March 2012

## Federal, Provincial and Territorial Teleconference on Cyber Security

May 28, 2011
2:00 p.m. to 3:00 p.m. (Eastern Time)

Local: 613-960-7514
Toll-free: 1-877-413-4790
Conference code:

## AGENDA

| | Time | Item |
|---|---|---|
| 1. | 2:00<br>*5 min* | **Opening Remarks**<br>Robert Dick, Director General, National Cyber Security, Public Safety Canada |
| 2. | 2:05<br>*10 min* | **Debrief on FPT Clerks Meeting**<br>Rennie Marcoux, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office (TBD)<br>*For information: Debrief on the FPT Clerks meeting that took place on January 23, 2012.* |
| 3. | 2:15<br>*20 min* | **Cyber Incident Management Framework**<br>Robert Dick, Director General, National Cyber Security, Public Safety Canada<br>*For information and discussion: Provide an update on activities to date, including pilot projects with Ontario and Manitoba, and seek input on the proposed way forward* |
| 4. | 2:35<br>*5 min* | **Memorandum of Understanding (MOU) on Information Sharing**<br>Robert Dick, Director General, National Cyber Security, Public Safety Canada<br>*For information: Provide an update on the status of the MOU* |
| 5. | 2:40<br>*5 min* | **Academic Conference on Critical Infrastructure and Cyber Security**<br>Robert Dick, Director General, National Cyber Security, Public Safety Canada<br>*For information: Provide an overview of the conference and the broader academic engagement strategy* |
| 6. | 2:45<br>*5 min* | **Overview of National Cyber Security Directorate's Objectives for 2012-13**<br>Robert Dick, Director General, National Cyber Security, Public Safety Canada<br>*For information: Provide an overview of the planned objectives and activities for fiscal year 2012-13* |
| 7. | 2:50<br>*10 min* | **Roundtable**<br>All participants |

# DEBRIEF ON THE OUTCOME OF THE FEDERAL, PROVINCIAL AND TERRITORIAL CLERKS DISCUSSION OF CYBER SECURITY

(For information)

## PROPOSED TALKING POINTS

- I understand that the January 23 FPT Clerks discussion on cyber security was very positive, and that there was support for enhanced intergovernmental collaboration on cyber security.
- I would like to ask Ms. Rennie Marcoux, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office, to give us a debrief?

## ISSUE

Rennie Marcoux will provide a debrief of the January 23, 2012, meeting of the Federal, Provincial and Territorial Clerks on cyber security.

## BACKGROUND

Cyber security was discussed at the last FPT Clerks meeting, at the request of the BC Clerk. Clerks were provided with an all-hazards threat briefing by the Canadian Security Intelligence Service and a cyber threat briefing by the Communications Security Establishment (represented by John Adams). Both briefings were generally well received, although the ensuing discussion focused mainly on the all-hazards briefing. Clerks expressed a strong desire to receive regular threat briefings, and touched on the issues of information sharing practices. The Clerk committed to clearing one individual from each jurisdiction at the TOP SECRET level, and to clear an appropriate number of PT staff to the SECRET level.

## CONSIDERATIONS

[redacted]

## CURRENT STATUS

Public Safety Canada is working with PTs on a number of fronts related to cyber security:

- finalising an MOU on information sharing;
- conducting a table top exercise to coordinate FPT responses to cyber incidents;
- consulting FPT officials on CCIRC's products and services;
- building trust by convening regular meetings of the ADM FPT cyber committee, and participating on the National Chief Information Officer Subcommittee on Information Protection (NCSIP) committee at the operational level;
- partnering on public awareness; and
- seeking their collaboration on research and broader academic engagement.

## CONCLUSION

Public Safety Canada will continue to collaborate with PTs on cyber security with the long term objective of moving to a more strategic level of cooperation and developing a shared agenda for action.

Prepared by: Semira Selman
Approved by: Sebastien Labelle

2012

**UNCLASSIFIED**

DATE:

File No.: 386626
RDIMS No.: 581360

## MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

## FEDERAL, PROVINCIAL AND TERRITORIAL TELECONFERENCE ON CYBER SECURITY ON APRIL 3, 2012

(For decision)

## ISSUE

It is proposed that you chair a meeting of the Federal, Provincial and Territorial Assistant Deputy Ministers Committee on Cyber Security (FPT ADM Committee on Cyber) on April 3, 2012, from 14:00 to 15:00 (EST).

A copy of the draft agenda is attached for your ease of reference (**TAB A**).

## BACKGROUND

The previous meeting of the FPT ADM Committee on Cyber was held on December 15, 2011, via teleconference and was chaired by Bob Gordon, Special Advisor on Cyber Security. A copy of the minutes from the meeting is attached for your ease of reference (**TAB B**). Mr. Gordon proposed to hold the next meeting in March 2012, and the Committee agreed.

## CURRENT STATUS

It is proposed that Rennie Marcoux, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office (PCO), debrief the members on the outcome of the Federal, Provincial, Territorial Clerks meeting, which took place on January 23, 2012. Of note are two cyber security related outcomes:

- Mr. Wouters committed to ensuring that every jurisdiction has at least one individual that has been cleared through the federal government's clearance process to the "SECRET" level in order to receive classified briefings and support the provincial/territorial Clerk/Cabinet Secretary in fulfilling their responsibilities;

s.14(a)
s.21(1)(c)

- Public Safety's Deputy Minister will be asked to examine FPT collaboration on security/cyber security issues and provide recommendations on further actions to be taken. Cyber security could return to the agenda in a future meeting.

Necessary arrangements are being made with Ms. Marcoux's Office to ensure that she is prepared to speak at the teleconference. We will be working with PCO to coordinate on the issue of security clearances as we have already initiated a process to clear two officials per jurisdiction. We will also prepare a letter of response for the second item.

[redacted]

It is proposed that you lead a discussion on the way forward for the development of a cyber incident management framework. The framework would provide a consolidated approach to the management and coordination of a significant cyber event in Canada. The framework would be based on voluntary compliance and partnerships between governments, critical infrastructure and industry.

It is suggested that you inform the group that the next in-person meeting of the National CIO Subcommittee on Information Protection (NCSIP) scheduled for June 2012, in Prince Edward Island, will include an extra day during which Public Safety Canada will lead discussions on Canadian Cyber Incident Response Centre (CCIRC) products and services, and run through a "table top" exercise to support the development of a cyber incident management framework.

It is recommended that you inform the group that Public Safety Canada will be hosting an academic conference on critical infrastructure and cyber security issues. The conference will bring together the academic community and Public Safety officials to discuss existing academic views and models in the area of critical infrastructure and cyber security and identify key challenges. An agenda and participant list is currently being developed.

Finally, Stéphanie Durand, Director General of Communication, will provide an update on the public awareness campaign and the upcoming preparations for October cyber security month.

## RECOMMENDATION

It is recommended that you convene and chair the proposed FPT ADM Committee on Cyber. Should you agree, a briefing package will be prepared for your use at the meeting and will be sent to you under a separate cover.

Should you require additional information, please do not hesitate to contact me or Mr. Sébastien Labelle, Director of Partnership and Engagement at (613) 990-2665.

Robert Dick
Director General
National Cyber Security

Enclosure: (3)

I approve:

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Semira Selman

April 2012

Tab A

**Federal, Provincial and Territorial Teleconference on Cyber Security**

April 3, 2011
2:00 p.m. to 3:00 p.m. (Eastern Time)

Local: 613-960-7514
Toll-free: 1-877-413-4790
Conference code:

## AGENDA

| | Time | Item |
|---|---|---|
| 1. | 2:00<br>*5 min* | **Opening Remarks**<br>Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada |
| 2. | 2:05<br>*10 min* | **Debrief on FPT Clerks Meeting**<br>Rennie Marcoux, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office (TBD)<br>*For information: Debrief on the FPT Clerks meeting that took place on January 23, 2012.* |
| 3. | 2:15<br>*10 min* | **Memorandum of Understanding (MOU) on Information Sharing**<br>Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada<br>*For discussion: Seek preliminary views on the MOU* |
| 4. | 2:25<br>*15 min* | **Cyber Incident Management Framework**<br>Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada<br>*For discussion: Seek input on the proposed way forward* |
| 5. | 2:40<br>*5 min* | **June meeting of the National CIO Subcommittee on Information Protection (NCSIP)**<br>Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada<br>*For information: Provide an overview of the proposed agenda for the additional day to the NCSIP meeting* |
| 6. | 2:45<br>*5 min* | **Academic Conference on Critical Infrastructure and Cyber Security**<br>Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada<br>*For information: Provide an overview of the conference* |
| 7. | 2:50<br>*5 min* | **Public Awareness Campaign**<br>Stéphanie Durand, Director General of Communication, Public Safety Canada<br>*For information: Provide an update on the public awareness campaign and next steps* |

Tab B

## Federal, Provincial, Territorial (FPT) Teleconference on Cyber Security, December 15, 2011

## Meeting Summary

***List of participants***

Public Safety Canada: Bob Gordon (chair), Robert Dick, Stéphanie Durand, Sébastien Labelle and Windy Anderson

British Columbia: Rob Todd
Alberta: Kate Rozmahel, Tim McCreight
Saskatchewan: John Masters, Duane Mckay
Manitoba: Don Mackinnon
Ontario: Robert Chiarelli
[redacted]
Nova Scotia : Wallace Peers
Newfoundland and Labrador : Tracy English
Not on the call: New Brunswick, Prince Edward Island, Yukon, Northwest Territories and Nunavut

***Summary of Action items:***

- Public Safety Canada will:
    - share metrics on the Public Awareness Campaign (attached);
    - share the list of FPT communications working group members (attached);
    - send a note describing purpose of our visits (forthcoming);
    - send official invitation for consultations on the Canadian Cyber Incident Response Centre (CCIRC)– January 2012;
    - share draft Memorandum of Understanding on information sharing for comment and review – January 2012;
    - share a draft gap analysis document for comment and review – (Winter 2012);
    - share a summary from the London Cyber Space Conference (attached); and
    - share information on the upcoming control systems (SCADA) workshops (attached).

