



**THE
OTTAWA**

AFCEAN
April 2005

Inside This Issue

<i>April PD Report</i>	<i>p1</i>
<i>Upcoming Events</i>	<i>p1</i>
<i>IT Security Course</i>	<i>p3</i>
<i>Golf 2005</i>	<i>p4</i>
<i>May Meeting</i>	<i>p4</i>
<i>Your Input</i>	<i>p4</i>

The **Ottawa AFCEAN** is published by:

AFCEA Ottawa Chapter
1 Stafford Rd., East
Suite 197
Nepean, On
K2H 1B9

Tel: (613) 721-6031

Fax: (613) 721-0092

email:

info@afceaottawa.org

Editor:

Bill Hawken

Tel: (613) 841-2912

e-mail:

hawkenw@hotmail.com

Associate Editor:

David W. Edmunds

Business Information

Processors

e-mail:

d.edmunds@rogers.com

The Challenge of Protecting Canada's Critical Infrastructure

Laurie Mack

National Principal, Security and Privacy Solutions, IBM Canada

PD Presentation Report

Ms. Mack opened her presentation by noting that on December 12, the government announced the commitment to review and improve national emergency coordination by creating Public Safety and Emergency Preparedness Canada (PSEPC), releasing the National Security Policy, and developing the national Emergency Management System. The National Security Policy highlights Critical Infrastructure Protection (CIP) and cyber security as national security priorities.

CIP is a proposed approach for governments and critical infrastructures where owners and operators collaborate to assure the continued viability and resiliency of national Critical Infrastructure (CI). CI has been divided by PSEPC into 10 sectors, each with a lead department or agency within the Government of Canada. [*Sector scopes and leads are shown on the presentation slides and notes for Slides 4 and 5.*]

Ms. Mack asked, rhetorically, "Why should we care?" Her response was to focus on national safety and security. The National CI (NCI) comprises 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. The National Critical Infrastructure is made up of the critical assets (continued on page 2)

Upcoming Events

Luncheons:

May 3rd, 2005, Army Officers' Mess

Alice Sturgeon, CIO Branch Treasury Board

June 7th, 2005, Army Officers' Mess

Michael Turner, PWGSC

Golf:

May 19th, 2005, The Meadows

Chapter website: www.afcea.ca/ottawa.htm

Web Services by:

Groupe
adga
Group

The Challenge of Protecting Canada's Critical Infrastructure

(continued from page 1) of the NCI sectors. They are identified by assessing the impact of their loss on the operation of the sector and other sectors, and the consequent losses. Criticality is based on the core values using the criteria of lives, health, safety, security, economic well-being, and effective functioning of governments. Impact and consequences are assessed by six factors: Concentration of People and Assets, Economic, Critical Infrastructure Sector, Interdependency, Service Delivery, and Public Confidence. Interdependencies are increasingly important as our critical infrastructures become more complex, interconnected, and vulnerable. She said that the PSEPC approach is towards an overarching, integrated, federal emergency readiness, response and recovery framework, including protection of both cyber and physical CI regardless of the nature of the vulnerability or source of the threat. This is to be achieved through collaboration and partnerships.

Laurie said that the need for CIP is growing. Provinces, territories, and private sectors are finding that closer ties between their Emergency Measures Organizations (EMOs), cyber security, risk management, and CIP are developing. PSEPC sees roles and responsibilities for CIP following a collaborative framework. Owners and operators are accountable for safeguarding their own CI. All partners will develop, lead and manage their own CIP strategies and programs. All partners will share and work with partners (exercises, R&D, best practices and lessons learned). Sector lead departments and agencies represent the Government of Canada in sector initiatives and enable information sharing with all levels of government and interdependent sectors, and must contribute to the federal government's CIP functional responsibilities. Many problems on jurisdictions, strategies, the PSEPC role, and federal functional responsibilities remain to be resolved. The National CIP Strategy will focus on working with critical infrastructure sectors, owners and operators to identify critical assets, raising national awareness, assessing the risks and threats to physical and cyber infrastructure, improving threat and vulnerability warning and reporting. It will also focus on conducting interdependency analyses and research and development projects, facilitating cross-sector response and recovery coordination, obtaining agreement on measures for response and recovery to CI failures, evaluating regular comprehensive national exercises, and lessons learned analysis. The next steps for the development of CIP Strategy are to consult with provincial and territorial leaders, industry representatives, and key international partners. PSEPC is now leading at provincial town hall meetings. Further steps include developing a national CIP strategy and a national cyber security strategy. PSEPC believes that CI is sufficiently resilient to assure continuity; 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,



Ottawa Chapter Program VP Kelly Stewart-Belisle thanked Ms. Mack for her presentation

demonstrating leadership to other sectors; and new knowledge and tools for CIP are shared.

