



**THE
OTTAWA**

AFCEAN
November 2005

Inside This Issue

<i>October PD Report</i>	<i>p1</i>
<i>Upcoming Events</i>	<i>p1</i>
<i>Your Input</i>	<i>p3</i>
<i>December Meeting</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

**Josée Brousseau, Communication Security Establishment (CSE), Director
Canadian Cryptographic Modernization Program (CCMP)**

The Canadian Cryptographic Modernization Program

October PD Meeting Presentation, reported by Bill Hawken

PD Presentation Report

Ms. Brousseau began by expressing her pleasure with the opportunity to “get the word out” through her presentation to AFCEA Ottawa. She outlined her presentation in the context of the strategy and vision for IT security in general.

Ms. Brousseau then highlighted the CSE and CCMP Mission:

“To enhance Canada’s safety and prosperity by ensuring the protection and interoperability of Government of Canada classified information and communications.”

She then outlined the two services CSE provides to the Government of Canada: Signals intelligence (SIGINT) in support of Government policy, specifically Defence Policy and especially National Security Policy; and protection of government information. CCMP falls under the latter service by providing protection of classified communications, fitting into the overall strategy governing where information technology security needs to go.

She stressed that CSE crosses all domains and CCMP covers the classified realms. At present, the state of the art is “system high”, whereby all information on a network, regardless of classification, must be protected to the level of the most highly classified information transported. However, the long term vision is to collapse security domains so that all information can be carried on a network regardless of classification or clearance of personnel using it. Technology is catching up and there is light at the end of the tunnel; it is estimated that the vision will be attainable in 15-20 years.

Ms. Brousseau went on to explain that there are some 42 departments and agencies of government requiring a classified communi- (continued on page 2)

Upcoming Events

Luncheons:

December 6th, 2005, Army Officers’ Mess Speaker: J.F Sauriol - Phirelight

January 10th, 2006, Army Officers’ Mess

Chapter website: www.afceaottawa.ca

Web Services by:



The Canadian Cryptographic Modernization Program

(continued from page 1) cations transmission capability. At present, only high-grade technology is available to meet these needs and there is a need to move on to new technologies. She pointed out that the requirement is for interoperability and that the need for security increases the challenge. She also stressed that present technology is 20-30 years old, reaching end-of-life and requires modernization and upgrade. Vendors will gradually drop their support for the older technology, creating a maintenance nightmare if we stay with these technologies.

Ms. Brousseau noted that in 1999, the U.S. had initiated a large crypto modernization program and that the U.K. also has a program. Canada's program started in 2002, with the Department of National Defence as the largest stakeholder. There are other major players in the security and intelligence communities as well as smaller, but equally important stakeholders, whose requirements must be met.

She then stated that the question of what the stakeholders need and want has been addressed through consultation, and the results summarized under six objectives: ensure classified information protection; enhance interoperability; leverage knowledge transfer for critical infrastructure protection; implement an affordable solution; enable business transformation; and address sovereignty. She illustrated the interoperability objective by reminding the audience of the breadth of the information exchange requirements among all elements of government organizations including police and border agencies. Applying lessons learned is a key element of leveraging knowledge. Security, traditionally seen as a "party pooper" must now take on a fresh image as a key enabler because we can't do business without it. Addressing sovereignty includes creating the freedom to deploy when, where and how we want to, but our use of U.S. technology and the need to address the issue affordably poses additional challenges. When leveraging allied R&D, we need to use the knowledge in a way that maintains sovereignty.

Resolution of these issues to implement the strategy demands engagement of stakeholders. Doing this manageably has meant dealing with the issues in three chunks: creating a CCMP role as coordinator of individual departmental crypto modernization projects, including working through an interdepartmental advisory committee (IDAC) to achieve ADM-level consensus with annual reporting to Treasury Board; focussing significant resources on what will always be the largest individual partner, DND, notwithstanding increased PSEPC and border activities; and working with the U.S. National Security Agency, the U.K. and other allies to coordinate and influence activities wherever possible, to ensure necessary interoperability.

As a key component of this international effort, Canada participates in and contributes to numerous working groups. CSE is in the process of increasing and consolidating its capability base by building and increasing intellectual capacity so as to leverage knowledge available through cooperative efforts in the international community, notably "five eyes" work (AS/CA/NZ/UK/US).

