

Some of OC�PEP's Cyber Security Activities
Andrew McAllister
Director Cyber Protection Division
Office of Critical Infrastructure Protection and Emergency Preparedness (OC�PEP)

Reported by Dave Edmunds

Mr. McAllister commenced by outlining his presentation as an overview of OC�PEP and its Cyber Protection Division (CPD), followed by its activities and interests in the federal government, national, and international fields.

OC�PEP was created by the Prime Minister in February 2001, with the mission of enhancing the safety and security of Canadians in their physical and cyber environments. Its mandate is to provide national leadership of a new, modern and comprehensive approach to protecting Canada's critical infrastructure (the key physical and cyber components of the energy and utilities, communications, services, transportation, safety and government sectors), and to be the government's primary agency for ensuring national civil emergency preparedness – for all types of emergencies. OC�PEP's broad roles and mandate are defined in a Memorandum to Cabinet. Its cyber responsibilities are further defined in the Government of Canada (GoC) Security Policy (GSP) [http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/gsp-psg_e.asp]. It is responsible for providing the GoC 24/7 centre to report threats to the infrastructures critical to the functioning of the government of Canada, monitor and analyse cyber attacks and threats against GoC networks, issue alerts and advice to departments, co-ordinate federal response to cyber and physical threats, and respond to requests from departments for advice on cyber-related incident prevention, detection, response and recovery.

The main operational functions of the Cyber Protection Division (CPD) are incident handling, vulnerability assessment, special projects, cyber practices, and the OC�PEP Information Protection Centre (IPC). It operates in four constituent areas: the internal IPC, the GoC Cyber Incident Response Centre (CIRCC), the national provincial/territorial governments and critical infrastructure sector owners and operators, and internationally with other governments, their national cyber security response teams and other watch & warning networks.

The IPC's internal role is to protect and monitor OC�PEP's own cyber security in order to lead the Government IPC Working Group by example and by developing a repeatable baseline solution that clients can tailor to their needs.

GoC activities are mainly concerned with monitoring and analysis, incident handling, and coordinating the federal response. Monitoring and analysis efforts are concentrated on intrusion detection systems (IDS) issues, construction of an IDS model, and proof of concept. Trends analysis is being applied to product development for OC�PEP clients. Cyber incidents are handled by the CIRCC as the focal point for cyber protection, providing second tier support after initial response by individual affected departments. The CIRCC can draw upon support from DND, CSE, RCMP, CSIS, and other domestic and international peers. There is also a Cyber Incident Coordination System (CICS) which has coordinated teams ready to address cyber incident assessment, intelligence and warning, law enforcement, national security, outreach, and public

affairs. A triage procedure is used to coordinate OCIEPEP, RCMP, and CSIS.

In the national arena, the key thrusts are the development of a Canadian Cyber Coordination Strategy, the short-term implementation of information sharing, and capacity building. The Canadian Cyber Security Strategy will need to recognize that the vast majority of CI owners and operators of cyber systems are under equipped, under funded, and have a steep learning curve ahead. It must also provide a framework in which all levels of CI owners and operators can contribute and which is beneficial to all. Nevertheless, the major effort in Canada is the support to the non federal governments through weekly conference calls, support from the CIRCC, support to provincial IPCs, and support to CI owners and operators.

Internationally, OCIEPEP emphasizes formalizing bilateral relationships, building emergency and incident response networks, and participating in international cyber security initiatives. OCIEPEP currently participates with other Global Computer Emergency Response Teams, is a member of the Forum of Incident Response and Security Teams (FIRST), is a member of the US' Cyber Warning Information Network (CWIN), is one of four "hubs" in a global cyber security incident response watch network, and is active in efforts of APEC, G-8, OAS, etc.

[The Cyber Duty Officer is available, 24/7, at (613) 991-7000 or opscen@ociepep-bpiepc.gc.ca, the OCIEPEP Web site is <http://www.ociepep.gc.ca/index.asp>]