	**Natural Resources Canada (NRCan)** Supported by: Canadian Nuclear Safety Commission (CNSC), International Joint Commission (IJC), National Energy Board (NEB)
2.	Communications and Information Technology	**Industry Canada (IC)** Supported by: Public Safety and Emergency Preparedness (PSEPC)
3.	Finance	**Finance Canada**
4.	Health Care	**Health Canada (HC)**
5.	Food	**Agriculture and Agri-Food Canada (AAFC)** Supported by: Canadian Food Inspection Agency (CFIA), Canada Border Services Agency (CBSA), Health Canada
6.	Water	**Environment Canada (EC)** Supported by: Health Canada
7.	Transportation	**Transport Canada (TC)** Supported by: CBSA
8.	Safety	**Public Safety and Emergency Preparedness (PSEPC)** Supported by: Health Canada / National Defence (DND)
9.	Government	**Public Safety and Emergency Preparedness (PSEPC) and Treasury Board Secretariat (TBS)** [6]
10.	Manufacturing	**Industry Canada** Supported by: National Defence, Natural Resources Canada, Environment Canada

[6] PSEPC and the Treasury Board Secretariat collaborate on a joint project to identify, prioritize, and work with federal departments to protect the Government of Canada CI, centrally and regionally.

The following table lists the CIP functional responsibilities of the federal government.

Functional Responsibilities		**Department/Agency**
1.	NCIAP Leadership	PSEPC will provide the focal point for the integration of CIP activities, strategic coordination, and national-level policy development and integration.
2.	Information Sharing (Threat and Vulnerability Information / Integrated Threat Assessment Centre – Security and Intelligence Information / Alerts and Warnings Systems)	PSEPC will act as the focal point for coordinating, analyzing, and sharing threat and vulnerability information (cyber and physical). Other departments: AAFC, CBSA, CFIA, CSIS, CSE, DFAIT, DND, EC, Finance, HC, NRCan, PCO, RCMP, TC (other departments/agencies to be determined)
3.	Cyber Security (Information technology based networks and services)	CSE, CSIS, IC, PSEPC, RCMP
4.	Cyber Incident Management	CSIS – National Security Incidents RCMP – Criminal Incidents PSEPC, CSE – Other
5.	Physical Security	DND – Military RCMP – Civilian (other departments/agencies to be determined)
6.	Government of Canada: CIP and Cyber Security Strategies	CSE, CSIS, PSEPC, PWGSC, RCMP, TBS
7.	Research and Development	CSE, DRDC, IC, NRC, PSEPC, RCMP (other departments/agencies to be determined)
8.	U.S./International CIP and Cyber Security Coordination	CBSA, CSE, DFAIT, DND, PCO, PSEPC, RCMP

PSEPC's Responsibilities

PSEPC is the lead federal department for CIP. As such, PSEPC will collaborate with TBS in a joint project to identify, prioritize and work with federal departments to protect the Government of Canada CI, centrally and regionally. In addition, PSEPC provides CI-specific analysis, and acts as a conduit from the security and intelligence (S&I) community to its CI and emergency management partners.

The following lists the responsibilities of PSEPC at both headquarters and the regional office level.

PSEPC	Roles
Headquarters	• Development of the national CIP strategy • Development of the NCIAP • Coordination of the NCIAP (of lead federal departments/agencies, provinces/territories, sector associations, and international partnerships) • Implementation of the NCIAP (i.e., training and education, threat and vulnerability information, research and development, etc.) • Sustaining the NCIAP as a viable ongoing program after implementation • Strategic risk analysis and management
Regional Offices	• Support and coordination to provinces/territories • Coordination of federal departments in the regions • Represent Government of Canada in regional Canada/U.S. fora • Coordinate Government of Canada CIP through federal councils

References

Awareness, Training and Education for Critical Infrastructure Protection, Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, June 2003.

Discussion Paper on Information Sharing Policy Options, Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, February 2003.

Edlund & Associates*, Establishment of a National Advisory Council on Critical Infrastructure Protection (CIP)*, Prepared for Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, July 14, 2003. Unpublished Study

Guide to the Access to Information Act (ATIA), Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, December 2002.

Information Sharing Policy Framework, Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, December 2002.

National Critical Infrastructure Assurance Program (NCIAP) Discussion Paper, Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, November 2002. http://www.ocipep.gc.ca/critical/nciap/disc_e.asp

National Critical Infrastructure Assurance Program (NCIAP) Synopsis, Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, November 2002. http://www.ocipep.gc.ca/critical/nciap/synopsis_e.asp

National Critical Infrastructure Assurance Program (NCIAP) Update Reports, Public Safety and Emergency Preparedness Canada, Ottawa, Ontario, 2003–2004. http://www.ocipep.gc.ca/critical/nciap/update_e.asp

National Critical Infrastructure Protection Project (NCIPP) Concept Paper, Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, February 27, 2002.

PSEPC website: http://www.psepc.gc.ca/index.asp

An Assessment of Canada's National Critical Infrastructure Sectors, Prepared for Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, July 2003. http://www.ocipep.gc.ca/critical/nciap/nci_sector1_e.asp

The Zeta Group, *NCIAP Governance Paper*, Prepared for Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, March 2003. Unpublished Study.

Securing an Open Society: Canada's National Security Policy, Privy Council Office, Ottawa, Ontario, Canada, April 2004.
http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf

Selection Criteria to Identify and Rank Critical Infrastructure Assets, Public Safety and Emergency Preparedness Canada, Ottawa, Ontario. January 2004.
http://www.ocipep.gc.ca/critical/nciap/nci_criteria_e.asp

Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets, Prepared for Office of Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Ontario, December 19, 2002.

Government Security Policy, Treasury Board Secretariat, Ottawa, Ontario, February 2002. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

Integrated Risk Management Framework, Treasury Board Secretariat, Ottawa, Ontario, March 2000. http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp