National Critical Infrastructure Assurance Program

Update
Vol. 1, No. 1

March 31, 2003

Table of Contents

"In today's fluid and unpredictable security environment, we need to think differently and respond more creatively. This new environment has highlighted the need for leadership, coordination, and partnerships—across sectors, across regions, and across borders."

-Margaret Purdy, Former Associate Deputy Minister, OCIPEP

"Because the NCIAP will help make our NCI less vulnerable to disruptions, its benefits will be felt throughout Canada: by the people and by Canadian industry and governments."

-Jim Harlick, Assistant Deputy Minister, OCIPEP

1. About the NCIAP

The aim of the National Critical Infrastructure Assurance Program (NCIAP) is to promote a more resilient and viable national critical infrastructure (NCI) through a partnership among 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 our 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 our NCI, 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 development 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.

2. Why This Update?

To ensure that our partners are kept informed about ongoing developments in the NCIAP, the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) will provide regular updates on progress. These updates will enable partners to provide OCIPEP with valuable feedback and keep them actively engaged in the program's evolution.

This update is aimed at anyone with an interest in the NCIAP—those with a vested interest in Canada's NCI and who are working with OCIPEP to build an effective program to assure the continuity of the NCI. It highlights the status of past and current initiatives, successes and accomplishments over the past year, next steps, and future challenges.

Canadians expect that the private sector and all levels of government will cooperate to assure the continuity of critical services. We all have a stake in making the NCIAP function as effectively as possible.

3. Design of the NCIAP

OCIPEP has invited stakeholders to help shape the NCIAP by providing input on the concepts and questions presented in the November 2002 *NCIAP Discussion Paper*. As part of its partnership philosophy, OCIPEP has committed to sharing an aggregated summary of stakeholder comments.

3.1 Progress

Consultation

Consultation has been carried out with stakeholder groups in both industry and government. Minutes, records of discussion, and reports from these consultations were documented and shared with participants.

The table below highlights the particulars of these consultations.

Activity/Format	When	Sector and Group
Workshop	September 2002	OCIPEP staff (to discuss NCIAP scope and objectives)
Meetings	September 2002-February 2003	Lead federal infrastructure departments
Presentation	October 21, 2002	Federal/Provincial/Territorial Conference of Deputy Ministers
Provincial conferences and workshops	September 2002-January 2003	Alberta, Saskatchewan, Manitoba, New Brunswick, Newfoundland & Labrador
Presentations	September-March 2003	Industry stakeholders Working groups, committees Conferences, seminars, meetings
Workshop	December 11, 2002	Federal government departments and agencies (20)
Workshop	March 24, 2003	Government of Ontario
Workshop	March 26, 2003	Government of Saskatchewan

NCIAP Governance

A governance mechanism for the NCIAP is being developed. OCIPEP is examining governance models and structures that provide an appropriate role for stakeholders and partners. Our aim is to ensure that all interests are reflected in our planning and decision-making process and that partners help shape the direction of the NCIAP as it evolves.

3.2 Next Steps

Consultation

Continuous consultation will be encouraged and sought throughout 2003-04, in which representatives from the federal and provincial governments and industry will meet to exchange information about their critical infrastructure (CI) initiatives and issues, and to explore opportunities for partnership. (Target: Throughout 2003-04)

Governance Paper

A document that examines various governance options and identifies a selected governance mechanism for the NCIAP will be developed. (Target: May 2003)

4. CI Identification

What constitutes a CI asset or service? How can we ensure uniformity in the criteria used to identify critical assets, services, and other infrastructure in an environment where interdependence and interconnectedness are characteristic of most sectors?

The identification of CI assets can be an important first step toward the goal of assuring the continuity of services that will make the NCI more resilient and viable. This task can best be done by industry experts and by officials at various levels of government.

4.1 Progress

Tool to Assist Owners and Operators to Identify CI Assets

OCIPEP has produced a resource aimed at assisting CI owners and operators to develop the criteria needed to identify assets and to establish the relative criticality of these assets. It is anticipated that this resource, entitled *Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets*, will serve in the development of selection criteria for NCI assets. This resource will be refined in the coming months.