- PTs to brief their Clerks consistently to support:
    - continued intergovernmental collaboration on cyber security; and,
    - work to define how a major cyber incident would be handled nationally.

- PTs to support Public Safety Canada in establishing links with PT emergency management counterparts.

- PTs to identify a senior policy analyst contact.

- Next teleconference call: March 2012.

- Next in-person meeting: approximately June 2012.

## *Meeting Minutes*

Bob Gordon, chair of the teleconference call, welcomed participants and confirmed the agenda.

### *Public Awareness Campaign*

Stéphanie Durand, Director General of Communications, provided an overview of the *Get Cyber Safe* public awareness campaign. British Columbia requested metrics on Twitter use (attached).

Ms. Durand described the ongoing work with her provincial and territorial communications counterparts. The FPT group will be looking to finalize terms of reference and to discuss cyber incident management communications protocol. Ms. Durand thanked British Columbia and Newfoundland and Labrador for adding *Get Cyber Safe* buttons to their websites, and Tracy English for her assistance in finalizing the terms of reference for the working group. The list of FPT Working Group members is attached, and the next FPT Communications Working Group call will be held on January 10, 2012.

Ms. Durand indicated that the focus over the next year would be to leverage the collaboration of the private sector and critical infrastructure sectors and to solidify the existing FPT collaboration on communications. This could include joint public announcements, sharing best practices, and the preparations for cyber month in 2012, etc.

Ms. Durand provided an update on Public Safety Canada's is collaboration with its international partners.

### *January 23, 2012 Meeting of the Clerks*

Bob Gordon provided an overview of the upcoming Federal, Provincial, Territorial Clerks meeting on January 23, 2012. Mr. Gordon indicated that the Clerks have signalled a desire to discuss cyber security. The Government of Canada will be providing both an all hazards threat brief and a specific cyber security brief to promote a common understanding of the threats and risks.

PT clerks have also signalled an interest in exploring the ability of FPT governments to respond effectively to a significant cyber event. Mr. Gordon noted that support from provincial/territorial clerks is needed to move forward on the development of a framework that could respond to a major cyber incident. Although there are existing structures in place for emergency management, there is a need to better understand if and/or how cyber fits within them. In moving forward on this file, it will be essential to establish strong linkages between the emergency management and the cyber security communities.

In order to effectively assess the adequacy of current tools, Public Safety Canada will be developing a number of scenarios and exercises. We will be developing these but will need assistance to run through them. Mr. Gordon also indicated that federally, Public Safety Canada will lead a table top exercise in January, 2012 with the key agencies.

s.14(a)

s.15(1) - Int'l

### *Gap analysis and action plan*

Mr. Gordon [redacted]

### *Other items*

Mr. Gordon provided a debrief of the November 2011 London Cyber Space Conference, which brought together more than 700 participants from 60 countries. The participants included senior government officials, industry leaders, and representatives of the Internet technical community and civil society. The purpose was to begin dialogue on the principles for governing behaviours in cyberspace. The Conference focused on five topics: economic growth and development, social benefits, international security, cyber crime and ensuring safe and reliable access. The summary of the Conference is attached, as requested by Alberta.

Mr. Gordon also indicated that [redacted]

Adam Hatfield, Director of Technical Advice, provided a debrief of the control systems (SCADA) workshop that took place in Newfoundland and Labrador in November 2011, noting that the workshop was a success with high turnout. He also indicated that there will be two more workshops, one January 31 to February 1, 2012, in Montreal, and one in March, 2012, in Calgary. Additional information is attached.

### *Next Steps / Roundtable*

Mr. Gordon summarized the call indicating that there will be a number of deliverables coming from Public Safety Canada over the next five months. He invited interested jurisdictions to chair or co-chair the meetings in the future.

Mr. Gordon also asked jurisdictions to identify a senior policy analyst to assist in preparing future calls and to help work through some policy issues.

The next teleconference call is proposed for March 2012, followed by an in person meeting in June 2012.

s.19(1)

## Téléconférence fédérale, provinciale et territoriale (FPT) sur la cybersécurité
## Le 15 décembre 2011

# Sommaire de la réunion

### *Liste des participants*

Sécurité publique Canada : Bob Gordon (président), Robert Dick, Stéphanie Durand, Sébastien Labelle et Windy Anderson

Colombie-Britannique : Rob Todd
Alberta : Kate Rozmahel, Tim McCreight
Saskatchewan : John Masters, Duane Mckay
Manitoba : Don Mackinnon
Ontario : Robert Chiarelli
[redacted]
Nouvelle-Écosse : Wallace Peers
Terre-Neuve-et-Labrador : Tracy English
Absents : Nouveau-Brunswick, Île-du-Prince-Édouard, Yukon, Territoires du Nord-Ouest et Nunavut

### *Résumé des mesures de suivi*

- Sécurité publique Canada :
  - communiquera les paramètres de la campagne de sensibilisation du public (ci-joints);
  - enverra la liste des membres du Groupe de travail FPT sur les communications (ci-jointe);
  - transmettra un document décrivant l'objectif de nos visites (à suivre);
  - enverra une invitation officielle aux consultations sur le Centre canadien de réponse aux incidents cybernétiques (CCRIC) – janvier 2012;
  - communiquera l'ébauche du protocole d'entente sur l'échange d'information aux fins d'examen et de commentaires – janvier 2012;
  - enverra l'ébauche du document d'analyse des lacunes aux fins d'examen et de commentaires – hiver 2012;
  - transmettra un résumé de la Conférence de Londres sur le cyberespace (ci-joint);
  - transmettra de l'information sur les prochains ateliers sur les systèmes de contrôle (SCADA) (ci-jointe).

- Les provinces et les territoires (PT) tiendront leurs greffiers au courant des éléments nouveaux afin de soutenir :
  - la collaboration intergouvernementale constante en matière de cybersécurité;
  - le travail visant à définir la façon d'intervenir face à des cyberincidents majeurs à l'échelle nationale.

- Les PT aideront Sécurité publique Canada à établir des relations avec ses homologues provinciaux et territoriaux responsables de la gestion des urgences.

- Les PT choisiront un analyste principal des politiques en tant que personne-ressource.

- Prochaine téléconférence : mars 2012.

- Prochaine réunion en personne : juin 2012 (environ).

## *Compte rendu de la réunion*

Bob Gordon, président de la téléconférence, accueille les participants et confirme l'ordre du jour.

### *Campagne de sensibilisation du public*

Stéphanie Durand, directrice générale des Communications, donne un aperçu de la campagne de sensibilisation du public « Get Cyber Safe ». La Colombie-Britannique demande quels sont les paramètres liés à l'utilisation de Twitter (ci-joints).

Mme Durand décrit le travail continu effectué en collaboration avec ses homologues provinciaux et territoriaux en matière de communications. Le Groupe FPT souhaite terminer le mandat et discuter du protocole de communication pour la gestion des cyberincidents. Mme Durand remercie la Colombie-Britannique et Terre-Neuve-et-Labrador d'avoir ajouté les boutons « Pensez cybersécurité » sur leur site Web, ainsi queTracy English de son aide relativement à la finalisation du mandat pour le Groupe de travail. Vous trouverez ci-joint la liste des membres du Groupe de travail FPT. La prochaine téléconférence du Groupe de travail FPT sur les communications se tiendra le 10 janvier 2012.

Mme Durand précise qu'au cours de la prochaine année, il faudra se concentrer sur le renforcement de la collaboration du secteur privé et des secteurs des infrastructures essentielles, ainsi que sur la solidification de la collaboration FPT existante en matière de communications. Nous pourrions entre autres faire des annonces publiques conjointes, échanger des pratiques exemplaires et nous préparer pour le mois de la cybersécurité en 2012.

Mme Durand fait le point sur la collaboration de Sécurité publique Canada avec ses partenaires internationaux.

### *Réunion des greffiers du 23 janvier 2012*

Bob Gordon donne un aperçu de la prochaine réunion FPT des greffiers qui se tiendra le 23 janvier 2012. M. Gordon précise que les greffiers ont exprimé le désir de discuter de la cybersécurité. Le gouvernement du Canada fournira de l'information sur tous les types de menace et plus particulièrement sur la cybersécurité afin de favoriser une compréhension commune des menaces et des risques.

Les greffiers des PT ont également exprimé l'intérêt d'examiner la capacité des gouvernements FPT d'intervenir efficacement en cas de cyberincident majeur. M. Gordon précise que l'appui des greffiers provinciaux et territoriaux sera nécessaire pour aller de l'avant avec l'élaboration d'un cadre qui pourrait orienter l'intervention en cas de cyberincident majeur. Même s'il existe déjà des structures pour la gestion des urgences, il faut essayer de mieux comprendre si l'aspect cybernétique est applicable à ces structures et, si oui, comment. Dans ce dossier, il sera essentiel d'établir des relations solides entre les intervenants des domaines de la gestion des urgences et de la cybersécurité.

Afin d'évaluer adéquatement la pertinence des outils actuels, Sécurité publique Canada élaborera un certain nombre de scénarios et d'exercices. Nous nous chargerons de cette tâche, mais nous aurons besoin d'aide pour les passer en revue. M. Gordon affirme aussi qu'à l'échelle nationale, Sécurité publique Canada dirigera un exercice sur table qui aura lieu en janvier 2012 avec les principaux organismes.

Les représentants provinciaux acceptent de collaborer avec Sécurité publique Canada pour mener des exercices à Ottawa au printemps 2012. Des bénévoles provinciaux ont été choisis lors de la réunion du Sous-comité des dirigeants principaux de l'information sur la protection de l'information (SCDPI) d'octobre 2011. Parmi ces bénévoles mentionnons Rick Ouellette, Tim McCreight, Stu Hackett, Carl Rajack et Patrick Hoger. M. Gordon déclare que d'autres personnes peuvent également participer au processus de consultation. L'invitation officielle sera lancée en janvier 2012.

M. Gordon précise que Sécurité publique Canada aura besoin d'aide pour établir des relations avec ses homologues provinciaux et territoriaux responsables de la gestion des urgences. Entre janvier et mars 2012, Sébastien Labelle, Kent Schramm et Semira Selman visiteront bon nombre d'administrations pour discuter de certaines questions, notamment le cadre de gestion des cyberincidents et l'analyse globale des lacunes. Vous trouverez ci-joint un document contenant davantage de renseignements à ce sujet.