Ms. Brousseau then turned to the CCMP schedule, which she explained is built around families of technologies. These include an Electronic Key Management infrastructure as well as a Classified Security Management Infrastructure (CSMI) whose purpose is to build an infrastructure under all of the technology families of projects. Throughout the program, an ongoing R&D-like effort will monitor new capabilities (e.g. VoIP, Wireless, Optical, etc) to ensure that Canada is at the table influencing developments and ensuring that key technology improvements are pulled into the project families.

Implementation will involve undertaking projects a few at a time. Currently, there are replacement projects under way to address end-of-life issues without adding new capability. In the near term, some modernization will be undertaken, in particular the rekey infrastructure and secure voice/telephone including secure GSM telephone once coverage issues have been worked. In the longer term, newer concepts included within the CSE vision such as network-centric warfare will be introduced.

Currently, work is under way to define and plan some of these new projects, including the first two phases of the CSMI effort and Link Encryption. The link encryption effort has undertaken a complete review to determine what should be changed or redesigned, including the feasibility of moving directly to network encryption instead of replacing link encryption equipment.

Future work will include implementation of CSMI Phase 3, an effort Ms. Brousseau would like to see move faster. Along with its many advantages, network encryption has some drawbacks and security issues to be evaluated, including possible vulnerability to traffic analysis entailed by the presence on the network of IP addresses. She notes that 40% of the DND radio inventory includes modular crypto requiring replacement. It is intended a much as possible to leverage previous TCCCS work in order to re-use existing systems instead of starting over. Other work will include an exciting initiative examining the possibility of secure mobile service such as Blackberry providing wireless secure voice, e-mail and other services. A DND contribution to this effort will provide the opportunity to influence the direction this initiative will take, while monitoring R and D in related areas.

(cont on p. 3)

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.

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

(from page 2) Ms. Brousseau concluded by reiterating that ensuring the protection and interoperability of GoC classified information and communications is crucial to the safety and prosperity of Canadians. She noted that CCMP is receiving solid support and is seeing considerable enthusiasm among the many participating Government departments and excitement in industry as the vision takes shape.

Ms Brousseau then took questions from the audience. Asked how Canada was able to catch up to other key players in the crypto arena, she replied that being small, with fewer stakeholders, we can be more agile; furthermore, our decentralized construct has helped in moving ahead.



Ottawa Chapter President Kelly Stewart-Belisle thanked Ms Brousseau for her presentation

She stated that even though the US started in 1999 and we started in 2002, Canada has definitely caught up and it's her (Ms. Brousseau's) job to create and maintain momentum. She noted the importance of the periodic lessons learned review in continual reshaping of the program. She was then asked whether Canada would develop its own crypto capability. She replied that while there are discussions on this subject, it is unlikely that Canada will develop an indigenous capability because of the need for interoperability among not only all national players, but also with all of our allies, especially in North America.

Ms. Brousseau then expressed her thanks for the invitation and opportunity to speak to the AFCEA Ottawa Chapter.

[Ms. Brousseau's presentation slides will be found at <http://www.afceaottawa.ca/presentations.htm>, Ottawa Chapter.]

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



December PD Meeting:

Tuesday, December 6th, 2005 at 12:00 noon

Army Officers' Mess, 149 Somerset Street, Ottawa

Speaker: JF Sauriol

Chief Security Consultant Phirelight E- Business Solutions

Topic: Identity Theft

This presentation will begin by describing probably the most alarming trend in security attacks for individuals: identity theft. You receive a harmless e-mail from your financial institution doing a survey or advising you that they need to update their client database. You follow the link, fill in the form, and 2 minutes later you are broke!!! We will examine the latest attack patterns and identify strategies to prevent being the 1 out of 8 Canadians expected to become victims to various phishing schemes. Examples of common attacks will also be presented.

Cost: \$5.00 for government; \$15 for industry.

To Register:

Fill out the [Meeting Registration Form](#)

[Pay for Meetings with Credit Card](#)

or by email at info@afceaottawa.org

or by calling 721-6031.

Deadline for registrations is Friday, Dec 2 , 2005.

For more information please call 721-6031.