4.2 Next Steps

NCI Sector Criteria Definition

OCIPEP is conducting an assessment of sector criteria definitions used in the provinces and in other countries, with the aim of refining Canadian NCI sector definitions to make them more comprehensive. (Target: June 2003)

5. Government of Canada CIPP

One of the six CI sectors currently identified by OCIPEP is the government sector, which includes the Government of Canada (GoC)'s own CI. An important aspect of the NCIAP is "getting the GoC house in order." This will be achieved through the GoC Critical Infrastructure Protection Project (CIPP), which will assist departments and agencies in protecting their CI as part of their normal operations.

5.1 Progress

A draft project and work plan is being developed, which will be shared with selected federal government departments to test the validity of the plans.

5.2 Next Steps

A project team is being established to implement the project. (Target: By December 31, 2003, one volunteer department is to be assessed. By March 2007, assessments for the entire GoC are to be completed.)

6. Information Exchange

The nature and scope of information sharing mechanisms, which will form a key component of the NCIAP, has been the focus of a number of initiatives. The key to such mechanisms will be to strike a balance between the public's right to know about issues related to public safety and the need to protect sensitive or proprietary information. Other key issues to overcome include the fact that industry wants information from government but is reluctant to share its own information, and federal government agencies themselves may be reluctant to share information with other organizations.

6.1 Progress

Information Sharing Policy Framework

To address these challenges, an *Information Sharing Policy Framework for OCIPEP* was prepared and shared with industry. This framework outlines OCIPEP's role in information exchange within government and between governments and industry. Under the NCIAP, each industry sector will determine an appropriate model of information sharing based upon its own assessment of vulnerabilities and desired level of government participation. Possible models include

- setting up of Information Sharing and Analysis Centres (ISACs);
- direct exchange (via bilateral agreements) among industry associations or individual companies; and
- centralized collection of information via the federal government.

Guide to the Access to Information Act

One of the concerns associated with information exchange expressed by industry is the potential disclosure of sensitive or proprietary information under the *Access to Information Act* (ATIA). OCIPEP has, therefore, prepared a plain language *Guide to the Access to Information Act,* which outlines the purpose of the Act, the application of the Act, how ATIA requests are processed, and exclusions and exemptions.

6.2 Next Steps

Explore Effectiveness of Information Sharing Mechanisms

Industry Canada is exploring information sharing mechanisms to promote information sharing with the telecommunications sector. OCIPEP plans to evaluate and review the lessons learned from this study, and to determine the potential for wider use and applicability for information sharing among partners as part of the NCIAP. (Target: 2003)

7. Exchanging Threat Information / Exercise Programs

While the GoC has extensive networks that generate threat-related information, other CI owners and operators may likewise learn of potential threats via their own contacts and associations.

Exercises are used to help assess independent actions taken by industry and government, how information is shared between government and industry, and the level of consultation between government and industry at key decision points in response to physical and cyber threats to CI.

7.1 Progress

Various threat scenarios have been developed and tested in tabletop exercises with some industry associations (e.g., Canadian Electricity Association).

The process of walking through each of the potential scenarios with government and industry sector representatives helps to clarify roles and responsibilities and to temper expectations. The threat scenarios present the following situations:

- Industry receives a general threat against the industry.
- The GoC receives credible and specific threats against an industry.
- A terrorist incident affects CI.

7.2 Next Steps

Threat scenarios will be developed and tested with other industry partners (Canadian Bankers Association and Canadian Telecommunications Emergency Preparedness Association). (Target: 2003)

OCIPEP will further develop its program that disseminates alerts, advisories, information notes, and other analyses to CI owners and operators in Canada. (Target: 2003)

8. Awareness, Training, and Education

Raising awareness of critical infrastructure protection (CIP) issues among stakeholders is essential for moving forward with an effective NCIAP. Furthermore, the development, implementation, and ongoing management and operation of CIP programs nationally and at other levels requires stakeholders to have an appropriate level of knowledge and skills.

