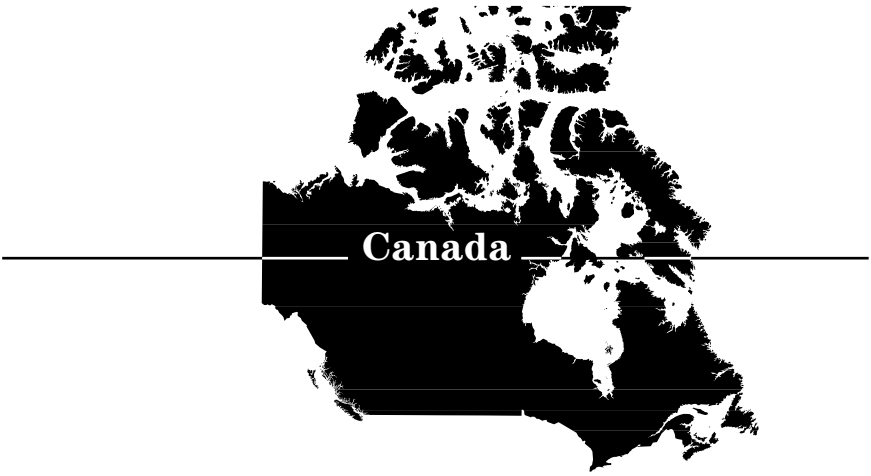
CIIP Country Surveys



The Country Survey of Canada 2004 was mainly written by Shannon Hiegel, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), Canada. In addition, Louise Forgues, Colin Knight, and Paul Pagotto from OCIPEP as well as Dan Lambert, Solicitor General Canada, provided valuable input.

Canada

Critical Sectors

In Canada, CI is made up of clearly identified components that come together under the heading of National Critical Infrastructures (NCI). "Canada's critical infrastructure consists of those physical and information technology facilities, networks 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."[106]

Canada's NCI is grouped into ten sectors with sub-sectors. The identification of these sectors was a dynamic process of dialog involving domestic stakeholders and the exchange of information on the international scene. The sectors are the following:[107]

- Communications and Information Technology (Telecommunications, Software, Hardware, Networks (Internet)),
- Energy and Utilities (Electrical Power, Natural Gas, Oil Production and Transmission Systems),
- Finance (Banking, Securities, Investment),
- Food (Food Safety, Agriculture and Food Industry, Food Distribution),
- Government (Government Facilities, Government Services (e.g., Meteorological Services), Key National Symbols (Cultural Institutions and National Sites and Monuments),
- Health Care (Hospitals, Laboratories, Pharmaceuticals),
- Manufacturing (Chemical Industry and Defense Production, Defense Industrial Base),
- Safety (Chemical, Biological, Radiological, and Nuclear Safety; Hazardous Materials; Emergency Services (Police, Fire, Ambulance, and others)),
- Transportation (Air, Rail, Marine, Surface),
- Water (Drinking Water, Wastewater Management).

106 http://www.ocipep.gc.ca/critical/index_e.asp.

107 J.E. Harlick (OCIPEP): Understanding Critical Infrastructure Protection. *Presentation at the PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century'*, Stockholm, 17–18 November 2003.

Initiatives and Policy

Canadian cyber-protection activities focus on awareness and the resilience of information technology systems and assets. This includes components such as telecommunications, computers and software, the Internet, and satellites, as well as interconnected computers and networks and the services they provide.

Policies and programs (such as the *National Critical Infrastructure Assurance Program*, NCIAP) are in place or under development to ensure that Canada is prepared for attacks and has the ability to recover key services as quickly as possible. The government of Canada wants to be in a position to identify threats to vulnerabilities in advance and to disruptions as they happen, allowing it to quickly issue warnings and provide guidance to owners and operators of critical infrastructures.

To provide credible national leadership, the government of Canada must first ensure an adequate level of protection for its own portion of the national critical infrastructure (in the physical realm and in cyberspace). This means having emergency plans, contingency plans, and business continuity plans for government systems, processes, and assets. The Government Security Policy prescribes the application of safeguards (physical and virtual) for federal departments and agencies.

Government-on-Line (GoL)

The government plans to implement a technology and policy framework that protects the security and privacy of Canadians in their electronic dealings with their government. This is part of the *Government-on-Line* (GoL)[108] policy. Canadians will be able to transmit applications and financial transactions securely on-line and in real-time. GoL must address the principal security requirements for electronic transactions (data integrity, data confidentiality, availability, authentication, and non-repudiation).