***Consultations sur le mandat réorienté du Centre canadien de réponse aux incidents cybernétiques (CCRIC)***

M. Gordon précise que depuis le lancement de la Stratégie de cybersécurité du Canada, il y a eu une redéfinition importante des rôles et des responsabilités en matière de gestion des cyberincidents quant aux systèmes du gouvernement du Canada. Le CCRIC demeure l'équipe nationale d'intervention en cas d'urgence informatique, mais la responsabilité relativement aux incidents qui surviennent à l'intérieur du gouvernement fédéral a été transférée au Centre de la sécurité des télécommunications Canada (CSTC). Le mandat du CCRIC a été réorienté davantage sur les intervenants nationaux, notamment les provinces et les territoires ainsi que les propriétaires et les exploitants des infrastructures essentielles. Sécurité publique Canada propose de tenir une séance de consultation avec les provinces et les territoires afin de s'assurer que les services fournis sont aussi utiles que possible.

Cette discussion aura lieu immédiatement après la discussion sur le cadre d'intervention face aux incidents qui se tiendra en avril 2012 avec les représentants des PT (point susmentionné). Une invitation officielle sera lancée le 31 janvier 2012.

s.14(a)

s.15(1) - Int'l

***Mécanismes d'échange d'information***

M. Gordon affirme que Sécurité publique Canada a collaboré avec l'Association canadienne de l'électricité pour établir un protocole d'entente (PE) quant à l'échange d'information. L'entente est sur le point d'être achevée.

M. Gordon précise que plusieurs provinces ont exprimé le désir d'établir un mécanisme d'échange d'information plus officiel. Pour donner suite à cette demande, Sécurité publique Canada rédige actuellement un PE sur l'échange d'information, que les PT pourront ensuite commenter. L'ébauche du PE sera communiquée en janvier 2012.

En attendant, Sécurité publique Canada examinera les options relatives à l'échange d'information classifiée et continuera d'échanger des renseignements précieux, comme il l'a fait à la réunion du SCDPI en octobre 2011.

***Analyse des lacunes et plan d'action***

M. Gordon [redacted]

***Autres points***

M. Gordon donne un compte rendu de la Conférence de Londres sur le cyberespace tenue en novembre 2011, qui a réuni plus de 700 participants de 60 pays. Parmi les participants figuraient des hauts fonctionnaires des gouvernements, des chefs de file de l'industrie et des représentants du milieu technique de l'Internet et de la société civile. La Conférence visait à amorcer le dialogue concernant les principes régissant les comportements dans le cyberespace. Elle portait expressément sur cinq sujets : le développement et la croissance économique, les avantages sociaux, la sécurité internationale, le cybercrime ainsi que l'accès sécuritaire et fiable. Vous trouverez ci-joint le résumé de la Conférence, comme il a été demandé par l'Alberta.

M. Gordon mentionne également [redacted]

Adam Hatfield, directeur des conseils techniques, donne un compte rendu de l'atelier sur les systèmes de contrôle (SCADA) qui s'est tenu à Terre-Neuve-et-Labrador en novembre 2011, précisant que l'atelier s'est avéré un succès grâce à son fort taux de participation. Il a aussi mentionné qu'il y aura deux autres ateliers; le premier sera donné du 31 janvier au 1er février 2012, à Montréal, et le deuxième, en mars 2012, à Calgary. Vous trouverez ci-joint des renseignements supplémentaires à cet égard.

***Prochaines étapes et tour de table***

M. Gordon résume la téléconférence en précisant qu'un certain nombre de produits seront livrés par Sécurité publique Canada au cours des cinq prochains mois. Il invite les administrations intéressées à présider ou à coprésider les prochaines réunions.

M. Gordon demande également aux administrations de choisir un analyste principal des politiques pour aider à préparer les prochaines téléconférences et pour aider à passer en revue certaines questions stratégiques.

On propose de tenir la prochaine téléconférence en mars 2012, suivie d'une réunion en personne en juin 2012.

Public Safety Canada
Sécurité publique Canada

# Cyber Security Awareness Month 2011 – Summary of Activities and Public Response

Canada

# Cyber Security Awareness Month – Media Coverage

- Minister Toews, joined by Lois Brown, Parliamentary Secretary to the Minister of International Cooperation, and representatives from the telecommunications sector, launched the GetCyberSafe campaign on October 3 with an event at the University of Ottawa

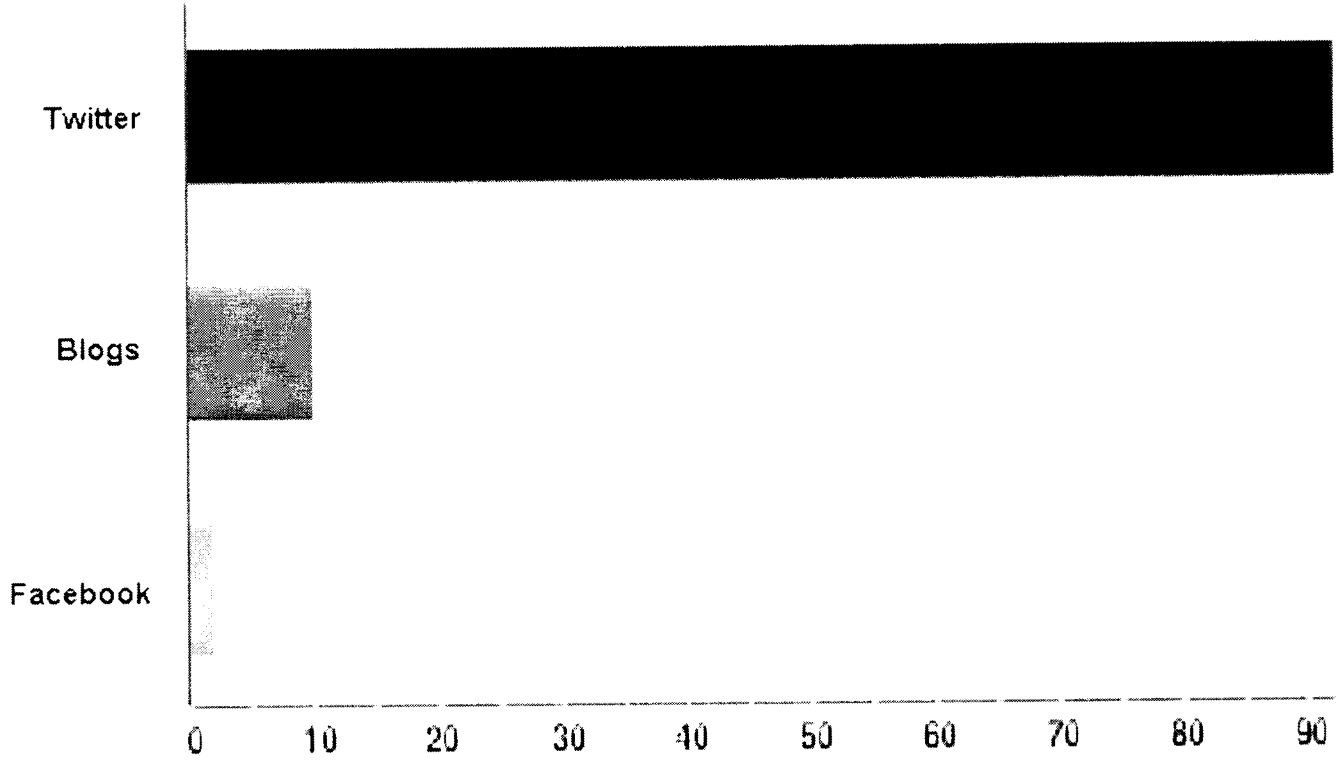
- Limited print but significant online media coverage in the days immediately following the launch, including all major national media outlets
  - Overall coverage was positive and supportive of the campaign

# Cyber Security Awareness Month: Media Coverage

- Broadcast media also gave prominent coverage to the campaign launch:
  - CBC reports included footage from the campaign's pre-roll video advertisement
  - CTV News reported on the launch event and aired several interviews on cyber security threats with industry professionals, including representatives from Open Media, the Canadian Police Association, and the Conference Board of Canada
  - Select reports on the launch did reference the high-profile IT security breach at Treasury Board Secretariat and the Department of Finance in January 2011

# Cyber Security Awareness Month – Social Media Coverage

- Initial discussions on social media regarding the launch of the GetCyberSafe campaign were distributed across social media platforms as follows:



# Cyber Security Awareness Month – Social Media Coverage

- In the days immediately following the launch, the CBC's *Cyber Security Q&A* was the most widely shared source of information regarding the *Get Cyber Safe* campaign

- *Twitter*
  - Twitter was the most active platform on the issue
  - In the days immediately following the launch, the CBC's *Cyber Security Q&A* was the most widely shared source of information regarding the *Get Cyber Safe* campaign.
  - Users primarily shared neutral statements declaring the launch of the campaign, or re-tweeted information from the CBC or the Public Safety Twitter accounts
  - Some users engaged in discussion about the campaign, displaying both positive and negative sentiments towards it

# Cyber Security Awareness Month – Twitter Activity

- 50 cyber-related tweets were issued during Cyber Security Awareness Month (including tips, media advisories, news releases, and photos) via the Departmental Twitter accounts:
  - 25 each via @safety_canada and @securite_canada

- 117 re-tweets of our cyber-related messaging:
  - 84 re-tweets of @safety_canada content
  - 33 re-tweets of @securite_canada content

- Organizations that re-tweeted our cyber-related content include:
  - Office of the Privacy Commissioner
  - Canadian Resource Centre for Victims of Crime
  - New Brunswick Crime Stoppers
  - London Drugs

# Cyber Security Awareness Month – Twitter Activity

- 192 new followers were gained during the month of October, many of which can most likely be attributed to Cyber Awareness tweets
  - 149 new followers to @safety_canada
  - 43 new followers of @securite_canada
  - Many of the new followers represent previously unengaged demographics

- For every 5 tweets issued from the @safety_canada account, an estimated 2,682 people are reached.*
- For every tweet issued from the @securite_canada account, an estimated 135 people are reached.*

*Note: TweetReach software was used to determine these estimates.