8.1 Progress

Inventory of CIP Programs, Activities and Issues

As part of OCIPEP's efforts to demonstrate leadership in providing our partners with information, OCIPEP is conducting an inventory of existing or planned CIP programs, activities, and issues of our partners in other levels of government and industry. (Target: 2003)

Awareness, Training, and Education Discussion Paper

A discussion paper is being prepared that examines the requirement for awareness raising, training, and education to support CIP. (Target: May 2003)

8.2 Next Steps

Raising Awareness

OCIPEP will develop and implement a national CIP awareness-raising program within the NCIAP. This program will be aimed at raising awareness of cyber CIP issues among all Canadians, and at developing sector-specific CIP awareness programs targeted at individuals and organizations within the sector. (Target: 2003)

9. Best Practices

The aim of the NCIAP is to increase NCI assurance capability and effectiveness. OCIPEP contributes to this aim by facilitating the sharing of best practices among stakeholders.

9.1 Progress

Best Practices for CIP

As part of OCIPEP's efforts to demonstrate leadership through the provision of guidance, OCIPEP is preparing a *Summary of Best Practices for CIP.* This document will be a review of CIP practices within various sectors, federal government departments, and countries. (Target: June 2003)

9.2 Next Steps

Best Practices for Risk Management

Because the NCIAP is based on a risk management approach and many CI stakeholders use risk management during their normal business practices, there exists an opportunity to apply proven risk management principles to the NCIAP.

OCIPEP intends to develop and share a repository of best practices as they pertain to risk management. This will be done by identifying an NCI industry sector that has strong experience in risk management, and in partnership with the sector association, exploring how its practices can be applied to other sectors. (Target: 2003)

10. Research

The federal government provides leadership, through the NCIAP, for the *assurance* of the continuity of CI owned and operated by the private sector or other levels of government. Measures aimed at achieving assurance and protection should come from owners and operators, with assistance from the federal government. To this end, OCIPEP, within the framework of the NCIAP, conducts research into various CI issues, with the aim of assisting owners and operators to develop the necessary CIP programs and processes.

10.1 Next Steps (Proposed)

Research on Infrastructure Interdependencies

CI interdependencies are not all identified, and some of those that are identified are not well understood. Understanding the threats to CI through interdependencies is important for the NCIAP's risk management approach.

OCIPEP will initiate research projects open to academic and other research organizations and sector associations. Research topics may include interdependencies related to information technology (IT), geography, supply chain, and public response. Wherever possible, research will build on work already undertaken by other countries such as the United States, Britain, France, and Germany.

Research on All-Hazards Risk Profiles

Risks to CI have in the past been disproportionately focused on terrorist-related and cyber threats. Because the NCIAP is intended to apply to all hazards, an integrated all-hazards view of threats needs to be developed and promoted. This view would properly situate terrorist, cyber, and other CIP specific risks with other "traditional" risks.

OCIPEP intends to conduct research, via one or more industry sector associations, to assess the impact of the "new" hazards relative to traditional hazards and to integrate new threats into traditional threat profiles. The new threat profile will be integrated in the planned awareness raising efforts to illustrate the all-hazards approach.

11. The Road Ahead

The NCIAP must move beyond providing a framework, and develop programs and partnerships that provide assurance of the continuity of Canada's NCI.

The consultations conducted to date have revealed that stakeholders seek more concrete details about the NCIAP, in particular in developing criteria for determining CI, and in the areas of governance, information sharing, warning/alert system, risk management models, and vulnerability assessments.

We will minimize the potential for confusion by being clear about the terminology we use when discussing NCI issues. We will demonstrate leadership by getting our own GoC house in order, by setting clear goals, by working with and coordinating efforts of partners, and by implementing the clear vision that is articulated in the *NCIAP Discussion Paper*.

Since the NCIAP is built around the importance and value of information exchange, effort must be focused on overcoming roadblocks to the sharing of vital information. We need to find ways of mitigating restrictive policies that thwart information sharing by government. At the same time, we need to balance the benefits of information sharing with the need to limit information sharing with people and organizations that do not have the required security clearances. The *desire* to know must be balanced with the *need* to know. These and other issues will be discussed with NCI stakeholders over the coming months.

Finally, a position paper will be released in summer 2003 that sets clear directions and goals for all partners with an interest in assuring a more viable and resilient CI for Canadians.

12. For More Information

If you have questions or comments, please contact

Louise Forgues
Director, Program Initiatives
Tel: (613) 990-3498
E-mail: louise.forgues@ocipep-bpiepc.gc.ca

Visit the OCIPEP web site at www.ocipep-bpiepc.gc.ca