



Government
of Canada

Gouvernement
du Canada



**Office of Critical
Infrastructure Protection and
Emergency Preparedness**

**Carnegie Mellon University
Software Engineering Institute**

Information Survivability Workshop

**Gary O'Bright
Director General, Operations
March 19, 2002**

Canada^{ca}

NATIONAL CRITICAL INFRASTRUCTURE

- Energy and utilities
- Telecommunications
- Services (financial, health, food)
- Transportation
- Safety (nuclear, search and rescue, emergency services)
- Government (government-wide mission critical systems)

VULNERABILITIES

- Interdependencies
 - across sectors
 - across nations
 - across international borders
- The Internet
- Inadequate software

THREATS - PHYSICAL AND CYBER

- Natural: floods, earthquakes, tornadoes
- Human: accidental or intentional
- Cyber: hackers, worms, viruses, cyber-terrorism

ESCALATING IMPACT

Incident	Date	Time to Spread	Cost
Cascade	1990	3 years	US\$ 50M
Concept	1995	4 months	US\$ 60M
Melissa	1999	4 days	US\$300M
I Love You	2000	1 day	US\$8B
Code Red	2001	Hours	US\$2.6B


Total cost for all security breaches in 2001 was US\$1.6T
(Price Waterhouse Coopers, 2001)

NATIONAL CRITICAL INFRASTRUCTURE & THE GOVERNMENT OF CANADA

- Essential to health, safety, security and economic well-being of citizens
- Fundamental government responsibility
- Essential to national priorities
 - e-commerce, e-government

OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND EMERGENCY PREPAREDNESS (OCIPEP)

- Created in February 2001
- Civilian agency within the Department of National Defence
- Provides leadership
- Dual mandate



Office of Critical
Infrastructure
Protection and
Emergency
Preparedness

The banner features a vertical gradient from light blue at the top to dark blue at the bottom. It contains a faint background image of a power transmission tower on the left and a stylized globe with a grid pattern on the right. At the bottom, there are overlapping autumn leaves in shades of orange, red, and blue, with a small circular graphic containing a starburst pattern.

EMERGENCY MANAGEMENT (EM) & CRITICAL INFRASTRUCTURE PROTECTION (CIP)

- EM
 - mitigation, preparedness, response, recovery
- CIP
 - protection, detection, response, recovery
- Similar events
 - ↓
- Similar impacts
 - ↓
- Similar responses

Office of Critical
Infrastructure
Protection and
Emergency
Preparedness

WHAT OCIPEP DOES (1)

- Emergency management
 - local government
 - provincial/territorial government
 - national government
 - non-governmental organizations
(e.g. Red Cross)
- Coordinate response to major incidents

WHAT OCIPEP DOES (2)

- Critical Infrastructure Protection
 - Government house-in-order
 - Advice, guidance, expertise
 - Monitoring and response
 - Alerts, advisories, information notes

WHAT OCIPEP DOES (3)

- Special events
- Joint operations
- Communications, education and awareness
- National programs

OCIPEP R & D

- Developing programs and priorities
- Exploring and establishing partnerships
- Centre for cyber expertise
- Internal research projects
- Ongoing work in emergency management
- Incident/event analysis

OCIPEP PARTNERSHIPS

- Across federal government
- Provincial/territorial governments
- Private sector
- US government
- Other countries

SEPTEMBER 11- LESSONS LEARNED

- Prepare for full range of disasters
- Think and plan ahead
- Shared responsibility - all levels of government, private sector, NGOs and first responders
- Avoid complacency - take emergency preparedness seriously
- Communicate - public vigilance and awareness

IMPEDIMENTS TO SURVIVABILITY

- Barriers to effective partnerships
 - information sharing in a competitive environment
 - liability
 - classified information
- Cost
- Lack of knowledge

Office of Critical
Infrastructure
Protection and
Emergency
Preparedness

www.ocipep-bpiepc.gc.ca

Canada 