Ms. Mack said that the National CIP strategy, working with provinces and industry, must have an integrated plan to identify the CI assets, identify and assess vulnerabilities and interdependencies, analyse the threats and risks, prioritize the CI, develop sector-specific strategic CIP programs that are consistent, sustainable, measurable and effective, implement those programs, and measure and promulgate the effectiveness of the programs.

[Ms. Mack's presentation slides will be found at:

www.afcea.ca, Ottawa Chapter.]

AFCEA CANADA IT SECURITY COURSE 2005 NOVEMBER 13 – 18, 2005

NavCanada Training Institute

1950 Montreal Road, Cornwall, Ontario, Canada K6H 6L2

<http://www.navcanada.ca/NavCanada.asp>

Arrival on 13 Nov 05 for check-in & registration

Program starts: 14 Nov 05, 08:30, Wrap-up: 18 Nov 05, 11:30

Check out Friday morning

SPECIAL NOTE:

The Government of Canada information technology security community views this course as a valuable element of information technology security awareness

WHO SHOULD ATTEND?

You should attend if you are in government or the private sector and are mandated to deal with information security issues.

You should possess an introductory level of knowledge in information technology (networking, computers, or telecommunications) to truly benefit from this course.

COMMENTS FROM PREVIOUS ATTENDEES

“The AFCEA Course at NAVCAN’s Cornwall facility is one of the best value introductions to the world of IT security in North America. The range of topics, the quality of instructors & facilities combine to deliver what I found to be an excellent overview of major IT security areas as well as a great survey of the latest trends. Highly recommended as an introduction or a refresher.” Louis S., Bell Canada, IT Security (Student 2003)

“I have been surprised by the fine and complete professional way this course(and the logistic facilities around it) have been prepared and organized. I definitely will send other people over to this course!” December 3rd, LTC Gevels Robert, Belgium Army, Chief INFOSEL

“Recommend to policy people also as a good survey of security. Great intro to TRA, and a good methodology which could be a model for business risk as well.”

“ The food is out of this world and the accommodations are more than sufficient. The atmosphere is relaxed and very good to make you want to learn. Finally I have been to a lot of presentations done by people that were very well paid to do so. To see volunteers doing the same job but 10 times better is outstanding. Thank you to all of you.”

Please visit <http://www.afcea.ca/security-course-flyer-Nov-2005.htm>

for links to the items below:

Course Overview

Registration Form

Sponsorship Form

AFCEA Membership Information

For information about joining AFCEA, or to make changes to your membership profile (e.g. change of address), visit the AFCEA International website at

www.afcea.org - click on “Join/Renew” or check the Portal.

If you should encounter problems, call 703-631-6158 or email

services@afcea.org.

The AFCEA
Ottawa
Chapter would
like to express its
continuing
gratitude to
TIME ICR for
providing its
voice message
system.



May PD Meeting:

Tuesday, May 3rd, 2005 at 12:00 noon

Army Officers' Mess, 149 Somerset Street, Ottawa

Speaker: Alice Sturgeon, Senior Director Architecture Do-
mains, CIO Branch Treasury Board

Topic: Identity Management in the Government of Canada:
Biometrics, Authentication and Standards

Booking Arrangements:

Please check the Chapter website www.afcea.ca/ottawa.htm or call 721-6031. Space is limited. Cost: \$15.00/person for industry or \$5.00/person for government employees. Pay by credit card in advance, or by cash or cheque at the door.

Registration deadline is Fri., April 29th

AFCEA OTTAWA / EDUCATION FUND ANNUAL GOLF TOURNAMENT and DINNER



Thursday, May 19, 2005

The Meadows Golf and Country Club, 4335 Hawthorne Road, Gloucester, Ontario

Visit www.afcea.ca/ottawa.htm for details.

Reader Feedback and Newsletter Submissions

In keeping with Chapter direction to bring more discussion to the areas of professional development and to broaden the scope of the AFCEAN newsletter, we would welcome your comments, articles and other contributions. All are encouraged to submit items of topical or general AFCEA interest (contracts and awards, promotions, upcoming events and courses) to the Editor for publication. Original articles which you the members may wish to submit or comment upon for publication are most welcome. Please take advantage of this opportunity to let AFCEANs worldwide know what you and your Chapter are doing. If you have any questions concerning the appropriateness of a submission please contact the AFCEAN Editor Bill Hawken at 841-2912 or hawkenw@hotmail.com