# GetCyberSafe Website Activity

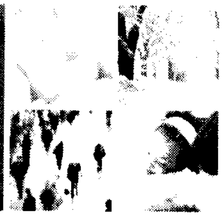
- Monthly Totals:
  - Page Views: 429,405
  - Total Hits: 7,461,661 *
  - Average page views per visitor: 2.81
  - Visitors: 152,896

- Average Daily Totals
  - Average Page Views per day: 13,851
  - Average Hits per day : 240,698 *
  - Average Visitors per day: 4,932

NOTES:

- One webpage does not equal one "hit". A hit is a request to a web server for a file (web page, image, Javascript, Cascading Style Sheet, etc.). When a web page is uploaded from a server the number of "hits" is equal to the number of files requested.
- Three days of traffic are absent due to technical difficulties: Thu 20/10/2011, Fri 21/10/2011, Sat 22/10/2011

# GetCyberSafe Website Activity



Most Popular Pages:

- Using Wi-Fi Networks
- Homepage
- Using Passwords
- Identity 101
- Quiz Results
- Email
- Banking and Finance

Multimedia:

- Video was requested 824 times
- Radio ad was requested 420 times

# GetCyberSafe Website Activity – Web Traffic Details

- More than 86% of all traffic is from desktop or laptop computers

- More than 7% of all traffic is from mobile browsers (tablets, smart phones)
  - This is higher than most .gc.ca. websites

- Most keywords searches include variations of the domain name
  - Search is likely to shift to subpage terms over time

# GetCyberSafe Website Activity – Partner Participation

- The GetCyberSafe button appeared on several other federal government websites including:
  - Treasury Board Secretariat
  - FightSpam.gc.ca (Industry Canada)
  - Correctional Service Canada
  - Canadian Security Intelligence Agency
  - Department of Fisheries and Oceans
  - Heritage Canada
  - Justice Canada
  - Human Resources and Social Development Canada.
- GetCyberSafe buttons also appear on the Government of British Columbia and Newfoundland and Labrador websites, and the Canadian Bankers Association added a link from their site

# Advertising – Media Buy

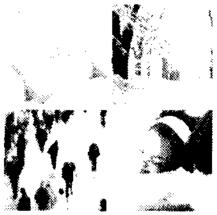
**Throughout the Month, a series of advertisements ran nationally:**

- **Banner Ads (multiple sizes)**
  - MSN Canada (incl. Homepage Takeover)
  - Yahoo! Canada (incl. Homepage Takeover)
  - Yahoo! Quebec
  - Xbox Live
  - CTV
  - Facebook
- **Mobile Banner Ads**
  - Sympatico network
- **Pre-Roll Videos**
  - MSN Canada
  - CTV Shows
- **Radio**

# Advertising – Online Clickthrough Rates

- Nearly **177,000 clicks** to GetCyberSafe.ca were generated through online advertising:
  - **CPM English:** CTR 0.052%
  - **CPM French:** CTR 0.065%
  - **Witnessing-only English (incl. Mobile):** CTR 0.862%
  - **Witnessing-only French (incl. Mobile):** CTR 2.484%
  - **Facebook English:** CTR 0.03%
  - **Facebook French:** CTR 0.04%

# Looking Ahead



## *Cyber Security Awareness Month 2012*

- Planned focus will be on delivering a national roll-out that highlights themes and week-by-week activities, including regional events, and will be informed by other documents like the partnership strategy and three-year look ahead.

- Consistent with the overall direction of the cyber security public awareness campaign, Cyber Security Awareness Month will have an increased focus on activities with partners, including the private sector, provinces and territories, and international allies.

s.19(1)

## FPT Cyber Contacts

| *Region* | *Contact name* | *Title / Office* | *Phone* | *Email* |
|---|---|---|---|---|
| British Columbia | Trace Muldoon | Manager, Security Awareness Information Security Branch, Office of the Chief Information Officer | 250-356-1890 | Trace.Muldoon@gov.bc.ca |
| | Stu Hackett | Chief Information Security Officer<br>Information Security Branch,<br>Office of the Chief Information Officer | [redacted] | [redacted] |
| Alberta | Tim McCreight | | | tim.mccreight@gov.ab.ca |
| Saskatchewan | [redacted] | [redacted] | [redacted] | [redacted] |
| | Art Jones | Communications Manager,<br>Ministry of Corrections, Public Safety and Policing | 306-787-8606 | art.jones@gov.sk.ca |
| Manitoba | Deborah Kiel | Coordinator, Advertising and Program Promotion<br>**Communications Services Manitoba** | 204-945-3812 | [redacted] |
| Ontario | Robert Chiarelli | Sr. Manager, Corporate Security Branch<br>Office of the Corporate CIO | 416-327-3362 | rob.chiarelli@ontario.ca |
| Québec | [redacted] | | | [redacted] |
| | | | | |
| New Brunswick | Steven Pyett | | | steven.pyett@gnb.ca |
| Prince Edward Island | Scott Cudmore | Director, Enterprise Architecture Services, ITSS | | fscudmore@gov.pe.ca; |
| | Erin Mitchell | Director of Policy, Policing and Crime Prevention<br>Department of Justice & Public Safety | 902-368-6619 | etmitchell@gov.pe.ca |
| Nova Scotia | Wallace Peers | Provincial IT Security Authority<br>Chief Information Office | [redacted] | [redacted] |

Last updated: 06/01/2012 3:26:00 PM

s.19(1)

| | | | | |
|---|---|---|---|---|
| Newfoundland and Labrador | Alison Randal | | | AlisonRandell@gov.nl.ca |
| Northwest Territories | [redacted] | [redacted] | [redacted] | [redacted] |
| Yukon Territory | Aisha Montgomery | | | aisha.montgomery@gov.yk.ca |
| | Shane Horsnell | | | shane.horsnell@gov.yk.ca |
| Nunavut | | | | |

rob.chiarelli@ontario.ca; [redacted] Trace.Muldoon@gov.bc.ca; [redacted]; AlisonRandell@gov.nl.ca;
[redacted] fscudmore@gov.pe.ca; jetmitchell@gov.pe.ca; [redacted]
aisha.montgomery@gov.yk.ca; shane.horsnell@gov.yk.ca; steven.pyett@gnb.ca; tim.mccreight@gov.ab.ca; [redacted]
[redacted] art.jones@gov.sk.ca

Last updated: 06/01/2012 3:26:00 PM

Page 33

is a duplicate

est un duplicata

Page 34

is a duplicate

est un duplicata

# London Conference on Cyberspace
# November 1-2, 2011
# Key Take Aways

The conference brought together more than 700 participants from 60 countries, representing senior government officials, industry leaders, and representatives of the Internet technical community and civil society, to begin a dialogue on principles for governing behaviour in cyberspace. The Conference focussed on the five topics highlighted below.

- The dialogue presented an alternative way forward to counter proposals for creating an international treaty to govern cyberspace. This was an important step as it provided an alternative to the treaty regime being proposed by countries such as Russia and China. Until the Conference, countries opposed to the treaty approach, e.g. Canada, the United Kingdom, United States, Australia and New Zealand, were unable to offer an alternative to Russian and Chinese proposals.

- The conference recognized the critical role that the Internet plays as an engine and facilitator of **economic growth and development**, especially in the developing world. Particular focus was given to the benefits of broadband access, and to a secure and reliable cyberspace that is free from government and commercial censorship, consistent with international legal obligations. Recognition was given to the existing work on the Internet and growth by groups such as the Organisation for Economic Co-operation and Development (OECD), and to work in the Council of Europe. The focus of future activity should build on existing work rather than creating new institutions.

- On the theme of **social benefits**, all delegates reaffirmed the overwhelmingly positive and transformative benefits that the Internet has brought to citizens, societies and governments. Emphasis was given to the importance of engaging the youth community and the conference agreed that efforts to improve cyber security must not be achieved at the expense of human rights.

- Participants discussed **international security** issues and underlined the importance of the principle that governments act proportionately in cyberspace. Also underscored was the belief that states should continue to comply with existing rules of international law and the traditional norms of behaviour that govern interstate relations.

- Recognition was given to the significant threat to economic and social well being from **cyber crime** and the requirement for a concerted and urgent international effort to address this problem. This was an area where delegates expressed strong support for practical collaboration and capacity development on cross border law enforcement. Comments were heard that addressing cyber crime is not only the responsibility of government, but that industry has a shared responsibility to do more to prevent cyber crime for example through more secure devices, systems and services.

- The European Convention on Cybercrime (the Budapest Convention) was acknowledged as the best existing model for addressing cyber crime. Even if states are unable or unwilling to sign up to the Convention, they were encouraged to adopt the practical measures outlined in the Convention such as the establishment of 24 hours points of contact for police investigating cyber crime cases. Canada has not yet ratified the Convention, although it did sign it in October, 2001.

- There was general agreement that **ensuring safe and reliable access** to global interoperability and resilience underpins the economic and social benefits of the Internet and that governments, industry and civil society must work together to preserve and enhance them.

- A consistent message was the need for increased public-private engagement in matters relating to cyberspace. This engagement has to occur both at the national and international level.

- Confidence building measures between nation states are required to avoid missteps in cyberspace in much the same way these were used during the Cold War. Delegates welcomed the work the Organization for Security and Co-operation in Europe (OSCE) is doing to develop specific confidence building measures applicable in cyber space.

- In discussing Internet governance, speakers voiced different opinions on the role of government versus civil society. One speaker in particular warned that the Internet will be the age of people not the government and that the young want to get rid of the barriers imposed by governments. For the youth, "the world of the Internet is the real world, not the fake world of the government".

- Countries, such as the Netherlands, are establishing new mechanisms to provide advice to national governments on strategic issues relating to cyberspace. Recent cyber attacks have been a wake up call for both government and industry. In the case of the Netherlands, they have created a Cyber Security Council, comprised of private sector executives and senior government officials. In January 2012, the Netherlands will launch a National Cyber Security Centre to facilitate government, private sector and academia to share information and analysis on new cyber trends and threats. There may be an opportunity for Canada to participate with the Netherlands in their initiatives.

Public Safety Canada    Sécurité publique Canada

RCMP·GRC

# Protecting Canada's Critical Infrastructure: 2012 SCADA and Industrial Control Systems Security Workshop Montréal, Québec

**Dates**

January 31 2012 – February 1 2012

**Event details**

The workshop is a two-day training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators better secure their most critical SCADA and industrial control system and information technology assets.

Recognized experts along with representatives from the federal Government will provide briefs on the latest threats and steps that can be taken to increase the security of SCADA and industrial control systems.

**Benefits of attending**

- ✓ Gain a greater awareness of the threats to SCADA and industrial control systems and how to defend against them
- ✓ Learn about what resources are available to assist organizations
- ✓ Learn the challenges of securing control systems and arm yourself with case studies showing what others have done and the lessons they have learned
- ✓ Learn about some of the latest research activities
- ✓ Exchange information and ideas in a trusted environment with other control systems owners and operators
- ✓ Better understand the role of government and its current capabilities

**Technical level**

The training is lecture style (hands-off) but technical in nature and takes place at the intermediate to advanced level.

**Who should attend**

- ✓ Plant Managers, Engineering and Operations Management, Project Managers, Automation and Control Managers, Process Control and SCADA Engineers, Plant Engineers
- ✓ Information Security and IT Professionals in Organizations that Deploy Industrial Control Systems
- ✓ Control System Vendor Developers and Integrators
- ✓ Government Leaders Responsible for Policy and Regulation of Utilities and Other Process Control Users
- ✓ Academic and Research Laboratory Leaders

Public Safety Canada Sécurité publique Canada

RCMP·GRC

**Speakers**

- ✓ Public Safety Canada
- ✓ Canadian Cyber Incident Response Centre
- ✓ Royal Canadian Mounted Police
- ✓ Department of Homeland Security Control Systems Security Program (to be confirmed)
- ✓ Federal Bureau of Investigation (to be confirmed)
- ✓ Canadian Security Intelligence Service
- ✓ Defence Research and Development Canada
- ✓ Mark Fabro, President and Chief Security Scientist, Lofty Perch

**Topics**

- ✓ Threats and vulnerabilities
- ✓ Incident management and forensics analysis
- ✓ Architecture and operation best practices
- ✓ Emerging research
- ✓ Security technologies and standards
- ✓ Red and blue team training exercise overviews
- ✓ Procurement standards and best practices

**Cost**

There is no cost for entry to the workshop. All other costs are the responsibility of the attendee.

**Venue**

Palais des congrès de Montréal
1001 Place Jean-Paul-Riopelle, Montréal, Quebec
Room 513 ABC
Phone: 514-871-8122
Fax: 514-871-9389
info@congresmtl.com
www.congresmtl.com

**Application to attend**

Due to the sensitive nature of some of the material presented entry to the workshop will be restricted to approved participants. The workshops are limited to 150 participants.

To register send the following information to the contacts provided below.

- ✓ Name
- ✓ Position title
- ✓ Organization
- ✓ Email address
- ✓ Telephone number
- ✓

**Contact**

Lukasz Johaniuk
613-991-3643
lukasz.johaniuk@ps-sp.gc.ca

Allison Araneta
613-993-8258
allison.araneta@ps-sp.gc.ca

Pages 39 to / à 42

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14

of the Access to Information

de la Loi sur l'accès à l'information

Pages 43 to / à 51

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Def, 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

s.19(1)

10/03/2012

550 280

From: Weir, Sarah On Behalf Of Dick, Robert

To: [redacted] [redacted] [redacted]
kate.rozmahel@gov.ab.ca; [redacted] tim.mccreight@gov.ab.ca;
[redacted] ; dmlg@leg.gov.mb.ca; [redacted]
[redacted]
Rob.Chiarelli@Ontario.ca; carl.rajack@ontario.ca; [redacted]
[redacted]
[redacted] rick.ouellette@gnb.ca; jamie.rees@gnb.ca;
etmitchell@gov.pe.ca; mjmuise@gov.pe.ca; UNDERWPC@gov.ns.ca;
[redacted] tenglish@gov.nl.ca; paulscott@gov.nl.ca;
AlisonRandell@gov.nl.ca; shane.horsnell@gov.yk.ca; [redacted]
[redacted]

Cc: Dick, Robert; Durand, Stéphanie; Labelle, Sébastien; Anderson, Windy

Subject: *FPT Cyber Security Teleconference Follow-up / Suivi appel téléconférence FPT la cybersécurité*

Dear colleagues,

As promised on our last call, please find attached a DRAFT Memorandum of Understanding (MOU) for the Sharing and Protection of Information. The MOU has also been shared with the National Chief Information Officer Subcommittee on Information Protection (NCSIP) membership. Please review the MOU and indicate your views to Sébastien Labelle, Director, Partnership and Engagement at (613) 990-2665 as soon as practicable.

The MOU will also be discussed at our next teleconference to be held on April 2, 2012, from 2:00 to 3:00 pm (EST).

Thank you,

Robert W. (Bob) Gordon
Special Advisor, Cyber Security / Conseiller spécial, cybersécurité
Public Safety Canada / Sécurité publique Canada
340 Laurier Avenue West / 340 avenue Laurier Quest
Ottawa, Ontario K1A 0P9 / Ottawa (Ontario) K1A 0P8
613 949-7380 Fax/Téléc.: 613 990-3287
E-Mail / Courriel: Robert.Gordon@ps-sp.gc.ca

Chers collègues,

Comme il a été convenu lors de notre dernier appel téléconférence, vous trouverez ci-joint une VERSION PRÉLIMINAIRE du protocole d'entente sur l'échange et la protection des renseignements. Le protocole d'entente a également été partagé avec les membres du le Sous-comité national des DPI sur la protection de l'information (SNPDI). Nous vous demandons de réviser le protocole d'entente et de communiquer vos commentaires à Sébastien Labelle, directeur, Partenariat et mobilisation, au 613-990-2665 le plus rapidement possible.

Une discussion sur le protocole d'entente aura également lieu lors de notre prochain appel conférence qui aura lieu le 2 Avril 2012 de 14 :00 à 15 :00.

Merci.
Robert W. (Bob) Gordon
Special Advisor, Cyber Security / Conseiller spécial, cybersécurité
Public Safety Canada / Sécurité publique Canada
340 Laurier Avenue West / 340 avenue Laurier Quest
Ottawa, Ontario K1A 0P9 / Ottawa (Ontario) K1A 0P8
613 949-7380 Fax/Téléc.: 613 990-3287
E-Mail / Courriel: Robert.Gordon@ps-sp.gc.ca

April 2012

UNCLASSIFIED

# MEMORANDUM OF UNDERSTNADING ON INFORMATION SHARING

(For discussion)

## PROPOSED TALKING POINTS

s.14
s.15(1) - Subv
s.16(2)
s.21(1)(b)
s.23

- I would like to hear any views you may have on the Memorandum of Understanding (MOU) we shared with you ?

- I would like to note that the MOU was As committed, we have shared the draft MOU for We have heard from a few of you about the It is proposed that you seek any preliminary views on the MOU or interest in formalizing the information sharing process. At the same time, it is proposed that you inform the group that a similar MOU has been signed with the Canadian Electricity Association (CEA) and is currently being operationalized.

-

## ISSUE

Discussion of the Memorandum of Understanding (MOU) on information sharing.

## BACKGROUND

Several provinces had expressed an interest in a more formal information sharing mechanism. To respond to this request, Public Safety Canada drafted an MOU for information sharing for provincial and territorial input and comments. The draft MOU was sent to the members of the National Chief Information Officer Subcommittee on Information Protection (NCSIP) on February 17, 2012, and the ADM level FPT Committee on Cyber on March 19, 2012.

## CONSIDERATIONS

The MOU will enable the sharing of operational information between Canadian Cyber Incident Response Centre (CCIRC) and other levels of government, deepening existing relationships and facilitating risk management activities. The effectiveness of these risk management activities depend on the degree to which different levels of government share accurate, useful and timely information. The MOU has been approved by Public Safety's Legal Services, and is attached (**TAB A**).

## CURRENT STATUS

[redacted]

[redacted]

An MOU for information sharing has been signed with the Canadian Electricity Association and the agreement is being implemented.

## CONCLUSION

Ideally, MOUs would be signed by interested provinces and territories before end of April, 2012.

Prepared by: Semira Selman
Approved by: Sébastien Labelle

Pages 56 to / à 60

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14

of the Access to Information

de la Loi sur l'accès à l'information

**UNCLASSIFIED**

DATE:

File No.:383236
RDIMS No.:487791

## MEMORANDUM FOR THE ASSISTANT DEPUTY MINISTER

## NEXT CYBER SECURITY TELECONFERENCE WITH PROVINCES AND TERRITORIES

(Decision sought)

### ISSUE

To seek your approval to hold the next teleconference call proposed for November 16, 2011, with provincial and territorial cyber interlocutors.

### BACKGROUND

The last teleconference call with provinces and territories took place on August 3, 2011. Bob Gordon, Senior Advisor, chaired the call on your behalf. A high level summary of the meeting is enclosed (**TAB A**). While they expressed concerns over capacity issues, provinces and territories agree on the importance of working together on cyber security and have expressed an interest in holding regular meetings to maintain momentum and move issues forward.

### CURRENT STATUS

Federal, provincial, and territorial Clerks and Cabinet Secretaries met via videoconference on September 23, 2011. At the instigation of the British Columbia co chair, cyber security was proposed and accepted as an agenda item for their January 2012 meeting. This portion of the meeting will include:

1) a discussion on the common public sector management challenges such as contingency planning and roles and responsibilities across jurisdictions;
2) an exchange of knowledge and best practices; and,
3) a security briefing on the general threat environment.

.../2

s.14(a)

s.21(1)(b)

We advised our provincial and territorial interlocutors, and the National Chief Information Officer Subcommittee on Information Protection (NCSIP), in advance of the videoconference that cyber security was to be discussed, however, we have not yet shared the outcome. I will be briefing NCSIP in Fredericton, October 26 - 28, 2011.

The Clerks' meeting (item number one in particular) could be a good opportunity to launch a discussion on the need for a national framework for cyber incident management. Such a framework, which would ultimately include the private sector and align with international efforts, is an important mechanism to ensure that in mitigating and responding to incidents, roles, responsibilities, protocols and authorities are clear. The United States has a national incident management plan in place that could serve to guide development of a Canadian framework. To build support for this discussion among the provinces and territories, I will be presenting information on the existing emergency management framework, along with an initial assessment of operational gaps a national cyber framework would need to address, at the October meeting of the NCSIP.

It is proposed that a similar discussion be initiated with the provincial and territorial cyber interlocutors at the upcoming teleconference. [redacted] The efforts should be focused on highlighting the gap in the current emergency management framework and building consensus for collaborative work in this area. Collaborating with provinces and territories on these issues would help to frame necessary discussion on legal and policy authorities (and gaps), and jurisdictional roles and responsibilities. A proposed agenda for the teleconference is attached (**TAB B**).

On other fronts, the federal, provincial, territorial communications working group struck by Public Safety Canada's Director General of Communications has begun initial engagement on public awareness efforts. Stéphanie Durand is now working to formalize the collaboration through Terms of Reference.

## RECOMMENDATION

It is recommended that you send the proposed email invitation for the next teleconference call (**TAB C**) to the provincial and territorial cyber interlocutors. Attached to the invitation would be the proposed agenda, annotated look-ahead calendar of key cyber related events, as well as, the guiding principles document for the London Conference.

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Marie Anick Maillé, Director, Engagement and Partnership, National Cyber Security, at 613-990-9379.

Robert Dick
Director General
National Cyber Security

Enclosures: (3)

Prepared by: Semira Selman

I approve:

______________________________

Lynda Clairmont
Assistant Deputy Minister
National Security

Tab A

**Hayward, Jane**

| | |
|---|---|
| **From:** | Gordon, Robert |
| **Sent:** | August-03-11 2:35 PM |
| **To:** | Clairmont, Lynda; Dick, Robert |
| **Cc:** | Coburn, Stacey; Hatfield, Adam; Maillé, Marie Anick; Durand, Stéphanie; Hannan, Andrew |
| **Subject:** | FPT Teleconference onCyber Security, August 3, 2011 |

Today's teleconference call was successful. A more fulsome report and follow-up plan will be prepared for your information.

10 provinces and terrirtories participated - some had advised us in advance that they would be unable to participate. As arranged in advance, Marie Anick will provide feedback to Quebec and PEI representatives who were unable to join the call; the same option will be extended to Nunavut.

Call participants indicated a desire to participate in a number of areas, e.g. serveral expressed strong support and desire to participate with the Communications Branch Public Awareness Campaign - we are already receiving emails from some participants identifying their interlocutors. Suggestions were offered in areas such as: a desire to participate in discussions for future engagement with CCIRC and refining their products; the sharing of a calendar or map of cyber activity, messaging and key cyber security concepts each level is preparing; that we consider methods of working together to engage the academic world with a focus of providing cyber security training; sharing best practices in the training of government employees; exchanging ideas on the impact of the introduction of multiple personal electronic devices into the work-place.

Participants expressed interest in mainitaing the mometum of the group and suggested that a monthly teleconference call with twice yearly meetings. However, none offered to host the next one but we will pursue this directly with some provinces, at this point likely Alberta or BC would be interested.

Bob

Tab B

# *FEDERAL PROVINCIAL TERRITORIAL TELECONFERENCE ON CYBER SECURITY*

**December 15, 2011**
**1:00 p.m. to 2:00 p.m. (Eastern Time)**

**Teleconference**

Local: **613-960-7514**
Toll-free: 1-877-413-4790
Conference leader code: **3444**
Conference code: 9078299

## AGENDA

- Welcome and Confirmation of Agenda
- Situational Awareness (5 minutes) – Windy Anderson
  - Director of CCIRC will provide a quick overview of key cyber threats and events
- Update on Public Awareness Campaign (5 minutes) – Stéphanie Durand
  - Debrief on the work of the FPT communications working group and planned activities for remainder of 2011-12
- January 23, 2012 Meeting of the Clerks (15 minutes) – Bob Gordon and others
  - Provide further information on the upcoming Clerks meeting
  - Propose a review of existing emergency response protocols to assess their applicability for cyber incidents
- Consultations on CCIRC's refocused mandate (5 minutes) - Bob Gordon and others
  - Plans to hold a consultation session in Ottawa on CCIRC's refocused mandate, including services and product offerings
- Information exchange mechanisms (10 minutes) - Bob Gordon and others
  - Propose striking a small working group to develop information sharing mechanisms and protocols (e.g., standard information sharing MOU, common terminology, etc.)
- Gap analysis and action plan (5 minutes) - Bob Gordon and others
  - Discuss developing a gap analysis and an action plan for FPT collaboration on cyber security
- Other items (10 minutes)
  - Debrief on the London Cyber Space Conference – Bob Gordon
  - Update on the control system (SCADA) workshops – Adam Hatfield
- Next Steps /Roundtable (5 minutes)

s.19(1)

Tab C

TO: [redacted]
kate.rozmahel@gov.ab.ca; [redacted] tim.mccreight@gov.ab.ca;
[redacted] dmlg@leg.gov.mb.ca; [redacted]
[redacted] Rob.Chiarelli@Ontario.ca;
carl.rajack@ontario.ca; [redacted]
[redacted] rick.ouellette@gnb.ca; jamie.rees@gnb.ca;
etmitchell@gov.pe.ca; mjmuise@gov.pe.ca; UNDERWPC@gov.ns.ca;
[redacted] tenglish@gov.nl.ca; paulscott@gov.nl.ca;
AlisonRandell@gov.nl.ca; shane.horsnell@gov.yk.ca; [redacted]
[redacted] (currently no rep for Nunavut)

CC: DG Communications, Director of IGA

Dear Colleagues,

I would like to invite you to a teleconference on December 15, 2011, from 1:00 to 2:00 pm. We would like to debrief you on the outcome of the London Conference on cyber security norms and values, discuss the upcoming FPT Clerks and Cabinet Secretaries meeting, and propose next steps for FPT collaboration. A formal agenda, documents and dial-in information will follow.

Should you have any questions, please do not hesitate to communicate with Sébastien Labelle, Director of National Cyber Security Engagement and Partnerships at Sebastien.Labelle@ps-sp.gc.ca or (613) 990-2655 or Robert Dick, Director General, National Cyber Security at Robert.Dick@ps-sp.gc.ca or 613-990-2661.

I look forward to our continued collaboration in the area of cyber security.

Kind regards,

Bob Gordon, Special Advisor, Cyber Security

## AGENDA ITEM: FPT CLERKS MEETING

(For discussion)

### DESIRED OUTCOME

Provide additional information on the FPT Clerks meeting and secure support for the following outcomes:

- continued/increased intergovernmental collaboration on strategic, operational and communications issues; and,
- recommendation to review the existing emergency response protocols to assess their applicability for cyber incidents.

### PROPOSED TALKING POINTS

- As you may recall, the FPT Clerks meeting is coming up on January 23, 2012. The Clerks want a deeper understanding of the cyber security issues and would like to know that should a significant cyber event occur we would be able to effectively respond.
- To that end, we plan to provide the Clerks with an all hazards threat brief and a specific cyber security brief to ensure a common understanding of the threats and risks.
- Beyond that, we are seeking your support to brief up to your Clerks encouraging them to support intergovernmental collaboration on cyber security, and more specifically, to suggest a review of how a major cyber incident would be handled nationally.
- There is a lot of structure in place for emergency management, however, there is a need to better understand these structures and how cyber fits within them.
- We also need to establish better linkages with existing FPT committees on emergency management and critical infrastructure.
- I would like to hear your thoughts on this.

s.14(a)

s.19(1)

s.21(1)(a)

[redacted]

- Federally, we will conduct table top exercises beginning January, 2012, to ensure that the federal government can support cyber incident response on non-federal systems in a coordinated manner.
- Related to this work, we will need to better understand what information you need to protect your systems. We will be bringing a few provincial representatives identified at the October NCSIP meeting, including Rick Ouellette, Tim McCreight, Stu Hackett, Carl Rajack and [redacted] to consult on CCIRC's products and services. Not all of you were represented at that meeting so, if you are interested, please let me know– we can discuss this shortly.

## BACKGROUND

FPT clerks are meeting on January 23, 2012. Among other topics of discussion, cyber security is on the agenda at the request of provincial Clerks. PCO has invited the Director of CSIS to

s.19(1)
s.21(1)(a)

provide an overall threat briefing, while the head of CSEC will present the cyber-specific threat environment.

A total of one hour is set aside for the item, which will allow for a general discussion on the emerging threats, and provide the opportunity to discuss broader FPT engagement on cyber security including a need to review how a cyber incident would be handled at a national level.

## CONSIDERATIONS

This will be the first time the issue of emergency response for cyber incidents is brought up in this context – Robert Dick had presented to the National Subcommittee on Information Protection (NCSIP) in October on this issue. The reaction from the NCSIP group was positive with indication that it exceeds the scope of their mandate. A key challenge will be to ensure that the provincial emergency management leads are brought into this discussion. A number of the NCSIP members are also cyber interlocutors (B.C. Stu Hackett, AB Tim McCreight, [redacted] ON Carl Rajack, [redacted], N.B. Rick Ouellette, N.S. Wallace Peers, NU Fred Ruthven).

[redacted]

It will be important to note that we are also working with key federal partners to ensure clear roles and responsibilities and capacity to respond and assist to cyber incidents on non-government systems. To this end, Technical Advice is running a number of table top exercises with CCIRC, RCMP, CSIS and CTEC at Director, DG and ADM levels beginning January 13th to identify any potential gaps that would need to be addressed to ensure a coordinated response.

## CURRENT STATUS

Within NCSD, Kent Schramm has been identified as the lead on the development of the national cyber incident response framework. If provinces agree to undertake work in this area, as a first step, he will be meeting with those with more mature cyber security operations to discuss moving forward. It is expected that the development and validation of the framework would take approximately 18 months.

## CONCLUSION

Securing PT agreement to work collaboratively on development of a national cyber incident response framework would achieve a number of objectives:

- a key deliverable for FPT collaboration;

- clarity on roles and responsibilities;
- improved information sharing; and,
- enhanced cooperation with critical infrastructure sectors and municipalities.

# AGENDA ITEM: CONSULTATION ON CCIRC's REFOCUSED MANDATE

(For information and discussion)

## DESIRED OUTCOME

- Identify four provinces to take part in consultations on CCIRC's refocused mandate.

## PROPOSED TALKING POINTS

- As you are aware, since the launch of *Canada's Cyber Security Strategy* there have been significant realignments of roles and responsibilities for cyber incident management on Government of Canada systems.
- CCIRC continues to be the national Computer Emergency Response Team (CERT), but responsibility for incidents internal to the federal government has been transferred to CSEC.
- CCIRC's mandate has been refocused on national stakeholders including provinces and territories, and critical infrastructure owners and operators.
- To ensure we can partner with you and CI sectors as effectively as possible, we will hold a two day consultation session in Ottawa early in 2012 with key provincial volunteers, I had mentioned them earlier, and priority critical infrastructure sector representatives to help us identify needs and prioritize services.

## BACKGROUND

Since the launch of Canada's Cyber Security Strategy (the Strategy) in October 2010, there has been a significant realignment of roles and responsibilities for incident management on Government of Canada systems. CCIRC's mandate has been refocused on national stakeholders. It continued to play the national Computer Emergency Response Team (CERT) function.

CCIRC's priority clients for service provision are provinces and territories, critical infrastructure (CI) owners and operators with initial focus on the following initial priority sectors: telecommunications, finance and energy. CCIRC can provide situational awareness products and/or assistance to mitigate and respond to cyber security incidents.

## CONSIDERATIONS

CCIRC's proposed vision and mandate are in line with international CERT standards, i.e., focal point for reducing cyber risk to critical national assets, responding effectively to cyber threats or attacks against these assets and maintaining the trust relationship with national and international partners that is so vital to effective cyber operations.

While CCIRC role is clear, there is a need to consult with key stakeholders to secure agreement that the role is valid and complete, seek views on how it is implemented (e.g., services and products to be offered), and to prioritize service offerings to ensure best use of limited resources.

## CURRENT STATUS

Technical Advice, in consultation with CCIRC, is leading the development of formal articulation of CCIRC's vision and mandate. This work will be finalized in January 2012. Once formalized, it will be used to guide consultations with key stakeholders, including provinces and territories.

## CONCLUSION

Engaging with provinces and territories, and other key stakeholders, on CCIRC's refocused mandate will help meet two objectives:

- ensure that CCIRC has the buy in and cooperation (particularly on information exchange) to fulfill its national CERT mandate; and,
- is seen as a trusted and value added security partner by providing products and services that meet stakeholder needs.

s.14(a)

**CLASSIFICATION**

## AGENDA ITEM: PUBLIC AWARENESS CAMPAIGN

*(Update item)*

### ISSUE

Stephanie Durand will provide a brief update on activities related to the launch of the Get Cyber Safe public awareness campaign and related work with partners, including the provinces and territories.

### BACKGROUND

Communications provided an update on the campaign during the August conference call with the provinces and territories. The last conference call for the FPT Cyber Communications Working Group occurred on September 16, 2011. The next call for this Working Group is scheduled for January 10, 2012.

### CONSIDERATIONS

Only brief, summary details will be provided during this update, given that the FPT Cyber Communications Working Group will be holding its next conference call shortly after this one.

[redacted]

Some provinces and territories did help promote the launch of the Get Cyber Safe campaign through links and Web buttons on their respective sites.

### CURRENT STATUS

As reflected in the attached draft agenda, the primary topics to be discussed during the next FPT Cyber Communications Working Group conference call will be a summary of the campaign launch and Cyber Security Awareness Month, Terms of Reference for the Working Group, and proposed objectives and deliverables for the Working Group through December 2012. (A related deck will be circulated just prior the next FPT Cyber Communications Working Group call.)

### CONCLUSION

Provincial and territorial officials on this call, some of whom are contacts for the FPT Cyber Communications Working Group, should welcome an update on Get Cyber Safe but will be interested to know more about their involvement as the campaign moves forward.

Pages 74 to / à 75

are withheld pursuant to sections

sont retenues en vertu des articles

14(a), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

## AGENDA ITEM: INFORMATION EXCHANGE MECHANISMS

(For discussion)

### DESIRED OUTCOME

- PTs agree to review draft Memorandum of Understanding on information sharing.

### PROPOSED TALKING POINTS

- We had been approached by the Canadian Electricity Association to establish a Memorandum of Understanding (MOU) for information sharing. We are finalizing this agreement.
- Given that a number of you have indicated interest in establishing arrangements for information sharing, both classified and unclassified; we will begin by looking at this MOU as a template that could be used with all external partners for unclassified information sharing. In the New Year, we will share a draft MOU for information sharing for your input and comments.
- We hope this will be a starting point for further discussion on this issue. In the meantime, we will also be looking at the issue of classified information sharing.
- At the same time, we will continue to share valuable information as we did at the NCSIP meeting in October.

### BACKGROUND

Provinces and territories have raised enhanced information exchange as one of the key issues requiring intergovernmental collaboration. Better information exchange would also allow CCIRC to fulfill its mandate as it relies on external partners to voluntarily share information.

s.13(1)(c)

s.14(a)

s.19(1)

s.21(1)(a)

s.23

## CONSIDERATIONS

[redacted]

## CURRENT STATUS

[redacted]

[redacted]

NCSD is currently in the process of finalizing an MOU on unclassified information sharing that will be implemented with the Canadian Electricity Association on a pilot basis. [redacted]

## CONCLUSION

Moving forward on enhanced information sharing with PTs will address one of the key issues identified and support overall objectives for intergovernmental collaboration on cyber security.

s.19(1)

[redacted]

# Cyber interlocutors and coordonators

| | |
|---|---|
| [redacted] | |
| **Kate Rozmahel**<br>Assistant Deputy Minister<br>Corporate Chief Information Officer<br>Service Alberta | AB |
| [redacted] | |
| **Stu Hackett**<br>Chief Information and Security Officer<br>Ministry of Citizens' Services | BC |
| [redacted] | |
| **Rick Ouellette**<br>Corporate Information Security Officer<br>Department of Supply and Services | NB |
| **Tracy English**<br>Assistant Deputy Minister<br>Intergovernmental Affairs Secretariat<br>Executive Council | NL |
| [redacted] | |
| **Dave Heffernan**<br>Chief Information Officer<br>Department of Finance | NT |
| [redacted] | |

# PT CYBER SECURITY INTERLOCUTORS LIST

| Name and title | P/T | Coordinates | Status | Teleconference | |
|---|---|---|---|---|---|
| | | | | R | C |
| [redacted] | [redacted] | [redacted] | I | | |
| **Kate Rozmahel**<br>Assistant Deputy Minister<br>Corporate Chief Information Officer<br>Service Alberta | AB | kate.rozmahel@gov.ab.ca | I | R | |
| [redacted] | [redacted] | [redacted] | S | | |
| **Tim McCreight**<br>Executive Director<br>Corporate Information Security Office<br>Service Alberta | AB | tim.mccreight@gov.ab.ca | S | R | |
| [redacted] | [redacted] | [redacted] | I | | |
| **Stu Hackett**<br>Chief Information and Security Officer<br>Ministry of Citizens' Services | BC | [redacted] | I | R | |
| [redacted] | [redacted] | [redacted] | I | | |
| [redacted] | [redacted] | [redacted] | S | R | |

| | | | | |
|---|---|---|---|---|
| [redacted] | | | S | R |
| **Rick Ouellette**<br>Corporate Information Security Officer<br>Department of Supply and Services | NB | rick.ouellette@gnb.ca | I | |
| **Jamie Rees**<br>Senior Security Architect<br>Department of Supply and Services | NB | jamie.rees@gnb.ca | S | |
| **Tracy English**<br>Assistant Deputy Minister<br>Intergovernmental Affairs Secretariat<br>Executive Council | NL | tenglish@gov.nl.ca | I | |
| **Alison Randell**<br>Director<br>Information Protection, Information Management Branch<br>Office of the Chief Information Officer<br>Executive Council | NL | AlisonRandell@gov.nl.ca | S | R |
| [redacted] | | | I | |
| **Wallace Peers**<br>Provincial IT Security Authority<br>Chief Information Office | NS | [redacted] | S | |
| **Dave Heffernan**<br>Chief Information Officer<br>Department of Finance | NT | Dave_Heffernan@gov.nt.ca | I | R |
| [redacted] | | | I | |

| | | | | | |
|---|---|---|---|---|---|
| [redacted] | | | I | | [redacted] |
| **Carl Rajack**<br>Senior Manager<br>IT Security Operations<br>Office of the Corporate Chief Information Officer<br>Ministry of Government Services | ON | carl.rajack@ontario.ca | S | | [redacted] |
| **Robert Chiarelli**<br>Senior Manager<br>Corporate Security Branch<br>Office of the Corporate Chief Information Officer<br>Ministry of Government Services | ON | Rob.Chiarelli@Ontario.ca | S | R | [redacted] |
| [redacted] | | | I | | [redacted] |
| **Mike Muise**<br>Manager<br>Office of Information Protection<br>Finance and Municipal Affairs | PE | mjmuise@gov.pe.ca | S | | [redacted] |
| [redacted] | | | I | | [redacted] |
| [redacted] | | | S | R | [redacted] |

| | | | | |
|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | S | |
| [redacted] | [redacted] | [redacted] | I | |
| [redacted] | [redacted] | [redacted] | I | |
| **Shane Horsnell**<br>Director<br>Technology Infrastructure and Operations<br>Information & Technology Division<br>Highways adn Public Works | YK | shane.horsnell@gov.yk.ca | S | |

s.13(1)(c)
s.14(a)
s.21(1)(a)
s.21(1)(b)

May 2011

**UNCLASSIFIED**

DATE:

File No.:
RDIMS No.: 416549

**MEMORANDUM FOR THE ASSISTANT DEPUTY MINISTER**
c.c.: Robert Dick, Cyber Security

## FOLLOW UP ON THE FEDERAL/PROVINCIAL/TERITORIAL MEETING ON CYBER SECURITY

(For Action by May 12, 2011)

## ISSUE

To follow up on the federal/provincial/territorial meeting on cyber security you chaired in Ottawa on March 29, 2011.

## BACKGROUND

A key objective of the meeting was to identify priority areas for federal/provincial/territorial collaboration on cyber security; however, due to elections, this discussion did not take place. The provinces and territories did however raise a number of ideas that are helping us to shape where we need to focus our collective and individual efforts [redacted]

The atmosphere of the meeting was fairly positive and the provinces and territories echoed our commitment to cyber security as an important public policy priority and one that needs to be addressed jointly. [redacted]

The meeting also highlighted a number of key differences among provinces and territories that will need to be managed as we move forward; namely the:

.../2

s.14(a)

s.21(1)(a)

- diverse nature of the provincial/territorial cyber interlocutors - spanning from intergovernmental relations to technical experts; and,
- different needs, challenges, capacities and governance approaches to cyber security across jurisdictions.

## CONSIDERATIONS

[redacted]

Page 87

is withheld pursuant to sections

est retenue en vertu des articles

14(a), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

Phase 3: Implementation and Measuring Success

Phase 3 [redacted]

## RECOMMENDATION

To ensure momentum on federal/provincial/territorial engagement on cyber security, it is recommended that you send the attached follow up email to your colleagues (**Annex A**) as soon as possible.

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Ms. Marie Anick Maillé, Manager, Cyber Engagement and Partnerships at 613-990-9379.

Robert Dick

Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

Enclosure: (1)

s.14(a)
s.21(1)(a)

UNCLASSIFIED

DATE:

File No.:

**MEMORANDUM FOR THE ASSISTANT DEPUTY MINISTER**
c.c.: Robert Dick, Cyber Security

## FOLLOW UP ON THE FEDERAL/PROVINCIAL/TERITORIAL MEETING ON CYBER SECURITY

(For Action)

## ISSUE

Follow up on the March 29, 2011 federal/provincial/territorial meeting on cyber security held in Ottawa.

## BACKGROUND

On March 29, 2011 you chaired a federal/provincial/territorial meeting on cyber security. The purpose of the meeting was to discuss challenges, identify gaps and pressures within jurisdictions related to cyber security.

A number of ideas and issues were raised during the discussions [redacted]

The meeting discussions will help support the development of a common federal/provincial/territorial agenda on cyber security.

## CURRENT STATUS

To ensure momentum on federal/provincial/territorial engagement on cyber security, it is recommended that you send a follow up email to the provinces and territories (please see Annex A). The email reiterates federal commitment to working together on cyber security. The email shows immediate action on the part of the federal government to address some of the issues raised at the meeting including commitment for more effective incident reporting through the Canadian Cyber Incident Response Centre (CCIRC), commitment to engage provincial and territorial cyber interlocutors in developing public awareness efforts and sponsoring provincial and territorial officials' security clearances.

s.14(a)
s.21(1)(a)
s.21(1)(b)

The email also proposes next steps for federal/provincial/territorial engagement on cyber security. Based on input to date, it is proposed that Public Safety Canada take the lead on the development of a draft federal/provincial/territorial action plan which will identify objectives, activities and timelines. This draft action plan will be shared with the provinces and territories at the end of May for their input and review. A federal/provincial/territorial teleconference is proposed for June to discuss the draft agenda and next steps.

## CONSIDERATIONS

Discussions with provinces and territories have been positive and informative; [redacted]

While it is clear that provinces and territories have differing needs, challenges, capacities and governance approaches to cyber security, there is strong interest in pursuing partnership efforts. [redacted]

## CONCLUSION

Please find attached a draft of the proposed email to be sent to provincial and territorial partners (Annex A), as well as, the security clearance documentation (Annex B). Given the need to maintain momentum, it is recommended that the email be sent as soon as possible.

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Ms. Marie-Anick Maillé, Manager, Cyber Engagement and Partnerships at 613-990-9379.

Robert Dick

Enclosure: (2)

s.14(a)
s.21(1)(a)

**UNCLASSIFIED**

DATE:

File No.: 379689
RDIMS No.: 420804

## MEMORANDUM FOR THE ASSISTANT DEPUTY MINISTER

## NEXT STEPS FOR ENGAGEMENT WITH PROVINCES AND TERRITORIES ON CYBER SECURITY

(Decision sought)

### ISSUE

To seek your approval on the proposed next steps for engaging with provinces and territories on cyber security.

### BACKGROUND

Bilateral discussions and the federal/provincial/territorial meeting on cyber security you chaired in Ottawa on March 29, 2011, were generally positive and provided the required buy-in to move ahead with more substantive engagement: all parties agreed on the importance of cyber security and on the need for better intergovernmental collaboration. However, given the federal election, you were unable to conclude discussions or identify priority areas for future collaboration as intended.

### CONSIDERATIONS

The short and medium term objectives for engaging with provinces and territories on cyber security are to:

[redacted]

…/2

Page 93

is withheld pursuant to sections

est retenue en vertu des articles

14(a), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

s.14(a)
s.21(1)(a)

[redacted]

Regular meetings would cement the relationship and allow us to move the agenda forward. This could include an in-person meeting on a bi-annual basis, and teleconference calls and working group meetings as required. The first of these meetings could be held in November, 2011.

## RECOMMENDATION

It is recommended that you approve the suggested approach for continued engagement with provinces and territories on cyber security. This approach has been discussed and positively received by our key partners, namely, the Canadian Cyber Incident Response Centre, the Communications Directorate, the Intergovernmental Affairs Division, the Regional Operations Directorate, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the Treasury Board Secretariat.

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Ms. Marie Anick Maillé, Manager, Cyber Engagement and Partnership at 613-990-9379.

Robert Dick

Enclosures: (3)

Prepared by: Semira Selman

I approve:

____________________________________

Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

s.21(1)(a)

# "QUICK HITS" IDENTIFIED BY PUBLIC SAFETY CANADA

- **Sponsor security clearances:** Public Safety Canada will sponsor secret level security clearances for provincial and territorial cyber interlocutors plus one other official per jurisdiction. This will be done through the Privy Council Office with the help of the Canadian Security Intelligence Service and the Royal Canadian Mounted Police;
- **Improve incident information-sharing**: The Canadian Cyber Incident Response Centre (CCIRC) under its new mandate will improve incident alerts and information sharing tools. It will be proposed that these be developed in consultation with the provincial and territorial representatives within the Chief Information Officers' community.
- **Partner on education and public awareness activities**: Public Safety Canada's Director General of Communication will work with provincial/territorial senior officials (once identified) to explore existing/potential communications initiatives to promote public awareness. This group would discuss cyber month (October, 2011), as well as proposals such as the one put [redacted]

Bob Gordon, Conseiller spécial, Cybersécurité
Au nom de Lynda Clairmont, Sous-ministre adjointe, Gestion des mesures d'urgence et sécurité nationale

Dear Colleagues,

I am writing to follow up on our cyber security meeting held in Ottawa on March 29, 2011. The meeting was successful and the discussions provided insight into the challenges you face in addressing cyber security issues.

Many ideas were raised that merit further attention. Our discussions highlighted the great value in establishing information sharing mechanisms, exchanging policies, directives, guidelines, communication products and public policy analysis and the need for better coordination when engaging with our critical infrastructure sectors and other key partners. We now need to transform these ideas into concrete actions and prioritise our efforts.

With this in mind, I would like to propose a first teleconference on August 3, 2011, from 1:00 to 2:00 pm. In preparation for the teleconference, we would ask you to please identify priority areas or specific activities you feel should be the focus of our joint efforts in the coming months and identify the one(s) you may wish to lead on.

In addition, the teleconference will also be an opportunity for us to:

- Update you on Public Safety Canada's actions including the new mandate of the Canadian Cyber Incident Response Centre (CCIRC); and
- Update you on the federal public awareness campaign and discuss the possibility of partnering on this initiative.

Please submit your input and confirm your participation, or that of a delegate, by Thursday, July 28, 2011, to Marie Anick Maillé, Manager, Engagement and Partnership, National Cyber Security at MarieAnick.Maille@ps-sp.gc.ca or (613) 990-9379. A formal agenda and dial-in information will follow once we receive your input. Should you have any questions, please do not hesitate to communicate with Marie Anick Maillé or Robert Dick, Director General, National Cyber Security at Robert.Dick@ps-sp.gc.ca or 613-990-2661.

I would like to take this opportunity to reiterate our commitment to working together on cyber security. I look forward to our continued collaboration in the area of cyber security.

Kind regards,

Bob Gordon, Special Advisor (Cyber Security)
on behalf of Lynda Clairmont, Assistant Deputy Minister, Emergency Management and National Security

## FEDERAL/PROVINCIAL/TERRITORIAL TELECONFERENCE ON CYBER SECURITY – PROPOSED ANNOTATED AGENDA

**August 3, 2011**
**1:00 – 2:00 pm**

| Time | Item | Lead |
|---|---|---|
| **5 min** | **Welcome and Confirmation of Agenda** | **Public Safety Canada** |
| **15 min** | **Canadian Cyber Incident Response Centre (CCIRC)**<br>• Present the new mandate of the Canadian Cyber Incident Response Centre (CCIRC). | **Public Safety Canada** |
| **15 min** | **Public Awareness Campaign**<br>• Director General of Communication to present an update on federal public awareness campaign and seek partnership interest. | **Public Safety Canada** |
| **20 min** | **Priority Areas for Collaboration**<br>• Identify key priorities for future collaboration.<br>• Determine leads for key priorities identified. | **All** |
| **5 min** | **Next Steps**<br>• Determine a meeting schedule to move key priorities forward. | **All** |