The secure channel is a major component of the technology infrastructure that will allow citizens to access federal services over the Internet reliably and securely, and is a key part of the government's plan to get government programs and services on-line by 2005.

108 http://www.gol-ged.gc.ca/index_e.asp.

Information Technology Systems Research and Development

Several federal government agencies have research and development expertise in the area of information infrastructure protection. These include the *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP), *Defence Research and Development Canada*, the *Communications Security Establishment*, and *Industry Canada's Communications Research Centre*. These agencies have formed a joint working group to collaborate on information infrastructure research projects and to develop a joint long-term research agenda.

This initiative has led to a more efficient allocation of research funding, better sharing of expertise and awareness of research trends, and an improved understanding of the research capabilities and gaps within the government of Canada. This extensive initiative is expected to expand to include other Canadian government departments, as well as to develop international linkages to other research councils.

National Critical Infrastructure Assurance Program (NCIAP)

The events of 11 September 2001 have accelerated the implementation of the *National Critical Infrastructure Assurance Program* (NCIAP) [109]. The Canadian government is working on this program together with the provinces, territories, and the private sector.

The overall aim is to promote a more resilient and viable national critical infrastructure through partnership between governments and the private sector. Such partnership will enable two-way information exchange and more directed research and development. It will also develop the means to better assess risks, vulnerabilities, threats, and interdependencies that can affect the continuity of the NCI.

The NCIAP is currently a framework for cooperative action. The short-term goal is to bring together organizations with a stake in better assuring CI/CII, so that an approach can be jointly developed and the exact nature of the partnership and methods of information exchange can be designed. The NCIAP will evolve with the emergence of new needs and the changing risk environment. Through consultation and planning, the NCIAP will evolve from its current framework status to a fully operational program with a powerful yet flexible charter.

109 http://www.ocipep.gc.ca/info_pro/fact_sheets/general/CIP_NCIAP_e.asp.

All stakeholders can participate in and benefit from an array of products, multi-jurisdictional partnerships for information and sharing best practices, R&D efforts, training and awareness programs, and sectoral, regional, and national-international exercises.[110]

Readiness and Response Review

The *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP) is coordinating the development of frameworks to help improve the readiness and response capability associated with emergency management (physical and virtual) both for the government of Canada as well as on a national basis, the latter to be a collaborative effort with major stakeholders and partners. This initiative is intended, when implemented, to provide more effective governance arrangements, to increase the coordination between the variety of initiatives and programs which constitute the substance of readiness and response, and to provide more effective management tools to maintain and adapt a readiness and response capability. Proposals to implement new arrangements are anticipated at the end of 2003.[111]

Information-Sharing

Information-sharing is arguably one of the most significant issues in CIIP. Canada has been working intensely to identify better ways to achieve this goal. Information-sharing can be viewed as a means to manage actions that can help deter, prevent, mitigate, and respond to the impact of a threat, as well as a tool to manage risk.

Canada is looking at the possibility of creating an information-sharing framework. This structure would provide a clear structure for the process of establishing information-sharing relationships, bridging silo-style structures, and encouraging consistent approaches among participants, while ensuring that such processes are workable for and relevant to all key stakeholders.

There is value in having centers for sharing and analysis of sensitive information about vulnerabilities, threats, intrusions, and anomalies within specific CI sectors. Government action alone cannot assure the protection

110 http://www.ocipep.gc.ca/critical/nciap/synopsis_e.asp.
111 http://www.ocipep.gc.ca/home/index_e.asp.

of vital services provided by CI in the current threat environment. The concept of information-sharing centers is important and Canada is considering with its partners whether and how such information-sharing mechanisms could be developed.

Organizational Overview

Public Agencies

In Canada, the lead agency dealing with CIP/CIIP is the *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP).

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

Recognizing Canada's increased interdependencies and vulnerabilities in Critical Infrastructure, the prime minister of Canada announced in February 2001 the creation of the *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP)[112]. The decision to combine critical infrastructure protection and emergency preparedness responsibilities in one organization reflected the new risk environment, in which physical and cyber dimensions of infrastructures are increasingly interconnected. Combining critical infrastructure protection and emergency management resources and policy tools with acquired knowledge and experience in emergency preparedness should ensure a stronger, more integrated, and effective national security posture. Critical infrastructure protection and emergency management are not seen as separate endeavors, but as part of the assurance and protection continuum.

In December 2003, the Prime Minister has announced that OCIPEP (so far in the Department of National Defense) will be integrated into a new portfolio, *Public Safety and Emergency Preparedness*, in order to maximize emergency preparedness and response to natural disaster and security emergencies.[113] OCIPEP collaborates closely with federal actors in the areas of law enforcement (the *Royal Canadian Mounted Police* (RCMP)), the national security and intelligence service (the *Canadian Security Intelligence Service* (CSIS)), and sector departments (e.g., *Industry Canada* as the lead for relations with the telecommunications sector), as well as other

112 http://www.ocipep.gc.ca/home/index_e.asp.
113 http://www.ocipep.gc.ca/home/index_e.asp.

departments and agencies (e.g., the *Treasury Board Secretariat* and the *Communications Security Establishment* (CSE)). Through partnership-building, the government of Canada also works together with the private sector and provincial/territorial governments focusing on developing a seamless, well-coordinated approach to CIIP.

Interdepartmental Committee

The government of Canada has also instituted an interdepartmental committee of senior officials to discuss strategic policies and issues related to its cybersecurity posture. This committee provides guidance on dealing with incidents that could have a serious widespread impact, where the potential impact is unknown, where it may impact on several critical infrastructure sectors, when response and mitigation steps are not obvious, or when the incident has potential national or international consequences.

Public Private Partnerships

The Canadian private sector, which owns and operates most of the nation's infrastructure, plays a key role in securing cyberspace. National sector associations such as the *Canadian Electricity Association* (CEA), the *Canadian Bankers Association* (CBA), the *Canadian Telecommunications Emergency Preparedness Association* (CTEPA), and others have been active in promoting enhanced CIP efforts. Currently, Canada's CI sectors are working to enhance information-sharing among their members, with government, and between sectors.

It is increasingly recognized that information on threats, vulnerabilities, corrective measures, and best practices should be shared widely, across sectors and with governments. Canadian industry and governments at all levels are working together to improve information-sharing and analysis efforts. Industry sectors have identified a variety of challenges, including such issues as timeliness and relevancy of threat information. As industry efforts to increase mutual cooperation and information-sharing mature, so too will the national ability to respond to and manage cyber incidents and attacks.

Early Warning Approaches

Integrated Government of Canada Response System

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), in partnership with law-enforcement and national security agencies, is developing a new response and co-ordination structure for cyber-incidents, which includes the monitoring of cyber-threats 24 hours a day and 7 days per week, serving as one of several points of contact for threat and incident information.

If a cyber-incident is suspected of constituting a criminal offence or involves threats to national security, the federal police (*Royal Canadian Mounted Police* (RCMP)) or federal intelligence service (*Canadian Security Intelligence Service*, CSIS) are contacted directly. Recognizing that it may be difficult for a reporting party to determine whether an incident has criminal or national-security implications, such cases could be reported to the *Government Emergency Operations Co-ordination Center*, where the *Cyber Incident Coordination System* (CICS) *Cyber Triage Unit* would examine it. This unit is composed of officials from OCIPEP, the RCMP, and CSIS who will assess the incident to determine appropriate lead and follow-on action.

The *Cyber Incident Coordination System* provides a comprehensive, coordinated, and integrated system of response to cyber-incidents and vulnerabilities. It has several advantages, including:

- The ability to draw on specific and specialized information technology expertise and resources in several departments and agencies;
- the ability to respond rapidly to an incident and quickly disseminate critical information to stakeholders to reduce the risk of incidents being replicated elsewhere in the government, provinces/territories, the private sector, and other countries;
- the ability to assist provinces, territories, municipalities, the private sector, and international partners in protecting their information systems; and
- the ability to build upon the strong partnerships and expertise that departments and agencies have developed over the years in their respective fields with Canadian and international partners.

Internationally, Canada participates in global watch and warning activities. Discussions are underway between Canada and its international partners to share information in real-time and to detect and prevent cyber-incidents as they emerge.

Timely Alerts and Advisories

Responsible agencies within the government of Canada disseminate alerts, advisories, and other reports pertaining to relevant information technology threats, vulnerabilities, and remedies. There are several channels through which the government of Canada issues alerts and advisories in relation to its information infrastructure. One of the public channels is through the OCIPEP website.[114]

114 http://www.ocipep.gc.ca/opsprods/index_e.asp.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger