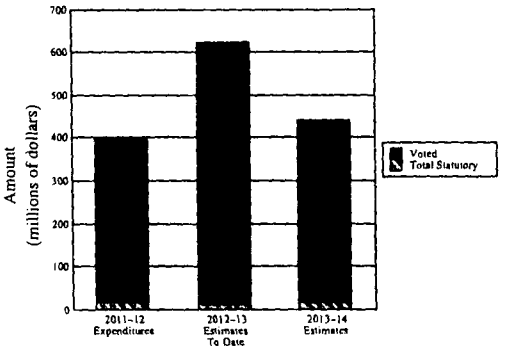
Public Safety and Emergency Preparedness

Raison d'être

The Department of Public Safety and Emergency Preparedness plays a key role in discharging the Government's fundamental responsibility for the safety and security of its citizens. Legislation governing the Department sets out two essential roles for the Department: (i) support the Minister's responsibility for all matters, except those assigned to another federal minister, related to public safety and emergency management including national leadership and (ii) coordinate the efforts of Public Safety's Portfolio agencies as well as provide guidance on their strategic priorities. The Department provides strategic policy advice on: national security; border strategies; countering crime; and emergency management. The Department also delivers a number of grant and contribution programs related to emergency management and community safety.

Organizational Estimate S

Budgetary



	2011–12 Expenditures	2012–13 Main Estimates	2012–13 Estimates To Date	2013–14 Estimates
		(dollars)		
Budgetary				
Voted				
1 Operating expenditures	141,648,763	124,671,421	128,028,599	124,342,301
5 Grants and contributions	244,162,360	292,939,791	479,440,792	300,628,590
Total voted	**385,811,123**	**417,611,212**	**607,469,391**	**424,970,891**
Total Statutory	*15,753,673*	*15,133,901*	*15,133,901*	*15,940,032*
Total budgetary	**401,564,796**	**432,745,113**	**622,603,292**	**440,910,923**

Note: Additional details by organization are available on the Treasury Board Secretariat web-site – www.tbs-sct.gc.ca.

Highlights

Public Safety and Emergency Preparedness is estimating budgetary expenditures of $440.9 million in 2013–14. Of this amount, $425.0 million requires approval by Parliament. The remaining $15.9 million represents statutory forecasts that do not require additional approval and are provided for information purposes.

The net spending increase of $8.2 million or 1.9 % is due to a decrease in operating funding of $0.3 million, an increase of $0.8 million in Employee Benefit Plans costs, a decrease in grants of $7.7 million, as well as an increase in contributions of $15.4 million.

Border Strategies

Major factors contributing to the net increase of $1.8 million in Border Strategies include:

• An increase of $1.0 million in Vote 1 for the implementation of national security and emergency management initiatives under the Beyond the Border: a shared vision for perimeter security and economic competitiveness.

In 2013–14, Public Safety and Emergency Preparedness will continue to promote the security of North America

François Guimont
Deputy Minister, Public Safety

Gary Robertson
Chief Financial Officer, Public Safety

through the implementation of initiatives under the Action Plan, such as in the areas of joint threat assessments and critical infrastructure resilience.

Countering Crime

Major factors contributing to the net decrease of $20.3 million in Countering Crime include:

• a decrease of $14.8 million in Vote 5 as a result of the sunsetting of a two year temporary funding arrangement for the sustainability of agreements under the First Nations Policing Program, net of funding received for the compensation, benefit and salary increases of the RCMP officers working for the Program;

• a decrease of $4.5 million ($1.7 million in Vote 1 and $2.8 million in Vote 5) as a result of the savings measures announced in Budget 2012; and,

• a decrease of $1.5 million in Vote 1 due to the realignment of budgets.

In 2013–14, Public Safety and Emergency Preparedness will aim to increase the effectiveness of the criminal justice system through exploring innovative cost-effective approaches to policing, and through advancing crime prevention initiatives such as the Community Benefit Investment initiatives. In addition, options for the renewal of the First Nations Policing Policy (FNPP) will be explored to ensure that the program continues to provide professional police services that are dedicated and responsive to the communities they serve.

Emergency Management

Major factors contributing to the net increase of $26.7 million in Emergency Management include:

• an increase of $38.2 million ($0.2 million in Vote 1 and $38.0 million in Vote 5) to provide financial support to Provinces and Territories for 2011 Flood Mitigation Investments;

• an increase of $1.1 million in Vote 1 for the implementation of national security and emergency management initiatives under the Beyond the Border: a shared vision for perimeter security and economic competitiveness;

• a decrease of $9.2 million ($2.7 million in Vote 1 and $6.5 million in Vote 5) as a result of the savings measures announced in Budget 2012. The $6.5 million decrease in Vote 5 relates to contributions to the provinces and municipalities pursuant to the *Emergency Management Act*;

• a decrease of $1.2 million in Vote 1 due to the realignment of budgets.

In 2013–14, Public Safety and Emergency Preparedness will work to enhance its capacity to respond to emergencies by ensuring that the Government Operations Centre (GOC) and regional offices have the equipment and infrastructure required to exercise national leadership and ensure sound information sharing and collaboration with other levels of government and emergency responders. The Department will make efforts to enhance the Government's resilience to prepare for, manage and recover from disasters, by reinforcing partnerships for national disaster mitigation while managing the increased costs of disaster recovery, and by renewing the Action Plan for Critical Infrastructure, with a focus on building resilience and a regional approach to risk management.

National Security

Major factors contributing to the net decrease of $2.4 million in National Security include:

• a decrease of $7.9 million in Vote 5 due to sunsetting of funds for the Ex Gratia payments to the families of the victims of Air India Flight 182;

• an increase of $1.8 million in Vote 5 for the Kanishka Project Research Initiative; and,

• an increase of $2.4 million in Vote 1 to strengthen the security of federal cyber systems.

In 2013–14, Public Safety and Emergency Preparedness will work to address emerging threats to the security of Canada, including terrorism, violent extremism, and transnational organized crime. The Department will ensure it has the necessary structures and equipment to meet Canada's obligations for cyber security and will continue to strengthen Canada's ability to intervene and respond to cyber security threats by working to secure government systems.

Internal Services

Major factors contributing to the net increase of $2.4 million in Internal Services include:

• an increase of $2.0 million in Vote 1 due to: the realignment of budgets; the implementation of national security and emergency management initiatives under the Beyond the Border: a shared vision for perimeter security and economic competitiveness; to maintain the standard of delivery of, and engage in new activities under the Continuity of Government program, and various other small initiatives; and

• a decrease of $1.2 million in Vote 1 as a result of the savings measures announced in Budget 2012.

For Estimates to date, please refer to the Supplementary Estimates (A), (B) and (C).

For further details on trends, please refer to the Report on Plans and Priorities.

Expenditures by Strategic Outcome and Program

Main

	2011–12 Expenditures	2012–13 Main Estimates	2013–14 Estimates
	(dollars)		
Budgetary			
A safe and resilient Canada.			
Countering Crime	170,120,151	209,999,507	189,707,922
Emergency Management	143,734,990	139,597,608	166,255,003
National Security	17,685,107	27,601,714	25,247,356
Border Strategies	2,946,130	2,522,140	4,297,690
The following program supports all strategic outcomes within this organization.			
Internal Services	67,078,418	53,024,144	55,402,952
Total	**401,564,796**	**432,745,113**	**440,910,923**

Note: Additional details by organization are available on the Treasury Board Secretariat web-site – www.tbs-sct.gc.ca.

Listing of Transfer Payments

Main

	2011–12 Expenditures	2012–13 Main Estimates	2012–13 Estimates To Date	2013–14 Estimates
		(dollars)		
Grants				
Grants in support of the Safer Communities Initiative	939,518	3,460,000	~~3,460,000~~ 2,960,000	2,960,000
Other National Voluntary Organizations active in the criminal justice sector	1,796,143	1,796,144	1,796,144	1,796,144
Kanishka Project Research Initiative	.....	500,000	500,000	700,000
Grants to provincial partners for the National Flagging System to identify and track high-risk violent offenders who jeopardize public safety	500,000	.....	500,000	500,000
Total Grants	**3,235,661**	**5,756,144**	~~6,256,144~~ 5,756,144	5,956,144
Contributions				
Payments to the provinces, territories, municipalities, Indian band councils and recognized authorities representing Indians on reserve, Indian communities on Crown land and Inuit communities, for the First Nations Policing Program	79,505,807	121,234,148	~~121,234,148~~ 78,489,148	105,184,130
Contributions to the provinces for assistance related to natural disasters	99,970,212	100,000,000	280,000,000	100,000,000
Contributions in support of the Safer Communities Initiative	42,279,554	40,139,899	~~40,139,899~~ 39,650,899	38,984,516
Financial Support to Provinces and Territories for 2011 Flood Mitigation Investments	.....	.....	50,000,000	37,950,000
Biology Casework Analysis Contribution Program	6,900,000	6,900,000	6,900,000	6,900,000
Kanishka Project Research Initiative	48,637	500,000	500,000	2,146,000
Contribution Program to Combat Child Sexual Exploitation and Human Trafficking	1,924,365	1,975,600	1,975,600	2,055,600
Aboriginal Community Safety Development Contribution Program	541,903	690,000	690,000	690,000
International Association of Fire Fighters, Canada	410,775	500,000	500,000	500,000
Payments to the provinces, territories, and public and private bodies in support of activities complementary to those of the Department of Public Safety and Emergency Preparedness	863,443	877,000	~~877,000~~ 617,000	362,000
			459,317,647	
Total Contributions	**232,444,696**	**272,816,647**	~~502,816,647~~	**294,672,446**
Total of listed Transfer Payments	**235,680,357**	**278,572,791**	~~509,072,791~~ 465,073,791	**300,628,590**

Interim Supply Requirements

Public Safety and Emergency Preparedness

Approved Items (dollars)

Vote No.	Vote wording and explanation(s) of Additional Twelfths	Total Main Estimates	Amount Granted
1	Public Safety and Emergency Preparedness – Operating expenditures and, pursuant to paragraph 29.1(2)(*a*) of the *Financial Administration Act*, authority to expend revenues received in a fiscal year through the provision of internal support services to other organizations to offset associated expenditures incurred in the fiscal year, and the payment to each member of the Queen's Privy Council for Canada who is a Minister without Portfolio or a Minister of State who does not preside over a Ministry of State of a salary not to exceed the salary paid to Ministers of State who preside over Ministries of State under the *Salaries Act*, as adjusted pursuant to the *Parliament of Canada Act* and pro rata for any period of less than a year No additional twelfths beyond the normal three-twelfths	124,342,301	31,085,575.25
5	Public Safety and Emergency Preparedness – The grants listed in the Estimates and contributions No additional twelfths beyond the normal three-twelfths	300,628,590	75,157,147.50

Items for inclusion in the Proposed Schedule 1 to the Appropriation Bill
(for the financial year ending March 31, 2014)

Unless specifically identified under the **Changes in 2013–14 Main Estimates** section, all vote wordings have been provided in earlier appropriation acts.

Vote No.	Items	Amount ($)	Total ($)
	PUBLIC SAFETY AND EMERGENCY PREPAREDNESS DEPARTMENT		
1	Public Safety and Emergency Preparedness – Operating expenditures and, pursuant to paragraph 29.1(2)(*a*) of the *Financial Administration Act*, authority to expend revenues received in a fiscal year through the provision of internal support services to other organizations to offset associated expenditures incurred in the fiscal year, and the payment to each member of the Queen's Privy Council for Canada who is a Minister without Portfolio or a Minister of State who does not preside over a Ministry of State of a salary not to exceed the salary paid to Ministers of State who preside over Ministries of State under the *Salaries Act*, as adjusted pursuant to the *Parliament of Canada Act* and pro rata for any period of less than a year	124,342,301	
5	Public Safety and Emergency Preparedness – The grants listed in the Estimates and contributions	300,628,590	
			424,970,891

2013–14 ESTIMATES

Statutory Forecasts

	2011–12 Expenditures	2012–13 Estimates To Date	Main 2013–14 Estimates
		(dollars)	
Budgetary			
Public Safety and Emergency Preparedness			
Contributions to employee benefit plans	15,676,137	15,056,385	[illegible]
Minister of Public Safety – Salary and motor car allowance	77,536	77,516	[illegible]

2013–14
ESTIMATES

Budgetary Expenditures by Standard Object

This table shows the forecast of total expenditures by Standard Object, which includes the types of goods or services to be acquired, or the transfer payments to be made and the revenues to be credited to the vote.

Definitions of standard objects available at: http://www.tpsgc-pwgsc.gc.ca/recgen/pceaf-gwcos/1112/7-intro-eng.html

Budgetary Expenditures by Standard Object

	Personnel	Transportation and communications	Information	Professional and special services	Rentals	Purchased repair and maintenance	Utilities, materials and supplies	Acquisition of land, buildings and works	Acquisition of machinery and equipment	Transfer payments	Public debt charges	Other subsidies and payments	Less: Revenues and other reductions	Total
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*		
Public Safety and Emergency Preparedness	107,094,806	4,359,279	2,147,897	18,859,617	4,296,445	1,694,416	809,009	1,019,565	2,398,811	300,628,590	.....	102,488	2,500,000	440,910,923

2013–14 ESTIMATES

Budgetary Expenditures by Strategic Outcome and Program

Main

Budgetary	2012–13		2013–14 Estimates				
	2011–12 Expenditures	Main Estimates	Operating	Capital	Transfer Payments	Revenues and other reductions	Total
Public Safety and Emergency Preparedness							
A safe and resilient Canada.							
Countering Crime	170,120,151	209,999,507	30,375,332	.....	159,332,590	.....	189,707,922
Emergency Management	143,734,990	139,597,608	27,805,003	.....	138,450,000	.....	166,255,003
National Security	17,685,107	27,601,714	22,401,356	.....	2,846,000	.....	25,247,356
Border Strategies	2,946,130	2,522,140	4,297,690	.....	.....	.....	4,297,690
The following program supports all strategic outcomes within this organization.							
Internal Services	67,078,418	53,024,144	57,902,952	.....	.....	(2,500,000)	55,402,952
Total	**401,564,796**	**432,745,113**	**142,782,333**	.....	**300,628,590**	**(2,500,000)**	**440,910,923**

Sécurité publique et Protection civile

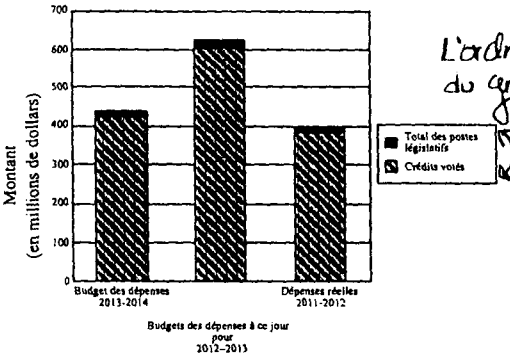
Raison d'être

Le ministère de la Sécurité publique et de la Protection civile joue un rôle clé en assumant la responsabilité fondamentale du gouvernement pour la sécurité de ses citoyens. La législation régissant le Ministère établit deux rôles essentiels pour celui-ci : (i) soutenir le ministre quant à ses responsabilités pour toutes questions relatives à la sécurité publique et à la gestion des urgences, à l'exception de celles attribuées à un autre ministre fédéral, y compris celles de leadership national et (ii) coordonner les efforts des organismes du portefeuille de Sécurité publique ainsi qu'offrir des orientations quant à leurs priorités stratégiques.

Le Ministère fournit des conseils sur diverses questions, notamment sur la sécurité nationale, les stratégies frontalières, la lutte au crime et la gestion des mesures d'urgence. Il met aussi en œuvre un certain nombre de programmes de subventions et de contributions liés à la gestion des urgences ainsi qu'à la sécurité des collectivités.

Budget des dépenses de l'organisation

Dépenses budgétaires



L'ordre des colonnes diffère du graphique dans la version anglaise
cet ordre est aussi inversée par rapport à version anglaise

	Dépenses réelles 2011-2012	2012-2013 Budget principal des dépenses	2012-2013 Budget des dépenses à ce jour	Budget des dépenses 2013-2014 principal
		(dollars)		
Budgétaire				
Crédits votés				
1 Dépenses de fonctionnement	141 648 763	124 671 421	128 028 599	124 842 301
5 Subventions et contributions	244 162 360	292 939 791	479 440 792	300 628 590
Total des crédits votés	**385 811 123**	**417 611 212**	**607 469 391**	**424 970 891**
Total des postes législatifs	*15 753 673*	*15 133 901*	*15 133 901*	*15 940 032*
Total des dépenses budgétaires	**401 564 796**	**432 745 113**	**622 603 292**	**440 910 923**

Nota : Des renseignements supplémentaires par organisation sont disponibles sur le site Web du Secrétariat du Conseil du Trésor – www.tbs-sct.gc.ca.

Faits saillants

Sécurité publique et Protection civile prévoit des dépenses budgétaires de 440,9 millions de dollars pour 2013-2014. De ce montant, 425,0 millions de dollars doivent être approuvés par le Parlement. Le solde de 15,9 millions de dollars représente les prévisions législatives qui ne nécessitent pas une approbation supplémentaire et qui sont fournies à titre d'information.

L'augmentation des dépenses nettes de 8,2 millions de dollars, soit 1,9 p. 100, est attribuable à une diminution de 0,3 million de dollars des dépenses de fonctionnement, à une augmentation de 0,8 million de dollars des coûts liés aux régimes d'avantages sociaux des employés, à une diminution de 7,7 millions de dollars des subventions ainsi qu'à une augmentation de 15,4 millions de dollars des contributions.

Stratégies frontalières

Les principaux facteurs contribuant à l'augmentation nette de 1,8 million de dollars pour les stratégies frontalières comprennent notamment :

• une augmentation de 1,0 million de dollars au crédit 1 pour la mise en œuvre des initiatives de sécurité nationale et de gestion des urgences dans le cadre de Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique du périmètre.

En 2013-2014, Sécurité publique et Protection civile continuera de promouvoir la sécurité de l'Amérique du Nord grâce à la mise en œuvre d'initiatives dans le cadre du Plan d'action, dans des secteurs comme les évaluations conjointes des menaces et la résilience des infrastructures essentielles.

Lutte au crime

Les principaux facteurs contribuant à la diminution nette de 20,3 millions de dollars pour la lutte au crime comprennent notamment :

• une diminution de 14,8 millions de dollars au crédit 5 en raison de la temporisation des fonds temporaires de deux ans pour la viabilité des accords conclus en vertu du Programme des services de police des Premières nations, nette du financement reçu pour les augmentation liées à la rémunération, aux avantages sociaux et aux salaires des agents de la GRC travaillant pour le Programme;

• une diminution de 4,5 millions de dollars (1,7 million de dollars au crédit 1 et 2,8 millions de dollars au crédit 5) en raison des mesures d'économies annoncées dans le budget fédéral de 2012; et

• une diminution de 1,5 million de dollars au crédit 1 attribuable au réalignement des budgets.

En 2013-2014, Sécurité publique et Protection civile visera à augmenter l'efficacité du système de justice pénale en explorant des approches innovatrices et rentables en matière de services de police et en améliorant les initiatives de prévention du crime, comme les initiatives d'investissements à bénéfice communautaire. De plus, des options de renouvellement pour le Programme des services de police des Premières nations seront examinées afin de veiller à ce que le programme continue d'offrir des services de police professionnels exclusifs et adaptés aux collectivités desservies.

Gestion des mesures d'urgence

Les principaux facteurs contribuant à l'augmentation nette de 26,7 millions de dollars pour la gestion des mesures d'urgence comprennent notamment :

• une augmentation de 38,2 millions de dollars (0,2 million de dollars au crédit 1 et 38,0 millions de dollars au crédit 5) pour fournir une aide financière aux provinces et aux territoires dans le cadre des mesures d'atténuation prises en 2011 en prévision des inondations;

• une augmentation de 1,1 million de dollars au crédit 1 pour la mise en œuvre des initiatives de sécurité nationale et de gestion des urgences dans le cadre de Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique du périmètre;

• une diminution de 9,2 millions de dollars (2,7 millions de dollars au crédit 1 et 6,5 millions de dollars au crédit 5) en raison des mesures d'économie annoncées dans le budget fédéral de 2012. La diminution de 6,5 millions de dollars au crédit 5 est liée aux contributions versées aux provinces et aux municipalités en vertu de la *Loi sur la gestion des urgences*; et

• une diminution de 1,2 million de dollars au crédit 1 en raison du réalignement des budgets.

En 2013-2014, Sécurité publique et Protection civile travaillera en vue d'améliorer sa capacité de répondre aux urgences en veillant à ce que le Centre des opérations du gouvernement (COG) et les bureaux régionaux disposent de l'équipement et de l'infrastructure nécessaires pour exercer un leadership national et assurer l'échange d'information et la collaboration avec d'autres échelons de gouvernement et d'intervention d'urgence. Le Ministère fera des efforts pour améliorer la résilience du gouvernement en matière de préparation, de gestion et de récupération en cas de catastrophes, en renforçant les partenariats pour l'atténuation des catastrophes nationales tout en gérant l'augmentation des coûts de la récupération à la suite de catastrophes, et en renouvelant le Plan d'action sur les infrastructures essentielles, avec une attention particulière sur le renforcement de la résilience et une approche régionale de la gestion du risque.

Sécurité nationale

Les principaux facteurs contribuant à la diminution nette de 2,4 millions de dollars pour la sécurité nationale comprennent notamment :

• une diminution de 7,9 millions de dollars au crédit 5 en raison de la temporisation des fonds pour les paiements à titre gracieux offerts aux familles des victimes du vol 182 d'Air India;

• une augmentation de 1,8 million de dollars au crédit 5 pour l'Initiative de recherche pour le projet Kanishka; et

• une augmentation de 2,4 millions de dollars au crédit 1 pour renforcer la sécurité des cybersystèmes fédéraux.

En 2013-2014, Sécurité publique et Protection civile abordera les menaces émergentes à la sécurité du Canada, incluant terrorisme, l'extrémisme violent et la criminalité transnationale organisée. Le Ministère veillera à ce qu'il dispose des équipements et des structures nécessaires pour remplir les obligations du Canada en matière de cybersécurité et continuera de renforcer la capacité du Canada d'intervenir et de répondre aux menaces en matière de cybersécurité en travaillant pour protéger les systèmes gouvernementaux.

Services internes

Les principaux facteurs contribuant à l'augmentation nette de 2,4 millions de dollars pour les services internes comprennent notamment :

• une augmentation de 2,0 millions de dollars au crédit 1 en raison du réalignement des budgets; de la mise en œuvre des initiatives de sécurité nationale et de gestion des urgences dans le cadre de Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique du périmètre; du maintien des normes de prestation de services et de la mise en place de nouvelles activités dans le cadre du Programme de continuité du gouvernement et divers autres initiatives mineures;

• une diminution de 1,2 million de dollars au crédit 1 à la suite des mesures d'économies annoncées dans le budget fédéral de 2012.

Pour le budget des dépenses à ce jour, veuillez consulter les Budgets supplémentaires des dépenses (A), (B) et (C).

Pour obtenir des renseignements supplémentaires sur les tendances, veuillez consulter le Rapport sur les plans et les priorités.

Dépenses par résultat stratégique et programme

Principal

	Dépenses réelles 2011-2012	2012-2013 Budget principal des dépenses	Budget des dépenses 2013-2014
	(en dollars)		
Budgétaire			
Un Canada sécuritaire et résilient.			
Lutte au crime	170,120,151	209,999,507	189,707,922
Gestion des mesures d'urgence	143,734,990	139,597,608	166,253,003
Sécurité nationale	17,685,107	2?,601,714	25,247,666
Stratégies frontalières	2,946,130	2,522,140	4,297,690
Le programme suivant appuie tous les résultats stratégiques de cette organisation.			
Services internes	67,078,418	53,024,144	55,402,952
Total	**401,564,796**	**432,745,113**	**440,910,923**

Numbers are not Formatted in French no Coma

Nota : Des renseignements supplémentaires par organisation sont disponibles sur le site Web du Secrétariat du Conseil du Trésor – www.tbs-sct.gc.ca.

Liste des paiements de transfert

	Dépenses réelles 2011-2012	2012-2013 Budget principal des dépenses	2012-2013 Budget des dépenses à ce jour	Budget des dépenses principal 2013-2014
		(en dollars)		
Subventions			2 960 000	
Subventions pour soutenir l'Initiative pour des communautés plus sûres	939 518	3 460 000	~~3 460 000~~	2 960 000
Autres organismes nationaux de bénévolat actifs dans le secteur de la justice pénale	1 796 143	1 796 144	1 796 144	1 796 144
Initiative de recherche pour le projet Kanishka	.....	500 000	500 000	700 000
Subventions aux partenaires provinciaux pour le Système national de repérage afin de repérer et de surveiller les délinquants violents à risque élevé qui mettent en péril la sécurité	500 000	.....	500 000	500 000
Total des subventions	**3 235 661**	**5 756 144**	~~6 256 144~~ 5 756 144	~~6 956 144~~ 5 956 144
Contributions				
Paiements aux provinces, aux territoires, aux municipalités, ainsi qu'aux conseils de bande, aux représentants officiels des Autochtones vivant dans les réserves, aux collectivités autochtones établies sur les terres de la Couronne et aux groupes inuits conformément au Programme de services de police des Premières nations	79 505 807	121 234 148	~~121 234 148~~ 78 484 148	~~105 184 830~~
Contributions versées aux provinces à titre d'aide financière en cas de catastrophes naturelles	99 970 212	100 000 000	280 000 000	100 000 000
Contributions pour soutenir l'Initiative pour des communautés plus sûres	42 279 554	40 139 899	~~40 139 899~~ 39 650 899	~~38 934 516~~
Aide financière aux provinces et aux territoires pour les mesures d'atténuation prises en 2011 en prévision des inondations	.....	.....	50 000 000	~~37 950 000~~
Programme de contributions pour les analyses biologiques	6 900 000	6 900 000	6 900 000	6 900 000
Initiative de recherche pour le projet Kanishka	48 637	500 000	500 000	~~2 146 000~~
Programme de contribution visant à combattre l'exploitation sexuelle des enfants et la traite de personnes	1 924 365	1 975 600	1 975 600	2 055 600
Programme de contributions à l'amélioration de la sécurité des collectivités autochtones	541 903	690 000	690 000	690 000

	Dépenses réelles 2011-2012	2012-2013 Budget principal des dépenses	2012-2013 Budget des dépenses à ce jour	Budget des dépenses Principal 2013-2014
		(en dollars)		
Association internationale des pompiers, Canada	410 775	500 000	500 000	500 000
Paiements aux provinces, aux territoires et aux organismes publics et privés pour appuyer des activités complémentaires à celles du ministère de la Sécurité publique et de la Protection civile	863 443	877 000	~~877 000~~ 617 000	362 000
			459 317 647	
Total des contributions	**232 444 696**	**272 816 647**	**~~502 816 647~~**	**294 672 446**
Total de la liste des paiements de transfert	**235 680 357**	**278 572 791**	**~~509 072 791~~** 465 073 791	**300 628 590**

Exigences en matière de crédits provisoires

Sécurité publique et Protection civile

Articles approuvés (dollars)

N° du crédit	Libellé de crédit at explications pour les douzièmes supplémentaires	Total du Budget principal des dépenses	Montant alloué
1	Sécurité publique et Protection civile – Dépenses de fonctionnement et, conformément au paragraphe 29.1(2) de la *Loi sur la gestion des finances publiques*, autorisation de dépenser les recettes perçues au cours d'un exercice pour la prestation de services de soutien internes à d'autres organisations pour compenser les dépenses connexes survenues au cours de l'exercice, ainsi que le versement, à chacun des membres du Conseil privé de la Reine pour le Canada qui a qualité de ministre sans portefeuille ou de ministre d'État, mais qui ne dirige pas un ministère d'État, d'un traitement n'excédant pas celui versé aux ministres d'État qui dirigent un ministère d'État, aux termes de la *Loi sur les traitements*, rajusté en vertu de la *Loi sur le Parlement du Canada* et au prorata, pour toute période inférieure à un an Aucun douzième supplémentaire n'est requis en plus des trois-douzièmes habituels	124 342 301	31 085 575,25
5	Sécurité publique et Protection civile – Subventions inscrites au Budget des dépenses et contributions Aucun douzième supplémentaire n'est requis en plus des trois-douzièmes habituels	300 628 590	75 157 147,50

Postes devant être inclus dans l'annexe 1 proposée au projet de loi de crédits
(pour l'année financière se terminant le 31 mars 2014)

Tous les libéllés des crédits sont tels qu'ils figuraient dans les lois de crédits antérieures, à moins d'avoir été précisément mentionnés dans la section **Changements au Budget principal des dépenses 2013-2014.**

N° du crédit	Postes	Montant ($)	Total ($)
	SÉCURITÉ PUBLIQUE ET PROTECTION CIVILE		
	MINISTÈRE		
1	Sécurité publique et Protection civile – Dépenses de fonctionnement et, conformément au paragraphe 29.1(2) de la *Loi sur la gestion des finances publiques*, autorisation de dépenser les recettes perçues au cours d'un exercice pour la prestation de services de soutien internes à d'autres organisations pour compenser les dépenses connexes survenues au cours de l'exercice, ainsi que le versement, à chacun des membres du Conseil privé de la Reine pour le Canada qui a qualité de ministre sans portefeuille ou de ministre d'État, mais qui ne dirige pas un ministère d'État, d'un traitement n'excédant pas celui versé aux ministres d'État qui dirigent un ministère d'État, aux termes de la *Loi sur les traitements*, rajusté en vertu de la *Loi sur le Parlement du Canada* et au prorata, pour toute période inférieure à un an	124 342 301	
5	Sécurité publique et Protection civile – Subventions inscrites au Budget des dépenses et contributions	300 628 590	
			424 970 891

BUDGET DES DÉPENSES
2013-2014

Prévisions législatives

	Dépenses réelles 2011-2012	Budget des dépenses 2012-2013	Budget des dépenses 2013-2014
		(en dollars)	
Budgétaire			
Sécurité publique et Protection civile			
Contributions aux régimes d'avantages sociaux des employés	15 676 137	15 056 385	15 860 930
Ministre de la Sécurité publique – Traitement et allocation pour automobile	77 536	77 516	79 102

BUDGET DES DÉPENSES
2013-2014

Dépenses budgétaires par article courant de dépense

Ce tableau indique les prévisions de dépenses globales par article courant de dépense qui inclut les types de biens ou de services qui doivent être acquis ou les paiements de transfert à effectuer et les recettes à valoir sur le crédit.

Definitions des articles courants fournies à: http://www.tpsgc-pwgsc.gc.ca/recgen/pceaf-gwcoa/1112/7-fra.html

Dépenses budgétaires par article courant de dépense

	Personnel	Transports et communications	Information	Services professionnels et spéciaux	Location	Achat de services de réparation et d'entretien	Services publics, fournitures et approvisionnements	Acquisition de terrains, de bâtiments et d'ouvrages	Acquisition de machines et de matériel	Paiements de transfert	Frais de la dette publique	Autres subventions et paiements	Moins : Recettes à valoir sur le crédit	Total
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*		
Sécurité publique et Protection civile	107,094,806	4,359,279	2,147,897	18,859,617	4,296,445	1,694,416	809,009	1,019,565	2,398,811	300,628,590	.....	102,488	2,500,000	440,910,923

numbers are not Formatted in French (no coma)

BUDGET DES DÉPENSES
2013-2014

Dépenses budgétaires par résultat stratégique et programme

Budgétaire

	réelles 2011-2012	2012-2013 Budget principal des dépenses	Budget des dépenses 2013-2014 Fonctionnement	Dépenses en capital	Paiements de transfert	Recettes et autres réductions	Total
Sécurité publique et Protection civile							
Un Canada sécuritaire et résilient							
Lutte au crime	170,120,151	209,999,507	30,375,332	.....	159,332,590	.....	189,707,922
Gestion des mesures d'urgence	143,734,990	139,597,608	27,805,003	.....	138,450,000	.....	166,255,003
Sécurité nationale	17,685,107	27,601,714	22,401,356	.....	2,846,000	.....	25,247,356
Stratégies frontalières	2,946,130	2,522,140	4,297,690	.....	.....	.....	4,297,690
Le programme suivant appuie tous les résultats stratégiques de cette organisation.							
Services internes	67,078,418	53,024,144	57,902,952	.....	.....	(2,500,000)	55,402,952
Total	**401,564,796**	**432,745,113**	**142,782,333**	.....	**300,628,590**	**(2,500,000)**	**440,910,923**

numbers are not formatted in French (nocoma)

Public Safety Canada | Sécurité publique Canada

Assistant Deputy Minister | Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

SECRET

DATE: FEB 0 1 2013

Why am I signing as a copy with typoset?

File No.: DEP-393033
RDIMS No.: 763139

MEMORANDUM FOR THE DEPUTY MINISTER

2013-14 MAIN ESTIMATES FOR PUBLIC SAFETY CANADA

(Signature required)

ISSUE

FEB 0 4 2013

The purpose of this memorandum is to request your approval of the final 2013-14 Main Estimates (ME) page proofs for the Department **(TAB A).** Treasury Board Secretariat (TBS) has requested that the page proofs be signed and returned by February 4, 2013.

BACKGROUND

Your signature on the page proofs signify that the Minister has been briefed regarding the content of the ME. A Memorandum to inform the Minister has been attached for your signature **(TAB C).**

Tabling of the Main Estimates in Parliament is tentatively scheduled during the week of February 25, 2013.

Changes have been made to the presentation of information in the *2013–14 Main Estimates*. A list of the major changes for Part II is attached **(TAB B).**

ANALYSIS

The Department's total funding requested in Main Estimates 2013-14 will total $440.9 million (including Employee Benefits Plans) compared to $432.7 million in 2012-13.

.../2

Canada

This represents a net spending increase of $8.2 million or 1.9% of the total departmental authorities due to a decrease in operating funding of $0.3 million, an increase of $0.8 million in Employee Benefit Plans costs, a decrease in grants of $7.7 million as well as an increase in contributions of $15.4 million.

Highlights of the changes in the 2013-14 ME are provided under Annex A.

CONSIDERATIONS

I approved the 2013-14 ME Page Proofs within 48 hours as required by TBS. However, I noted a number of changes to the Page Proofs. We requested that TBS provide a new set of Page Proofs reflecting these changes. However, TBS has not produced clean Page Proofs for your signature.

NEXT STEPS

A detailed portfolio-wide ministerial briefing will be arranged in advance of any requested appearance before Standing Committee.

A deck on the Department's Multi –Year Notional Budgets is being developed and will be presented to FMC.

RECOMMENDATION

A Memorandum to inform the Minister of the content of the 2013-14 Main Estimates has been provided for your signature. Similar briefing packages should be provided from each of the agencies in the Public Safety Portfolio.

We recommend that you sign the attached Memo to Minister as well as the enclosed 2013-14 Main Estimates page proofs by February 4, 2013.

Should you require additional information, please do not hesitate to contact me at 613-990-2615 or Rosanna Di Paola, Comptroller, at 613-998-0053.

Gary Robertson

Enclosures: (4)

Prepared by: Nancy Brunet

ANNEX A to the 2013-14 Main Estimates for Public Safety Canada

Highlights

Major factors contributing to the net increase include:

Increases:

- $38.2M ($0.2M in Vote 1 and $38.0M in Vote 5) to provide financial support to Provinces and Territories for 2011 Flood Mitigation Investments;
- $2.9M (in Vote 1) to strengthen the security of federal cyber systems;
- $2.5M (in Vote 1) for the implementation of national security and emergency management initiatives under the Beyond the Border: a shared vision for perimeter security and economic competitiveness;
- $1.8M (in Vote 5) for the Kanishka Project Research Initiative;
- $1.2M (in Vote 1) for Collective Bargaining increases for EC, EB, PA and PE;

Decreases:

- $15.2M ($6.0M in Vote 1 and $9.2M in Vote 5) as a result of the saving measures announced in Budget 2012;
- $14.8M ($15.0M in Vote 5 net of an increase of $0.2M) as a result of a two year temporary funding arrangement for the sustainability agreements under the First Nations Policing Program, net of funding received for the compensation, benefit and salary increases of the RCMP officers working for the Program;
- $7.9M (in Vote 5) due to the sunsetting of funds for the Ex Gratia payments to the families of the victims of Air India Flight 182;

Le français suit.

New This Year

Changes have been made to the presentation of information in the *2013–14 Main Estimates*. The major changes for Part II are:

- organizations are listed in alphabetical order rather than by portfolio;
- statutory amounts are summarized with details presented on TBS' Web site;
- amounts are presented to the dollar; and,
- the former Ministry Summary table is now the "Organizational Estimates" table for the individual organization.

Financial tables in Part I, as well as the new Organizational Estimates table and the table listing grants and contributions will contain four financial columns:

- 2011–12 actual expenditures as published in the Public Accounts of Canada;
- *2012–13 Main Estimates* as previously published;
- 2012–13 Estimates to date which will include the total of your Main Estimates and Supplementary Estimates tabled to date; and
- *2013–14 Main Estimates*.

The organizational "Highlights" narrative is located directly after the Organizational Estimates table and should be drafted to explain the key elements of the financial information presented in the Estimates document, particularly the financial information presented in the Organizational Estimates table. Characteristics of good highlights would include:

- explanations of trends, anomalies or variances;
- new initiatives for which funding was announced in Budget 2012;
- use of funds to achieve organizational plans and priorities (akin to an executive summary of your Report on Plans and Priorities); and,
- referring readers to the Report on Plans and Priorities or Corporate Plan for further details.

Nouveautés cette année

Des changements ont été apportés à la présentation de l'information dans le *Budget principal des dépenses 2013-2014*. Les principales modifications apportées à la partie II sont les suivantes :

- les organisations sont présentées en ordre alphabétique plutôt que par portefeuille;
- les montants législatifs sont résumés et les détails sont présentés sur le site Internet du Secrétariat;
- les montants sont indiqués au dollar près; et,
- l'ancien tableau « Sommaire du portefeuille » est remplacé par le tableau « Budget des dépenses de l'organisation » pour chaque organisations.

Les tableaux financiers de la partie I, ainsi que le nouveau tableau du budget des dépenses de l'organisation et le tableau indiquant les subventions et les contributions comprendront quatre colonnes :

- Dépenses réelles 2011-2012, telles que publiées dans les Comptes publics du Canada;
- *Budget principal des dépenses 2012-2013*, tel que publié auparavant;
- Budget des dépenses 2012-2013 à ce jour, qui comprendra le total de votre budget principal des dépenses et de vos budgets supplémentaires des dépenses déposés à ce jour;
- *Budget principal des dépenses 2013-2014*.

Les « Faits saillants » de l'organisation sont présentés directement après le tableau du budget des dépenses de l'organisation et devraient expliquer les principaux éléments des renseignements financiers présentés dans le document du budget des dépenses, plus particulièrement les renseignements financiers inscrits dans le tableau du budget des dépenses de l'organisation. Les faits saillants devraient comprendre les caractéristiques suivantes :

- une explication des tendances, des anomalies ou des écarts budgétaires;
- toutes nouvelles initiatives pour laquelle des fonds ont été annoncés dans le budget fédéral de 2012;
- une description de l'utilisation des fonds pour réaliser les plans et les priorités de l'organisation (comparable à un sommaire de votre rapport sur les plans et les priorités); et,
- un renvoi au rapport sur les plans et les priorités ou au plan ministériel de l'organisation permettant au lecteur d'obtenir plus de détails.

Public Safety Canada | Sécurité publique Canada
Deputy Minister | Sous-ministre
Ottawa, Canada
K1A 0P8

COPY

SECRET

DATE: FEV FEB 0 4 2013

File No.: DEP-393033
RDIMS No.: 765622

MEMORANDUM TO THE MINISTER

2013-14 MAIN ESTIMATES FOR PUBLIC SAFETY CANADA

(Information only)

ISSUE

The purpose of this memorandum is to provide you with an overview of Public Safety's Main Estimates for 2013-14 **(Tab A).**

Tabling of the Main Estimates in Parliament is tentatively scheduled during the week of February 25, 2013.

HIGHLIGHTS

The Department's total funding requested in Main Estimates 2013-14 will total $440.9 million (including Employee Benefits Plans) compared to $432.7 million in 2012-13. This represents a net spending increase of $8.2 million or 1.9% of the total departmental authorities due to a decrease in operating funding of $0.3 million, an increase of $0.8 million in Employee Benefit Plans costs, a decrease in grants of $7.7 million as well as an increase in contributions of $15.4 million.

Major factors contributing to the net increase include:

Increases:

- $38.2M ($0.2M in Vote 1 and $38.0M in Vote 5) to provide financial support to Provinces and Territories for 2011 Flood Mitigation Investments;
- $2.9M (in Vote 1) to strengthen the security of federal cyber systems;

.../2

Canada

- $2.5M (in Vote 1) for the implementation of national security and emergency management initiatives under the Beyond the Border: a shared vision for perimeter security and economic competitiveness;

- $1.8M (in Vote 5) for the Kanishka Project Research Initiative; and

- $1.2M (in Vote 1) for Collective Bargaining increases for EC, EB, PA and PE.

Decreases:

- $15.2M ($6.0M in Vote 1 and $9.2M in Vote 5) as a result of the saving measures announced in Budget 2012;

- $14.8M ($15.0M in Vote 5 net of an increase of $0.2M) as a result of a two year temporary funding arrangement for the sustainability agreements under the First Nations Policing Program, net of funding received for the compensation, benefit and salary increases of the Royal Canadian Mounted Police officers working for the Program; and

- $7.9M (in Vote 5) due to the sunsetting of funds for the Ex Gratia payments to the families of the victims of Air India Flight 182.

NEXT STEPS

You should be receiving similar briefing material from other agencies in the Portfolio. A fully integrated Portfolio briefing package will be prepared for your information, in anticipation of the tabling and possible appearance before Standing Committee. A Portfolio-wide meeting will be arranged to brief you in advance of any requested appearance before Standing Committee.

Should you require additional information, please do not hesitate to contact me or Mr. Gary Robertson Chief Financial Officer, Corporate Management Branch, at 613-990-2615.

François Guimont

Enclosure: (1)

Prepared by: Nancy Brunet

Public Safety Canada / Sécurité publique Canada

CMB
Branch /Branche
SGM

Routing Slip / Bordereau d'acheminement

File No / No de dossier : DEP-393033 Folder No:
Assistant Deputy Minister Quality Control / Contrôle de qualité du Sous-ministre adjoint : _____

Title / Titre : 2013-14 Main Estimates for Public Safety			**ACTION REQUIRED / MESURES À PRENDRE**		
Name / Nom	**Date**	**Initials / Initiales**	**Approval or signature / Approbation ou signature**	**Information**
Originator / Auteur Nancy Brunet	31/01/2013	NB	☐	☐
Director / Directeur Michael Dionais	31/01/13		☒	☐
Director General / Directeur général Rosanna Di Paola	31/01/13		☒	☐
Chief Audit Executive / Dirigeante principale de la vérification Rosemary Stephenson			☐	☐
Director General Communications / Directrice générale des communications Stéphanie Durand			☐	☐
Executive Director & Senior General Counsel LS / Directeur exécutif et Avocat général principal SJ Paul Shuttle			☐	☐
Assistant Deputy Minister SP / Sous-ministre adjoint PS Paul MacKinnon			☐	☐
Assistant Deputy Minister LP / Sous-ministre adjoint SPL Richard Wex			☐	☐
Assistant Deputy Minister CM / Sous-ministre adjoint GM Gary Robertson	FSB 1/13		☒	☐
Assistant Deputy Minister CSP / Sous-ministre adjoint SPP Shawn Tupper			☐	☐
Assistant Deputy Minister EMRO / Sous-ministre adjointe GMUOR Gina Wilson			☐	☐
Assistant Deputy Minister NS / Sous-ministre adjointe SN Lynda Clairmont			☐	☐
Associate Deputy Minister / Sous-ministre délégué Graham Flack			☐	☐
Deputy Minister / Sous-ministre François Guimont			☒	☐
Minister / Ministre The Honourable / L'honorable Vic Toews			☐	☒

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

Request to Add an Agenda Item

Title of the proposed item

[redacted] Status Report

Who is sponsoring this item? Are there any co-sponsors for this item?
(Names of sponsoring and co-sponsoring jurisdictions)
Justice Canada and [redacted]

Purpose of this item:

- ☐ **For Approval or For Decision**
- ☐ **For Discussion only**
- ☐ **Items that Don't Require a Discussion:**
  - ☐ **Consent Item** (Items for approval that are expected to have support and don't require a discussion)
  - **X☐X Written Update**

What types of discussion are the Deputy Ministers expected to have on this item? Please provide a brief rationale for the inclusion of this item on the agenda and explain what the expected outcome is. (max. 30 words)

This would be a brief written update, in report form, to Deputy Ministers on the work of [redacted] Working Group. It is not proposed that there would be any presentation or discussion.

Please identify key discussion questions for FPT DM discussion after the presentation.

Amount of time requested for this item: (Please include both presentation and expected discussion time, i.e. 15 minute presentation and 15 minute discussion)

Once completed please return to: Justice.Canada.FPT@justice.gc.ca

Not applicable, written update only

If there is to be a presentation, who will be making the presentation?
(Name, email address and phone number please)

Who will be the key contact for this agenda item?
(Name, email address and phone number please)
Karen Audcent (
Karen.Audcent@justice.gc.ca, 613-957-4733

If there will be a conference document, who will be drafting the document?
(Name, email address and phone number please)
Karen Audcent (
Karen.Audcent@justice.gc.ca, 613-957-4733

Please note that all Agenda Templates and Conference Documents will be circulated to all jurisdictions in advance of the meeting so that all parties are prepared for discussions.

s.14(a)

Once completed please return to: Justice.Canada.FPT@justice.gc.ca

Pages 41 to / à 44

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 45

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(c), 14(a), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 46 to / à 54

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

s.13(1)(c)
s.19(1)

Request to Add an Agenda Item

Title of the proposed item
Data Retention - Child Sexual Exploitation

Who is sponsoring this item? Are there any co-sponsors for this item?

Purpose of this item:
☐ **For Approval or For Decision**
✓ **For Discussion only**
☐ **Items that Don't Require a Discussion:**
- ☐ **Consent Item** (Items for approval that are expected to have support and don't require a discussion)
- ☐ **Written Update**

Could this item be the subject of an announcement?
✓ Yes ☐ No

Ministers could announce that this item will be monitored and discussed regularly at their meetings to ensure that Ministers are well aware of promising developments in the areas of data retention and preservation in order to protect children from the technologically assisted sexual exploitation.

What type of discussion are Ministers expected to have on this item? Please provide rational and expected outcomes.

- The would like to have a follow up discussion on the issue of data retention and data preservation with respect to child sexual exploitation.
- At the last FPT Ministers meeting this issue was discussed and it was proposed that the federal government consider increasing the preservation period in the former Bill C-51 for international cases from 21 to 90 days. At that time it was encouraged that this issue undergo continual review and work to ensure that we are doing the best that we can do and to keep abreast of how this issue is being managed in other countries.
- This will assist Canada in moving forward in developing a scheme for data retention given the importance of this in police investigations into child pornography.

Amount of time requested for this item: (Please include both presentation and expected discussion time, i.e. 15 minute presentation and 15 minute discussion)

Once completed please return to:

Minister would open up the discussion speaking to the issue for approximately five minutes. Followed by 15 minutes for discussion.

If there is to be a presentation, who will be making the presentation?

Who will be the key contact for this agenda item?

If there will be a conference document, who will be drafting the document?

Please note that all templates and Conference Documents will be circulated to all jurisdictions in advance of the meeting so that all parties are prepared for discussions.

s.19(1)

Once completed please return to:

Pages 57 to / à 58

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Request to Add an Agenda Item

s.14(a)

Title of the proposed item

[redacted]

Who is sponsoring this item? Are there any co-sponsors for this item?
Public Safety Canada

Purpose of this item:
☐ **For Approval or For Decision**
✓ **For Discussion only**
☐ **Items that Don't Require a Discussion:**
- ☐ **Consent Item** (Items for approval that are expected to have support and don't require a discussion)
- ☐ **Written Update**

Could this item be the subject of an announcement?
☐ Yes ✓ No

What type of discussion are Ministers expected to have on this item? Please provide rational and expected outcomes.

- To enhance Provincial/Territorial awareness of a national security issue that impacts their governments and jurisdictions;
- To reinforce positive action the federal government is taking; and
- To expand opportunities for Federal/Provincial/Territorial cooperation on national security and [redacted]

Amount of time requested for this item:
10 minute presentation and 5 minute discussion

If there is to be a presentation, who will be making the presentation?
Robert Dick, Director General, National Cyber Security Directorate,
robert.dick@ps.gc.ca, 613-990-2661

Who will be the key contact for this agenda item?
Robert Dick, Director General, National Cyber Security Directorate,
robert.dick@ps.gc.ca, 613-990-2661

If there will be a conference document, who will be drafting the document?
N/A

Once completed please return to: Justice.Canada.FPT@justice.gc.ca

Please note that all templates and Conference Documents will be circulated to all jurisdictions in advance of the meeting so that all parties are prepared for discussions.

Once completed please return to: Justice.Canada.FPT@justice.gc.ca

Pages 61 to / à 62

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Request to Add an Agenda Item

s.14(a)

Title of the proposed item

[redacted] Status Report

Who is sponsoring this item? Are there any co-sponsors for this item?
(Names of sponsoring and co-sponsoring jurisdictions)
Justice Canada

Purpose of this item:

☐ **For Approval or For Decision**
☐ **For Discussion only**
☐ **Items that Don't Require a Discussion:**
- ☐ **Consent Item** (Items for approval that are expected to have support and don't require a discussion)
- X☐ **Written Update**

Could this item be the subject of an announcement?

☐ Yes X☐ No

What type of discussion are Ministers expected to have on this item? Please provide rationale and expected outcomes.

None. Written information item only.

Amount of time requested for this item: (Please include both presentation and expected discussion time, i.e. 15 minute presentation and 15 minute discussion)
None. Written information item only.

If there is to be a presentation, who will be making the presentation?
(Name, email address and phone number please)

Who will be the key contact for this agenda item?
(Name, email address and phone number please)

Once completed please return to: Justice.Canada.FPT@justice.gc.ca

Karen Audcent, Karen.Audcent@justice.gc.ca, 613-957-4733

If there will be a conference document, who will be drafting the document?
(Name, email address and phone number please)
Karen Audcent, Karen. Audcent@justice.gc.ca, 613-957-4733

Please note that all templates and Conference Documents will be circulated to all jurisdictions in advance of the meeting so that all parties are prepared for discussions.

Once completed please return to: Justice.Canada.FPT@justice.gc.ca

Pages 65 to / à 66

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(c), 14(a)

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada
Assistant Deputy Minister | Sous-ministre adjoint
Ottawa, Canada
K1A 0P8

For your meeting with:
Ange Mancini
On: Tuesday, October 9, 2012, at 3:00 p.m.

SECRET

DATE: OCT 0 9 2012

FILE No.: 390536
RDIMS (Dragon) No.: 3591

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

MEETING WITH ANGE MANCINI,
FRENCH NATIONAL INTELLIGENCE COORDINATOR

(Information only)

SUMMARY

You will be meeting with Ange Mancini, the French *Coordonnnateur national du renseignement* on Tuesday October 9, 2012, from 3:00 to 3:30, in Boardroom 19C-3100. Mr. Mancini will be accompanied by:

- General Hubert de Reviers de Mauny, Advisor, *Conseil national du renseignement*;
- Vincent Martin Pavailler, Advisor, *Conseil national du renseignement*;
- Alexandre Vulic, First Counsellor, French Embassy;
- Christelle Sarnelli, Liaison Officer, *Direction générale de la sécurité extérieure* (foreign intelligence agency), French Embassy; and
- Colonel Thierry Cailloz, Homeland Security Attaché, French Embassy.

John Davies, Director General, National Security Policy Directorate, will support you at the meeting.

Mr. Mancini's biography is enclosed **(TAB A)**. Proposed key messages, in both English and French, are also attached **(TAB B)**. Information on Canada-France bilateral relations, provided by the Department of Foreign Affairs and International Trade, is enclosed **(TAB C)**.

.../2

STRATEGIC OBJECTIVES

The following are the recommended objectives for the meeting:

- emphasize the importance of the Canada-France public safety bilateral relationship;
- inquire about the upcoming white paper on defence and national security currently being developed, and whether that will lead to significant changes in national security priorities and funding;
- exchange views on approaches to cyber security, the international threat picture, and information-sharing in the context of the Beyond the Border agreement; and
- explore deeper cooperation on cyber issues.

BACKGROUND

France

On May 6, 2012, François Hollande, leader of the Socialist Party, was elected President of France. On May 15, 2012, Mr. Hollande named Jean-Marc Ayrault Prime Minister. Prime Minister Ayrault announced the composition of his Cabinet on May 16, 2012. The Minister's counterpart, Manuel Valls, was appointed Minister of the Interior.

On September 28, 2012, the Government released its first budget. The Government's main objective is to bring down the deficit to 3 per cent of the French GDP in 2013 from the current 4.5 per cent. Cuts include €2.2 B from defence programs and €2.8 B from administrative costs across all ministries. Also announced in the budget is the creation of 480 new police jobs that will be deployed to "priority security areas" – 15 areas identified by Minister Valls where more concerted and sustained efforts will be made to curb youth criminality.

Public Safety Relations

France is identified as a [redacted] in the International Strategic Framework. Canada and France have a history of cooperation on various public safety issues.

Law enforcement cooperation between Canada and France is excellent. The Royal Canadian Mounted Police (RCMP) and the *Police nationale* cooperate on a wide range of policing issues, but especially on criminal investigations. Canada and France are both members of the Financial Action Task Force and also contribute to the Caribbean

.../3

s.15(1) - Int'l

Financial Task Force forum, which aims to curtail money laundering and the traffic of drugs in the region. The RCMP works closely with the French domestic security agency, the *Direction centrale du renseignement intérieur* (DCRI), the *Sous-direction de la lutte anti-terroriste* and the *Unité centrale de lutte anti-terroriste* on counter-terrorism investigations. Both Canada and France are contributing civilian police to MINUSTAH. There are Extradition and Mutual Legal Assistance Treaties between Canada and France.

[redacted]

Canada (National Crime Prevention Centre) and France (*Secrétariat général du Comité interministériel des villes*) are both members of the International Centre for Crime Prevention (CIPC)'s Advisory and Policy Committee. The CIPC is located in Montreal, Quebec.

Conseil national du renseignement

As National Intelligence Coordinator to the President, Mr. Mancini heads the *Conseil national du renseignement* (CNR) and oversees its day-to-day activities. Reporting directly to the President, Mr. Mancini is the intelligence agencies' point of entry to President Hollande. Mr. Mancini was appointed in February 2011, replacing Bernard Bajolet, who met with then Deputy Minister Bill Baker in January 2010.

The CNR was born out of the 2008 French *White Paper on Defence and National Security*. The CNR's role is to coordinate intelligence analysis, eliminate redundancies, and fill the gaps in the current intelligence system. The President chairs CNR meetings, which is attended by the Prime Minister and the Ministers of Defence, Interior, Foreign Affairs and Finance, and other ministers as required.

A New White Paper on Defence and National Security for 2013

On July 13, 2012, Jean-Marie Guéhenno, former United Nations' Under-Secretary-General for Peacekeeping Operations, was appointed by President Hollande to head the White Paper Commission, responsible for drafting the document. The *White Paper on Defence and National Security* should be released in early 2013. The objective of the White Paper is to define France's national security priorities and capabilities over the next 15-20 years. Following its release, resources for the defence and national security portfolios for the period of 2014-2019 will be allocated through a military programme bill of law.

s.15(1) - Def
s.15(1) - Int'l

.../4

Approaches to Cyber Security

Canada-France Cooperation on Cyber Security

Canada, France and over 100 countries will attend the upcoming World Conference on International Telecommunications (WCIT) in Dubai in December 2012 to revise the International Telecommunication Regulations, a treaty binding instrument. Given the binding nature of the Conference outcome,

France's Approach to Cyber Security

France's domestic cyber security efforts are coordinated through the *Agence nationale de la sécurité des systèmes d'information* (ANSSI), created in 2009. ANSSI is responsible for: detecting and responding to cyber attacks against government systems; supporting the development of trusted products and services to protect networks in government and certain economic sectors (i.e. what is known as the supply chain in Canada); providing advice and support to critical infrastructure operators; and public awareness efforts.

Much like PS, ANSSI coordinates cyber security policy with line departments, such as Foreign Affairs, Finance, and Defence. ANSSI reports to the General Secretary for Defence and National Security, who in turn reports to the Prime Minister. Both the General Secretary and Prime Minister sit on the CNR. ANSSI's role is defensive. Charged with protecting and defending both government systems and overseeing the cyber security of critical infrastructure sectors, it has the power to set minimum cyber security requirements for all government departments and order telecommunications providers to undertake actions to strengthen their cyber security, either during a specific cyber incident or as part of routine mitigation measures.

Also responsible for signal intelligence, the DGSE leads France's offensive cyber activities for intelligence and military purposes. While the extent of France's offensive cyber capabilities is unknown, it is generally understood to have the expertise and skill to rival that of some Five Eyes members.

Cyber Threats

While other countries have similar challenges, they are beginning to

.../5

s.15(1) - Def
s.15(1) - Int'l

develop mechanisms to facilitate information sharing with the private sector. [redacted] Further, senior U.S. officials have begun denouncing China's economic cyber espionage publicly in Congressional hearings [redacted]

International Threat Environment

Terrorism

France remains a priority target for Islamist extremism, particularly Al Qaeda (AQ)-affiliated extremists, as evidenced by the March 2012 shootings in Toulouse by Mohamed Merah. Interest in France by senior AQ leadership has intensified in recent years, due in large part to France's intervention in Libya, as well and its close relationship to the U.S.

It is also worth noting that the French Minister of the Interior announced on October 3, 2012 the tabling of a *Bill regarding security and combating terrorism.* The bill will permit local arrests of individuals who have visited foreign combat training camps, as well as extend measures that were due to expire this year that allow French police access to the electronic or Internet communications of suspected terrorists.

[redacted]

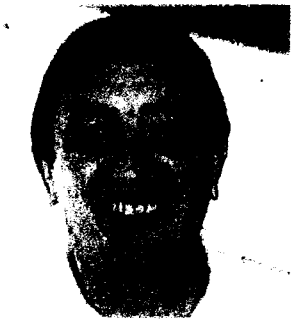
Should you require additional information, please do not hesitate to contact me at 613-949-6435 or Megan Nichols, Acting Director General, Border Policy and International Affairs Directorate, Strategic Policy Branch, at 613-998-2936.

Paul MacKinnon

Enclosures: (3)

Prepared by: Joey Cloutier

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)



Ange Mancini, National Intelligence Coordinator.

Ange Mancini was born on June 15, 1944, in Beausoleil, Alpes-Maritimes. He is the French intelligence national coordinator since February 23, 2011.

His father was a bricklayer from Italy. In 1963, he started a career in the National Police. In 1983, he served as the head of the *Service Régional de Police Judiciaire* of Ajaccio. In 1985, he created the *Recherche Assistance Intervention Dissuasion*. He served as its first Head from 1985 to 1990. In 1987, he helped arrest members of *Action directe* in the Loiret. From 1990 to 1995, he served as the head of the SRPJ of Versailles. He then served as the Deputy Head of the *Direction Centrale de la Police Judiciaire* until 1996.

From 1999 to 2002, he served as deputy prefect for security of Corse-du-Sud and Haute-Corse. He served as the prefect of French Guiana from 2002 to 2006, then of Landes, and later of Martinique.

He enjoys golf, cross-country cycling, and hunting

SECRET

MEETING WITH ANGE MANCINI, FRENCH NATIONAL INTELLIGENCE COORDINATOR

Key Messages

Upcoming White Paper and Defence Program Bill of Law

- I am noting with interest that a new White Paper on Defence and National Security is currently being developed.
    - Do you foresee significant changes in national security priorities?
    - Given the €2.2 B cuts in Defence spending already announced in this year's budget and the Government deficit reduction objective, do you anticipate budget cuts in the Defence Program Bill of Law (*Loi de programmation militaire*), to be released in 2013?

Cyber Security

- I understand that the French Government can compel telecommunication providers to take specific measures to strengthen their cyber security. Can you elaborate on the kind of measures the Government can direct the providers to take?

- [redacted]

- I understand that our officials are collaborating at the UN Group of Government Experts on Information Security to develop confidence and security building measures to reduce the risk of state conflict in cyberspace. This offers a more practical alternative to new treaties.

- [redacted]

- If you agree, I would appreciate it if your officials could provide a cyber security contact at the working level to my office. I will ensure that our officials get in touch.

International Threat Environment

- I would be interested in learning more about the newly tabled bill on security and combating terrorism (*Projet de loi relative a la sécurité et a la lutte contre le terrorisme*), tabled on October 3, 2012.

- How does France communicate and engage with the public on new and emerging threats?

s.15(1) - Int'l

Impact of the Beyond the Border Agreement on National Security and Information-Sharing

- Through the Beyond the Border Action Plan, Canada and the United States continue to build upon an already strong foundation of bilateral information-sharing for national security purposes.

- By enhancing our understanding of, each other's legal and operational systems, we have been successful in addressing a number of challenges to information-sharing. Work continues to identify and address other areas of improvement.

- Our intelligence agencies are also working on joint integrated threat assessments in order that we have a common understanding of threats, within, at, and away from our borders.

RENCONTRE AVEC ANGE MANCINI, COORDONNATEUR NATIONAL DU RENSEIGNEMENT DE LA FRANCE

Messages clés

Livre blanc et projet de loi relatif à la programmation militaire

- Je note avec intérêt que l'on est en train de préparer un nouveau Livre blanc sur la défense et la sécurité nationale.
  - Prévoyez-vous des changements importants aux priorités en matière de sécurité nationale?
  - Étant donné les réductions de 2,2 milliards d'euros dans le secteur de la défense qui ont été annoncées dans le cadre du budget de cette année et les objectifs de réduction du déficit du gouvernement, vous attendez-vous à ce que la *Loi de programmation militaire*, prévue en 2013, soit touchée par des compressions budgétaires?

Cybersécurité

- J'ai cru comprendre que le gouvernement de la France peut obliger les fournisseurs de services de télécommunications à prendre des mesures pour accroître leur propre cybersécurité. Pouvez-vous préciser le genre de mesures que le gouvernement peut ordonner?

- [redacted]

- Nos représentants font partie du Groupe d'experts gouvernementaux des Nations Unies sur la sécurité de l'information, lequel a pour mission d'établir des mesures de confiance et de sécurité en vue de réduire le risque de conflits entre les États dans le cyberespace. Cette approche est une solution de rechange pratique à la conclusion de nouveaux traités.

- [redacted]

- Si vous êtes d'accord, j'aimerais bien que vos représentants communiquent à mon bureau les coordonnées d'une personne ressource en cybersécurité au niveau opérationnel. Je veillerai à ce que mes représentants communiquent avec elle.

Environnement de la menace à l'échelon international

- J'aimerais en savoir plus sur le nouveau projet de loi relatif à la sécurité et à la lutte contre le terrorisme, qui a été présenté le 3 octobre 2012.

- Comment la France communique-t-elle au public les menaces nouvelles et émergentes et comment mobilise-t-elle la population?

Incidence du Plan d'action Par-delà la frontière sur la sécurité nationale et l'échange d'informations

- Dans le cadre du Plan d'action Par-delà la frontière, le Canada et les États-Unis continuent à prendre appui sur des assises solides afin d'élargir l'échange d'informations à des fins de sécurité nationale.

- En apprenant à mieux comprendre les systèmes juridiques et opérationnels de chacun, nos deux pays ont réussi à éliminer de nombreux obstacles à l'échange d'informations. Les travaux se poursuivent afin de relever les autres points à améliorer et à prendre les mesures nécessaires.

- Nos services de renseignements mènent ensemble des évaluations conjointes et intégrées de la menace afin que nous puissions comprendre de la même façon les menaces à l'intérieur et à l'extérieur de nos frontières.

France

Official Title French Republic

General Information:

Capital Paris

Total Area 547,030 km2 ***Population (million)*** 63.09

Currency 1 CAN$= 0.73 EURO (EUR)(2011)

National Holiday July 14 , Bastille Day

Language(s) French

Political Information:

Type of State Presidential republic

Type of Government

Semi-presidential democracy. Bicameral parliament with a 348-seat Senate (Sénat) (312 for metropolitan France, 21 for overseas departments and territories, and 12 for French nationals abroad) and a 577-seat National Assembly (Assemblée nationale). Prime Minister nominated by the National Assembly majority and appointed by the President. Council of Ministers (cabinet) appointed by the President on the suggestion of the Prime Minister. Administrative divisions: 26 regions and 100 departments. Governing party: Union for a Popular Movement (UMP).

Head of State President François Hollande

Head of Government
Prime Minister Jean-Marc Ayrault

Ministers Foreign Affairs: Laurent Fabius
Economy and Finance: Pierre Moscovici
Foreign Trade: Nicole Bricq

Main Political Parties

Socialist Party (PS), Union for a Popular Movement (UMP), Democratic Movement (MoDem), French Communist Party (PCF), Diverse Right (DD), Radical Left Party (PRG), Diverse Left (DVG), The Greens, Union of the Center (UDC), Democratic and European Social Rally (RDES), National Front (FN), Centrist Union (UC), Communist, Republican and Citizenship (CRC), Democratic Republican Left (GDR), New Centre (NC). Senate: UMP (132), PS (140), UC (31), CRC (21), RDSE (17), Indep. (7) Nationale Assembly: UMP (317), PS (204), GDR (25), NC (23), Indep. (8).

Elections President: 5 year term; next elections, April 2017. Senate members: 6 year terms; next election, September, 2014.

Economic Information: (2011)

	France	Canada
GDP: (billion)	$2,745.98	$1,720.70
GDP per capita:	$43,527.13	$49,900.00
GDP Growth rate: (%)	1.715	2.4
Inflation: (%)	2.293	2.9
Unemployment: (%)	9.675	7.4

Trade and investment: (2011)

Canadian Exports: $3,080,793,524

Canadian Imports: $5,551,688,769

Foreign Direct Investment in Canada $15,319 ***(million)***

Canadian Direct Investment to France $4,963 ***(million)***

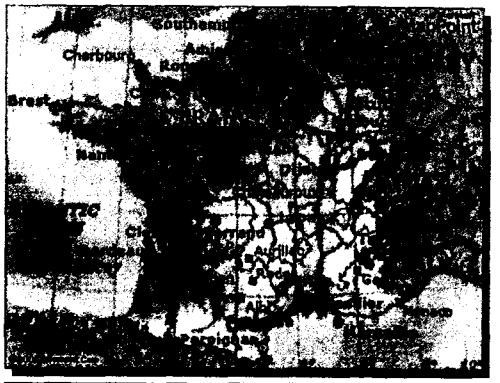
Representation:

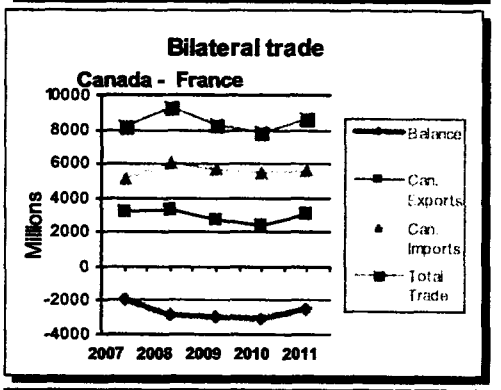
Foreign Representation in Canada

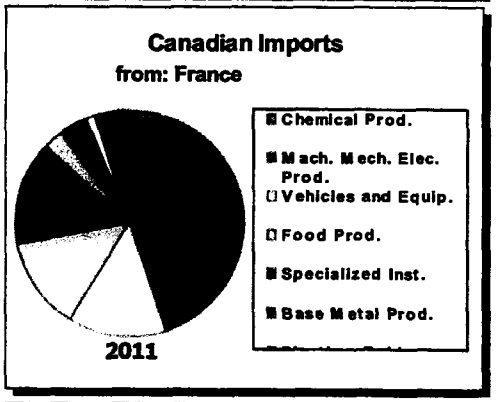
Ambassador Philippe Zeller

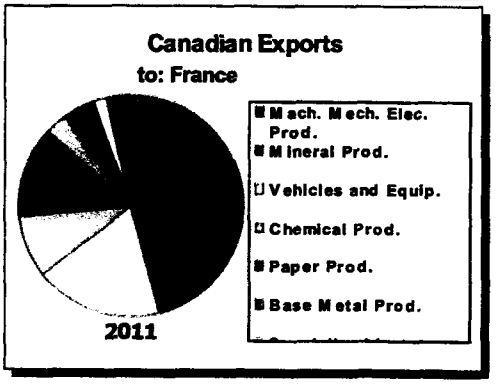
Canadian Representation Abroad

Ambassador Lawrence Cannon









Sources:
Statistics/Industry Canada
http://www.ic.gc.ca/eic/site/tdo-dcd.nsf/eng/Home
IMF
http://www.imf.org/external/data.htm

POLITICAL CONTEXT AND CANADA–FRANCE RELATIONS

ISSUE

France has a new government and is dealing with a difficult economic climate.

BACKGROUND

Political context in France

France is a unitary constitutional republic whose President, François Hollande, was elected in May 2012. President Hollande and his prime minister, Jean-Marc Ayrault, are both from the Socialist Party (SP). Furthermore, given the outcome of the legislative elections in June 2012, the Socialist Party holds the majority of institutional powers for the first time in history.

Four months into his mandate, President Hollande is confronted with a harsh reality: France must streamline its public accounts while contending with a difficult economic climate. Unemployment, which has risen for 16 straight months and is now around 10%, continues to climb. According to a significant segment of public opinion, the government is not doing enough to address the crisis and unemployment. Polls in August and September revealed that Hollande's approval rating has dropped by approximately 10 points to around 45–47%.

On September 28, 2012, Hollande, who was elected on a pro-growth platform, presented a budget that would produce the biggest cut to the public purse in 30 years. The budget, which will be presented to parliament next month, is intended to bring France's annual deficit to 3% of GDP in 2013, down from 4.5% this year. It places heavy emphasis on austerity measures, raising new revenues through corporate and personal taxes, and freezing total government spending. After raising about $9 billion in new taxes and modest cuts this year, with no GDP growth, Hollande had to find an additional $39 billion in this year's budget to hit the 3% goal. About $13 billion will come from new taxes on corporations and an additional $13 billion from new income taxes, including a new higher rate of 45% on incomes over $193,000, and a controversial, largely symbolic and supposedly temporary wealth tax of 75% on earnings over $1.3 million.

In the face of the Europe-wide economic crisis, Hollande has decided on a 3%-target budget: a clear message that France is in line with promises to Brussels. Yet while seeking to open a dialogue on growth revival by aligning himself with Italy and Spain, the President has made more vulnerable the fruitful and strategic Franco-German trust built by his predecessors over the past 5 decades. Now Germany has taken the lead for greater federal integration in Europe while the French government, whose majority on European issues remains divided and fragile, is staying behind.

Foreign policy

Given the scale of the crisis in France and across Europe, economic recovery has become one of the government's priorities. On August 27, 2012, during the traditional President's speech to French ambassadors, Hollande announced the launch of an action plan on "economic diplomacy," aimed in particular at supporting French companies abroad.

On the world stage, as a permanent member of the United Nations Security Council, NATO, the G8 and the G20, a nuclear power, a founding nation of the European Union and a key member of La Francophonie, France plays a leading role on major issues of international concern and is a key ally for Canada.

With respect to Syria, which is currently a major foreign policy priority for France, President Hollande recently encouraged the Syrian opposition to form an inclusive and representative provisional government that can become the legitimate representative of Syria. Hollande also announced that France would recognize such a government once formed. On September 25th, 2012, President Hollande made his first UN speech, in which he called upon the UN to immediately provide protection to areas liberated by rebels in Syria.

Public Safety Canada / Sécurité publique Canada

Border Policy and International Affairs Directorate
Branch / Direction générale
Strategic Policy Branch

Routing Slip / Bordereau d'acheminement

File No / No du dossier : ___CCM : 390536_____RDIMS (Dragon): 3591 _____

Deadline for DM's signature / Échéancier pour la signature du S-M : _____

Assistant Deputy Minister Quality Control / Contrôle de qualité du cabinet du Sous-ministre adjoint(e) : _____

Title / Titre : Meeting with Ange Mancini, French International Intelligence Coordinator, October 9, 2012, 3:30 p.m.-3:30 p.m.		**ACTION REQUIRED / MESURES À PRENDRE**		
Name / Nom	**Date**	**Initials / Initiales**	**Approval or signature / Approbation ou signature**	**Information**
Originator / Auteur Joey Cloutier	5/10/12	JC	☒	☐
Director / Directeur Joey Cloutier	5/10/12	JC	☒	☐
Acting Director General / Directeur général par intérim Megan Nichols		Mpn	☒	☐
Chief Audit Executive / Dirigeante principale de la vérification Rosemary Stephenson			☐	☐
Director General Communications / Directrice générale des communications Stéphanie Durand			☐	☐
Executive Director & Senior General Counsel LS / Directeur exécutif et Avocat général principal SJ Paul Shuttle			☐	☐
Assistant Deputy Minister SP / Sous-ministre adjoint PS Paul MacKinnon			☒	☐
Assistant Deputy Minister LP / Sous-ministre adjoint SPL Richard Wex			☐	☐
Assistant Deputy Minister CM / Sous-ministre adjoint GM Gary Robertson			☐	☐
Assistant Deputy Minister CSP / Sous-ministre adjoint SPP Shawn Tupper			☐	☐
Assistant Deputy Minister EMRO/ Sous-ministre adjointe GMUOR Gina Wilson			☐	☐
Senior Assistant Deputy Minister NS/ Sous-ministre adjointe principale SN Lynda Clairmont			☐	☐
Acting Deputy Minister / Sous-ministre par interim Graham Flack			☐	☒
Minister / Ministre The Honourable / L'honorable Vic Toews			☐	☐

For your meeting with:
Ange Mancini
On: Tuesday, October 9, 2012, at 3:00 p.m.

SECRET

DATE:

FILE No.: 390536
RDIMS (Dragon) No.: 3591

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

MEETING WITH ANGE MANCINI,
FRENCH NATIONAL INTELLIGENCE COORDINATOR

(Information only)

SUMMARY

You will be meeting with Ange Mancini, the French *Coordonnnateur national du renseignement* on Tuesday October 9, 2012, from 3:00 to 3:30, in Boardroom 19C-3100. Mr. Mancini will be accompanied by:

- General Hubert de Reviers de Mauny, Advisor, *Conseil national du renseignement*;
- Vincent Martin Pavailler, Advisor, *Conseil national du renseignement*;
- Alexandre Vulic, First Counsellor, French Embassy;
- Christelle Sarnelli, Liaison Officer, *Direction générale de la sécurité extérieure* (foreign intelligence agency), French Embassy; and
- Colonel Thierry Cailloz, Homeland Security Attaché, French Embassy.

John Davies, Director General, National Security Policy Directorate, will support you at the meeting.

Mr. Mancini's biography is enclosed **(TAB A)**. Proposed key messages, in both English and French, are also attached **(TAB B)**. Information on Canada-France bilateral relations, provided by the Department of Foreign Affairs and International Trade, is enclosed **(TAB C)**.

.../2

STRATEGIC OBJECTIVES

The following are the recommended objectives for the meeting:

- emphasize the importance of the Canada-France public safety bilateral relationship;
- inquire about the upcoming white paper on defence and national security currently being developed, and whether that will lead to significant changes in national security priorities and funding;
- exchange views on approaches to cyber security, the international threat picture, and information-sharing in the context of the Beyond the Border agreement; and
- explore deeper cooperation on cyber issues.

BACKGROUND

France

On May 6, 2012, François Hollande, leader of the Socialist Party, was elected President of France. On May 15, 2012, Mr. Hollande named Jean-Marc Ayrault Prime Minister. Prime Minister Ayrault announced the composition of his Cabinet on May 16, 2012. The Minister's counterpart, Manuel Valls, was appointed Minister of the Interior.

On September 28, 2012, the Government released its first budget. The Government's main objective is to bring down the deficit to 3 per cent of the French GDP in 2013 from the current 4.5 per cent. Cuts include €2.2 B from defence programs and €2.8 B from administrative costs across all ministries. Also announced in the budget is the creation of 480 new police jobs that will be deployed to "priority security areas" – 15 areas identified by Minister Valls where more concerted and sustained efforts will be made to curb youth criminality.

Public Safety Relations

France is identified as [redacted] in the International Strategic Framework. Canada and France have a history of cooperation on various public safety issues.

Law enforcement cooperation between Canada and France is excellent. The Royal Canadian Mounted Police (RCMP) and the *Police nationale* cooperate on a wide range of policing issues, but especially on criminal investigations. Canada and France are both members of the Financial Action Task Force and also contribute to the Caribbean

.../3

Financial Task Force forum, which aims to curtail money laundering and the traffic of drugs in the region. The RCMP works closely with the French domestic security agency, the *Direction centrale du renseignement intérieur* (DCRI), the *Sous-direction de la lutte anti-terroriste* and the *Unité centrale de lutte anti-terroriste* on counter-terrorism investigations. Both Canada and France are contributing civilian police to MINUSTAH. There are Extradition and Mutual Legal Assistance Treaties between Canada and France.

Canada (National Crime Prevention Centre) and France (*Secrétariat général du Comité interministériel des villes*) are both members of the International Centre for Crime Prevention (CIPC)'s Advisory and Policy Committee. The CIPC is located in Montreal, Quebec.

Conseil national du renseignement

As National Intelligence Coordinator to the President, Mr. Mancini heads the *Conseil national du renseignement* (CNR) and oversees its day-to-day activities. Reporting directly to the President, Mr. Mancini is the intelligence agencies' point of entry to President Hollande. Mr. Mancini was appointed in February 2011, replacing Bernard Bajolet, who met with then Deputy Minister Bill Baker in January 2010.

The CNR was born out of the 2008 French *White Paper on Defence and National Security*. The CNR's role is to coordinate intelligence analysis, eliminate redundancies, and fill the gaps in the current intelligence system. The President chairs CNR meetings, which is attended by the Prime Minister and the Ministers of Defence, Interior, Foreign Affairs and Finance, and other ministers as required.

A New White Paper on Defence and National Security for 2013

On July 13, 2012, Jean-Marie Guéhenno, former United Nations' Under-Secretary-General for Peacekeeping Operations, was appointed by President Hollande to head the White Paper Commission, responsible for drafting the document. The *White Paper on Defence and National Security* should be released in early 2013. The objective of the White Paper is to define France's national security priorities and capabilities over the next 15-20 years. Following its release, resources for the defence and national security portfolios for the period of 2014-2019 will be allocated through a military programme bill of law.

Approaches to Cyber Security

Canada-France Cooperation on Cyber Security

Canada, France and over 100 countries will attend the upcoming World Conference on International Telecommunications (WCIT) in Dubai in December 2012 to revise the International Telecommunication Regulations, a treaty binding instrument. Given the binding nature of the Conference outcome,

France's Approach to Cyber Security

France's domestic cyber security efforts are coordinated through the *Agence nationale de la sécurité des systèmes d'information* (ANSSI), created in 2009. ANSSI is responsible for: detecting and responding to cyber attacks against government systems; supporting the development of trusted products and services to protect networks in government and certain economic sectors (i.e. what is known as the supply chain in Canada); providing advice and support to critical infrastructure operators; and public awareness efforts.

Much like PS, ANSSI coordinates cyber security policy with line departments, such as Foreign Affairs, Finance, and Defence. ANSSI reports to the General Secretary for Defence and National Security, who in turn reports to the Prime Minister. Both the General Secretary and Prime Minister sit on the CNR. ANSSI's role is defensive. Charged with protecting and defending both government systems and overseeing the cyber security of critical infrastructure sectors, it has the power to set minimum cyber security requirements for all government departments and order telecommunications providers to undertake actions to strengthen their cyber security, either during a specific cyber incident or as part of routine mitigation measures.

Also responsible for signal intelligence, the DGSE leads France's offensive cyber activities for intelligence and military purposes. While the extent of France's offensive cyber capabilities is unknown, it is generally understood to have the expertise and skill to rival that of some Five Eyes members.

Cyber Threats

While other countries have similar challenges, they are beginning to

.../5

develop mechanisms to facilitate information sharing with the private sector. [redacted] companies. Further, senior U.S. officials have begun denouncing China's economic cyber espionage publicly in Congressional hearings and privately with Chinese officials.

International Threat Environment

Terrorism

France remains a priority target for Islamist extremism, particularly Al Qaeda (AQ)-affiliated extremists, as evidenced by the March 2012 shootings in Toulouse by Mohamed Merah. Interest in France by senior AQ leadership has intensified in recent years, due in large part to France's intervention in Libya, as well and its close relationship to the U.S.

It is also worth noting that the French Minister of the Interior announced on October 3, 2012 the tabling of a *Bill regarding security and combating terrorism*. The bill will permit local arrests of individuals who have visited foreign combat training camps, as well as extend measures that were due to expire this year that allow French police access to the electronic or Internet communications of suspected terrorists.

[redacted]

Should you require additional information, please do not hesitate to contact me at 613-949-6435 or Megan Nichols, Acting Director General, Border Policy and International Affairs Directorate, Strategic Policy Branch, at 613-998-2936.

Paul MacKinnon

s.13(1)(a)
s.15(1) -
Int'l
s.21(1)(a)

Enclosures: (3)

Prepared by: Joey Cloutier

SECRET

MEETING WITH ANGE MANCINI, FRENCH NATIONAL INTELLIGENCE COORDINATOR

Key Messages

Upcoming White Paper and Defence Program Bill of Law

- I am noting with interest that a new White Paper on Defence and National Security is currently being developed.
    - Do you foresee significant changes in national security priorities?
    - Given the €2.2 B cuts in Defence spending already announced in this year's budget and the Government deficit reduction objective, do you anticipate budget cuts in the Defence Program Bill of Law (*Loi de programmation militaire*), to be released in 2013?

Cyber Security

- I understand that the French Government can compel telecommunication providers to take specific measures to strengthen their cyber security. Can you elaborate on the kind of measures the Government can direct the providers to take?

- [redacted]

- I understand that our officials are collaborating at the UN Group of Government Experts on Information Security to develop confidence and security building measures to reduce the risk of state conflict in cyberspace. This offers a more practical alternative to new treaties.

- [redacted]

- If you agree, I would appreciate it if your officials could provide a cyber security contact at the working level to my office. I will ensure that our officials get in touch.

International Threat Environment

- I would be interested in learning more about the newly tabled bill on security and combating terrorism (*Projet de loi relative a la sécurité et a la lutte contre le terrorisme*), tabled on October 3, 2012.

- How does France communicate and engage with the public on new and emerging threats?

Impact of the Beyond the Border Agreement on National Security and Information-Sharing

- Through the Beyond the Border Action Plan, Canada and the United States continue to build upon an already strong foundation of bilateral information-sharing for national security purposes.

- By enhancing our understanding of, each other's legal and operational systems, we have been successful in addressing a number of challenges to information-sharing. Work continues to identify and address other areas of improvement.

- Our intelligence agencies are also working on joint integrated threat assessments in order that we have a common understanding of threats, within, at, and away from our borders.

Main File No. Dossier principal n°

TD No. Dossier temporaire n° 385-377

Subject Objet

Meeting with Roger Wilkins, Australian Secretary
of the Attorney General's Department
June 12, 2012

Government of Canada / Gouvernement du Canada

TEMPORARY DOCKET

DOSSIER TEMPORAIRE

SECRET

SECRET

Date	Referred to Remis à	Remarks Remarques	PA Date à classer	User's Initials Initiales de l'usager	BF Date Date à rappeler
June 7/12					
June 8/12	for AOMO	for approval		MD	
June 11/12	DMO	for info		JB	
JUIN 11 2012	DMO	Received			
JUIN 13 2012	SPB - AOMO	Seen by AOM Flack			
14 25	BPIA	File			
	Bates	fr BPIA files			
		CC Dr-Chim			

- Enclose papers on one case only.
- Quote main file no. on related correspondence.
- BF if unable to complete within 48 hours.

- Joindre les documents relatifs à un seul cas.
- Indiquer le n° du dossier principal et le n° du dossier temporaire sur toute correspondance connexe.
- Rappeler si toute intervention est impossible dans les 48 heures.

Main File No. Dossier principal n° | TD No. Dossier temporaire n°

TD No. Dossier temporaire n° | Main File No. Dossier principal n°

GC-99-3 (88/09) 7530-21-870-3673

Public Safety Canada / Sécurité publique Canada

Branch / Direction générale
Strategic Policy Branch / Border Policy and International Affairs

Routing Slip / Bordereau d'acheminement

File No / No du dossier : CCM388377 RDIMS: Dragon

Deadline for DM's signature / Échéancier pour la signature du S-M : _____

Assistant Deputy Minister Quality Control / Contrôle de qualité du cabinet du Sous-ministre adjoint(e) : _____

Title / Titre : Meeting with Roger Wilkins, Australian Secretary of the Attorney General's Department, June 12, 2012		**ACTION REQUIRED / MESURES À PRENDRE**		
Name / Nom	**Date**	**Initials / Initiales**	**Approval or signature / Approbation ou signature**	**Information**
Originator / Auteur Joey Cloutier			☒	☐
Director / Directeur Glen Linder	8 June 12	GL	☒	☐
Director General / Directeur général Barbara Motzney	8/6/12	BM	☒	☐
Chief Audit Executive / Dirigeante principale de la vérification Rosemary Stephenson			☐	☐
Director General Communications / Directrice générale des communications Stéphanie Durand			☐	☐
Executive Director & Senior General Counsel LS / Directeur exécutif et Avocat général principal SJ Paul Shuttle			☐	☐
Assistant Deputy Minister SP / Sous-ministre adjoint PS Paul MacKinnon			☒	☐
Assistant Deputy Minister LP / Sous-ministre adjoint SPL Richard Wex			☐	☐
Assistant Deputy Minister CM / Sous-ministre adjoint GM Gary Robertson			☐	☐
Assistant Deputy Minister CSP / Sous-ministre adjoint SPP Shawn Tupper			☐	☐
Assistant Deputy Minister EMRO/ Sous-ministre adjointe GMUOR Gina Wilson			☐	☐
Senior Assistant Deputy Minister NS/ Sous-ministre adjointe principale SN Lynda Clairmont			☐	☐
Acting Deputy Minister / Sous-ministre par interim Graham Flack			☐	☒
Minister / Ministre The Honourable / L'honorable Vic Toews			☐	☐

Public Safety Canada | Sécurité publique Canada

Assistant Deputy Minister | Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

Seen by the DM
Vu par le SM

JUIN JUN 12 2012

For your meeting with:
Roger Wilkins, Secretary,
Australian Attorney General's Department
On: Tuesday, June 12, 2012,
1:00 p.m.

SECRET

DATE: JUN 11 2012

File No.: 388377
RDIMS No.: 2508

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

MEETING WITH ROGER WILKINS,
SECRETARY, ATTORNEY GENERAL'S DEPARTMENT

(Information only)

SUMMARY

You will be meeting with Roger Wilkins, the Secretary, Australian Attorney General's Department on Thursday, June 14, 2012, at 1:00 p.m. in the DM's Boardroom. Mr. Wilkins will be accompanied by Louise Hand, Australian High Commissioner to Canada, and Bruce Soars, Deputy High Commissioner. Robert Gordon, Acting Senior Assistant Deputy Minister, National Security and Barbara Motzney, Director General, Border Policy and International Affairs will support you at the meeting.

Biographies **(TAB A)** and key messages **(TAB B)** are enclosed.

[redacted]

s.21(1)(a)

.../2

PUBLIC SAFETY RELATIONS

The Royal Canadian Mounted Police (RCMP) Liaison Officer (LO) in Kuala Lumpur also covers Australia and has a very good working relationship with the Australian Federal Police (AFP). During 2011, the RCMP posted a temporary LO to Canberra to support ongoing efforts to combat migrant smuggling. This temporary post ended in December 2011.

The Canada Border Services Agency (CBSA) also has an LO in Canberra and an Intelligence Liaison Officer who is embedded in Australia's Department of Immigration and Citizenship. CBSA cooperates actively with Australia through the Border Five Conference, the Five Country Conference, Asia-Pacific Economic Cooperation, and the World Customs Organization.

ISSUES

Review of Intelligence Agency Powers

In May 2012, the Australian Attorney General's Department announced proposed changes to the powers of Australian intelligence agencies. Of note, the proposal would permit the Attorney General to make changes to ASIO warrants, and enable the ASIS to provide self-defence and weapons training to individuals cooperating with ASIS.

In advance to moving forward with the proposed legislative changes, the Parliamentary Joint Committee on Intelligence and Security was asked by the Attorney General, Nicola Roxon, to hold public hearings to consider the proposed changes. The Committee is expected to report back by the end of July 2012.

As part of its commitment under the Air India Inquiry Action Plan, Canada has been developing options for an inter-agency review mechanism of Canada's security and intelligence community. While developing options, Public Safety (PS) officials have

.../3

been examining the Australian model of review, particularly the role of the Inspector General of Intelligence and Security. Australia's Inspector General has jurisdiction over all Australian intelligence agencies to determine whether they act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights. Both the Inspector General and the Prime Minister may initiate a review, and the Inspector General has the ability to ask the Prime Minister to look at additional departments and agencies.

[redacted] CSIS's current mandate is to passively collect information about suspected threats and provide advice to other departments and agencies. Amendments to Canada's security and intelligence framework are consistent with allied approaches and will ensure the Government has the authority and the operational flexibility to address and diminish threats.

Countering Violent Extremism

The Government of Australia's *Counter Terrorism White Paper* acknowledged the threat of "homegrown" terrorism and highlighted the importance of building community resilience to violent extremism. In May 2010, then Attorney General Robert McClelland announced $9.7 AUS million ($9.89M CDN) in funding to support a comprehensive government countering violent extremism (CVE) strategy. Its approach uses two mutually supportive streams of activity: traditional law enforcement and security measures, and programs to promote social harmony and community resilience.

Like Canada, Australia recognizes the importance of working with communities to build resilience to counter the influences of violent extremism, and they believe that communities are best placed to develop solutions to local problems. Specific Australian initiatives include:

- Identifying and diverting people at risk of violent extremism;
- Supporting rehabilitation and de-radicalization programs conducted by state and territory police and correctional services;
- Engaging with communities to improve social cohesion and resilience, including through local meetings with focus groups;
- Examining the role of the internet in the radicalization process;
- Improving responses to violent extremist messages and ensuring that they are evidence-based and appropriate to Australian circumstances; and
- Implementing the "Building Community Resilience Youth Mentoring Grants Program", which is a pilot project that provides grants from $5,000 to $200,000 for community-led programming.

.../4

The Australian Government also has a robust international CVE program, which receives approximately $3 million in funding each year from the Department of Foreign Affairs and International Trade, and is supervised by the Ambassador for Counter Terrorism, Bill Paterson. Australia's international CVE program has a strong focus on Southeast Asia, where the threat of terrorism to Australian citizens and interests is greatest.

Cyber Security Operational Cooperation

In November 2009, the *Australian Government Cyber Security Strategy* was announced. The Australian and Canadian strategies are well-aligned, as the focus of both strategies ensure that:

- Citizens are aware of cyber risks and take steps to protect their identities, privacy and finances online;
- Partnerships are established to ensure vital systems and networks are resilient and operate securely; and
- Government ensures its information and communications technologies are secure and resilient.

In June 2011, the Government of Australia announced that it would draft a "Cyber White Paper" to provide an integrated whole-of-government policy framework. It seeks to ensure that Australia can take full advantage of opportunities offered by the online environment while minimizing risks and enhancing trust and confidence in online engagement. This paper is expected to be publicly released soon.

Operationally, Australia's division of responsibilities between its government and national cyber response units is almost identical to that of Canada. Australia's National Cyber Security Operations Centre (CSOC) focuses on the highly sophisticated attacks against government departments, and it is housed within the Defence Department.

Running parallel to the CSOC is CERT Australia, the Australian government's focal point for engaging with the private sector, critical infrastructure and other systems of national interest. CERT Australia is hosted by the Attorney General's Department, and is the first point of contact for cyber security incidents affecting Australian networks.

[redacted] The U5 has national representation from the Canadian Cyber Incident Response Centre (CCIRC) and CERT Australia, respectively.

s.15(1) - Int'l

.../5

In a change which will take effect in 2015, Australia will be co-locating its government CERT with its public CERT. No similar amalgamation is planned in Canada.

One possible area where Canada and Australia may wish to broaden their operational cyber activities is in dealing with cyber threats to control systems, which are important for the running of many facets of critical infrastructure and their security is essential to the protection of critical infrastructure. This effort could also promote additional capability and resiliency within the U5 community.

Protection of Telecommunications Infrastructures

Australia

development of this network, an investment of $38 billion AUS ($38.75 CDN), is the most significant telecommunications reform in Australia's history: it aims to connect 93% of homes, schools and businesses to high speed broadband internet access.

Canada

CCIRC, which works hand in hand with national and international counterparts to collect, analyze and disseminate data on cyber threats, provides intelligence and technical support to the industry, and coordinates the national

.../6

response to any cyber security incident. Also included are strong partnerships built with the telecommunications industry (within the *Canada's Cyber Security Strategy* and the *National Strategy and Action Plan for Critical Infrastructure*), both at the operational and decision making levels, to address security issues within the sector. Further measures will be brought forward as the threat environment dictates.

Migrant Smuggling

Australia

In 2010, more than 130 vessels carried over 6,500 migrants to Australian waters and in 2011, Australia received 69 vessels carrying over 4,500 migrants, primarily from the Middle East and South Asia.

To address this issue, Australia signed an agreement with Malaysia in July 2011, pursuant to which Australia would send the next 800 mass-arrival asylum seekers to a holding centre in Malaysia in exchange for 4,000 refugees. The transfer of irregular migrants to Malaysia was intended to provide a significant disincentive to potential participants in mass arrivals. In August 2011, however, the Australian High Court struck down the agreement. To date, no further initiatives have been announced, and the Australian government has indicated its concern that the absence of offshore processing will lead to an increase in maritime arrivals.

Australia has also been promoting regional cooperation in Southeast Asia through the Bali Process, which it co-chairs with Indonesia. Both Australia and Canada value the Bali Process as it brings participants together to work on practical measures to help combat people smuggling, trafficking in persons and related transnational crimes in the Asia-Pacific region and beyond.

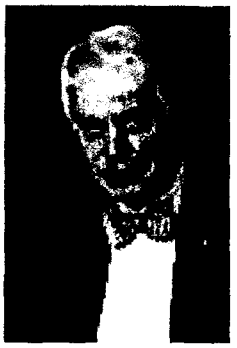
Should you require additional information, please do not hesitate to contact me at 613-949-6435 or Barbara Motzney, Director General, Border Policy and International Affairs Directorate, at 613-949-7260.

Paul MacKinnon

Enclosure: (2)

Prepared by: Joey Cloutier

Roger Wilkins
Secretary – Attorney General's Department



Roger Wilkins AO is Secretary of the Attorney General's Department, a position he has held since September 2008.

Prior to his appointment as Secretary of the Department, he was Head of Government and Public Sector Group Australia and New Zealand with Citi and was Citi's global public sector leader on climate change from 2006-2008.

From 1992-2006, Mr Wilkins was the Director General of the Cabinet Office in New South Wales where he played a leading role in areas of reform in administration and law, corporatisation and micro-economic reform.

Mr Wilkins has chaired a number of national taskforces and committees dealing with public sector reform, including the Council of Australian Government Committee on Regulatory Reform, the National Health Taskforce on Mental Health and the National Emissions Trading Taskforce.

He is a member of the Board of the International Forum of Federations and advises different federal systems especially on fiscal issues.

He was appointed an Officer of the Order of Australia in 2007 for service to public administration

s.19(1)

BIOGRAPHY FOR HER EXCELLENCY MS LOUISE HAND PSM
AUSTRALIAN HIGH COMMISSIONER TO CANADA

Ms Hand is a senior career officer with the Department of Foreign Affairs and Trade. Prior to her appointment as Australian High Commissioner to Canada, Ms Hand was seconded to the Department of Climate Change as the Ambassador for Climate Change (2009 - 2011). Ms Hand has served overseas as Minister and Deputy Head of Mission at the Australian Embassy, Jakarta (2005 to 2009), Ambassador to Cambodia (2000 to 2003), Counselor, Australian Permanent Mission on Disarmament, Geneva (1995 to 1998), and Third later Second Secretary, Australian Embassy, Vienna (1986 to 1989).

In Canberra, Ms Hand has held the positions of Assistant Secretary, Arms Control Branch (1999 to 2000), Director, Ministerial and Executive Liaison Section (1999), Director, Business Affairs Unit (1993 to 1994) and Executive Assistant to the Secretary (1992 to 1993).

Ms Hand holds a Bachelor of Arts and Masters Qualifying degree from the University of Queensland and an MBA from Deakin University. She is married and has two daughters. In January 2009, she was awarded a Public Service Medal for her work in Indonesia.

Suite 710, 50 O'Connor Street, Ottawa, Ontario, K1P 6L2, Canada
Telephone: 1 613 236 0841 Facsimile: 1 613 216 1321

TAB 03

MEETING WITH ROGER WILKINS
SECRETARY, ATTORNEY GENERAL'S DEPARTMENT

KEY MESSAGES

Intelligence Cooperation and Review of Intelligence Agency Powers

- Convey that the Canadian Government is exploring options to create "inter-agency review" of the Canadian security and intelligence community, and that we are very interested in the Australian review model, particularly the work of the Inspector General of Intelligence and Security.

- Convey an understanding that Australia is seeking to implement legislative changes to Australian Intelligence Agencies' powers, including to the domestic security agency's warrant regime, and that we are interested in learning more about the Australian plans.

Approaches to Countering Violent Extremism

- Explain that Sunni Islamist extremism remains the greatest threat to Canada and Canadian interests abroad, and will likely remain such for the foreseeable future.

- Note that a number of individuals in Canada and abroad are involved in terrorism related activities and we are increasingly concerned with:
    - "Lone actor" terrorists – individuals who act alone and outside any formal command structure, and whose actions and behaviour are difficult to predict and profile; and
    - Foreign-based extremist activities and the practice of terrorist groups recruiting and training Canadians to fight in foreign countries.

- With respect to the latter, we are aware of Canadians having travelled or attempted to travel from Canada to Somalia, the Afghanistan-Pakistan tribal areas, and Yemen to engage in terrorism-related activities.

- Note that radicalisation in prisons is also a growing concern in Canada, and that addressing it presents unique challenges.

- Explain that Canada is addressing the threat in a number of ways, including:
    - Coordination of intelligence and law enforcement;
    - Outreach to communities;
    - Research: through the Kanishka Project, Canada will invest $10 million over five years in research on pressing questions of terrorism, counter-terrorism, and violent extremism; and
    - Close relationships with international partners.

Cyber Security Cooperation

- Note that cyber security requires a whole-of-government approach to succeed, along with a strong international dimension.

- Convey your belief that the work the Australians are doing [redacted] towards cyber security links directly on the national effort we are leading here, both in the operational response to cyber incidents, but also to support law enforcement and national and international policy coordination.

- Note that there are many practical ways we can advance between our countries:

    - Indicate that there may be some practical things on CERT-to-CERT cooperation our officials can discuss, and we should have our officials pursue these; and

    - [redacted] has shown real value in addressing some very complicated international issues.

Protection of telecommunications Infrastructures against Cyber Attacks

- Indicate that Canada takes national security very seriously and that a thriving telecommunications industry must fundamentally be a safe and secure one.

- Further indicate that this is particularly important as these networks are the backbone of our economy.

- Explain that Canada has in place the tools and mechanisms to identify, mitigate and address any risk to Canada's telecommunications sector, and that we work with our partners, like Australia, to better leverage knowledge, intelligence and expertise.

- Congratulate Australia on their massive National Broadband Network undertaking:
    - Ask how the Australians see the procurement process unrolling;
    - Ask whether the Australians [redacted]
    - Ask what the Australians see as the key next steps and challenges as the telecommunications sector evolves, in the longer term.

s.15(1) - Int'l

Lawful Access

- Convey that Canada shares Australia's concerns that the capabilities of law enforcement and national security agencies not be lost as a result of developments in the area of technology and telecommunications.

- Indicate your understanding that Australian authorities are able to access information about subscribers from a service provider, without a warrant, and ask whether there were any criticisms from privacy advocates and if so, ask how the Government addresses them.

- Convey your understanding that Australia is expected to propose legislative amendments to ensure that vital investigative tools are not lost, and note that we will be following these developments closely and, in due time, would be interested in hearing how these amendments have advanced Australia's public safety objectives.

Migrant Smuggling

- Explain that the issue of migrant smuggling is a national security priority for our Government.

- Note that two migrant vessels arrived on Canada's west coast in 2009 and 2010.

- Explain that we currently have a Bill before Parliament that we believe will deter those who undertake human smuggling activities, and that will also create disincentives to potential irregular arrivals themselves.

- Convey Canada's appreciation for cooperation between our two countries in the key areas of intelligence, law enforcement and multilateral efforts to combat human smuggling.

For your meeting with:
Roger Wilkins, Secretary,
Australian Attorney General's Department
On: Tuesday, June 12, 2012,
1:00 p.m.

SECRET

DATE:

File No.: 388377
RDIMS No.: 2508

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

MEETING WITH ROGER WILKINS, SECRETARY, ATTORNEY GENERAL'S DEPARTMENT

(Information only)

SUMMARY

You will be meeting with Roger Wilkins, the Secretary, Australian Attorney General's Department on Thursday, June 14, 2012, at 1:00 p.m. in the DM's Boardroom. Mr. Wilkins will be accompanied by Louise Hand, Australian High Commissioner to Canada, and Bruce Soars, Deputy High Commissioner. Robert Gordon, Acting Senior Assistant Deputy Minister, National Security and Barbara Motzney, Director General, Border Policy and International Affairs will support you at the meeting.

Biographies **(TAB A)** and key messages **(TAB B)** are enclosed.

[redacted]

s.21(1)(a)

.../2

PUBLIC SAFETY RELATIONS

The Royal Canadian Mounted Police (RCMP) Liaison Officer (LO) in Kuala Lumpur also covers Australia and has a very good working relationship with the Australian Federal Police (AFP). During 2011, the RCMP posted a temporary LO to Canberra to support ongoing efforts to combat migrant smuggling. This temporary post ended in December 2011.

The Canada Border Services Agency (CBSA) also has an LO in Canberra and an Intelligence Liaison Officer who is embedded in Australia's Department of Immigration and Citizenship. CBSA cooperates actively with Australia through the Border Five Conference, the Five Country Conference, Asia-Pacific Economic Cooperation, and the World Customs Organization.

ISSUES

Review of Intelligence Agency Powers

In May 2012, the Australian Attorney General's Department announced proposed changes to the powers of Australian intelligence agencies. Of note, the proposal would permit the Attorney General to make changes to ASIO warrants, and enable the ASIS to provide self-defence and weapons training to individuals cooperating with ASIS.

In advance to moving forward with the proposed legislative changes, the Parliamentary Joint Committee on Intelligence and Security was asked by the Attorney General, Nicola Roxon, to hold public hearings to consider the proposed changes. The Committee is expected to report back by the end of July 2012.

As part of its commitment under the Air India Inquiry Action Plan, Canada has been developing options for an inter-agency review mechanism of Canada's security and intelligence community. While developing options, Public Safety (PS) officials have

.../3

been examining the Australian model of review, particularly the role of the Inspector General of Intelligence and Security. Australia's Inspector General has jurisdiction over all Australian intelligence agencies to determine whether they act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights. Both the Inspector General and the Prime Minister may initiate a review, and the Inspector General has the ability to ask the Prime Minister to look at additional departments and agencies.

[redacted] CSIS's current mandate is to passively collect information about suspected threats and provide advice to other departments and agencies. Amendments to Canada's security and intelligence framework are consistent with allied approaches and will ensure the Government has the authority and the operational flexibility to address and diminish threats.

Countering Violent Extremism

The Government of Australia's *Counter Terrorism White Paper* acknowledged the threat of "homegrown" terrorism and highlighted the importance of building community resilience to violent extremism. In May 2010, then Attorney General Robert McClelland announced $9.7 AUS million ($9.89M CDN) in funding to support a comprehensive government countering violent extremism (CVE) strategy. Its approach uses two mutually supportive streams of activity: traditional law enforcement and security measures, and programs to promote social harmony and community resilience.

Like Canada, Australia recognizes the importance of working with communities to build resilience to counter the influences of violent extremism, and they believe that communities are best placed to develop solutions to local problems. Specific Australian initiatives include:

- Identifying and diverting people at risk of violent extremism;
- Supporting rehabilitation and de-radicalization programs conducted by state and territory police and correctional services;
- Engaging with communities to improve social cohesion and resilience, including through local meetings with focus groups;
- Examining the role of the internet in the radicalization process;
- Improving responses to violent extremist messages and ensuring that they are evidence-based and appropriate to Australian circumstances; and
- Implementing the "Building Community Resilience Youth Mentoring Grants Program", which is a pilot project that provides grants from $5,000 to $200,000 for community-led programming.

The Australian Government also has a robust international CVE program, which receives approximately $3 million in funding each year from the Department of Foreign Affairs and International Trade, and is supervised by the Ambassador for Counter Terrorism, Bill Paterson. Australia's international CVE program has a strong focus on Southeast Asia, where the threat of terrorism to Australian citizens and interests is greatest.

Cyber Security Operational Cooperation

In November 2009, the *Australian Government Cyber Security Strategy* was announced. The Australian and Canadian strategies are well-aligned, as the focus of both strategies ensure that:

- Citizens are aware of cyber risks and take steps to protect their identities, privacy and finances online;
- Partnerships are established to ensure vital systems and networks are resilient and operate securely; and
- Government ensures its information and communications technologies are secure and resilient.

In June 2011, the Government of Australia announced that it would draft a "Cyber White Paper" to provide an integrated whole-of-government policy framework. It seeks to ensure that Australia can take full advantage of opportunities offered by the online environment while minimizing risks and enhancing trust and confidence in online engagement. This paper is expected to be publicly released soon.

Operationally, Australia's division of responsibilities between its government and national cyber response units is almost identical to that of Canada. Australia's National Cyber Security Operations Centre (CSOC) focuses on the highly sophisticated attacks against government departments, and it is housed within the Defence Department.

Running parallel to the CSOC is CERT Australia, the Australian government's focal point for engaging with the private sector, critical infrastructure and other systems of national interest. CERT Australia is hosted by the Attorney General's Department, and is the first point of contact for cyber security incidents affecting Australian networks.

[redacted] The U5 has national representation from the Canadian Cyber Incident Response Centre (CCIRC) and CERT Australia, respectively.

.../5

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

In a change which will take effect in 2015, Australia will be co-locating its government CERT with its public CERT. [redacted] No similar amalgamation is planned in Canada.

One possible area where Canada and Australia may wish to broaden their operational cyber activities is in dealing with cyber threats to control systems, which are important for the running of many facets of critical infrastructure and their security is essential to the protection of critical infrastructure. [redacted] This effort could also promote additional capability and resiliency within the U5 community.

Protection of Telecommunications Infrastructures

Australia

[redacted] development of this network, an investment of $38 billion AUS ($38.75 CDN), is the most significant telecommunications reform in Australia's history: it aims to connect 93% of homes, schools and businesses to high speed broadband internet access.

Canada

[redacted] CCIRC, which works hand in hand with national and international counterparts to collect, analyze and disseminate data on cyber threats, provides intelligence and technical support to the industry, and coordinates the national

.../6

response to any cyber security incident. Also included are strong partnerships built with the telecommunications industry (within the *Canada's Cyber Security Strategy* and the *National Strategy and Action Plan for Critical Infrastructure*), both at the operational and decision making levels, to address security issues within the sector. Further measures will be brought forward as the threat environment dictates.

Migrant Smuggling

Australia

In 2010, more than 130 vessels carried over 6,500 migrants to Australian waters and in 2011, Australia received 69 vessels carrying over 4,500 migrants, primarily from the Middle East and South Asia.

To address this issue, Australia signed an agreement with Malaysia in July 2011, pursuant to which Australia would send the next 800 mass-arrival asylum seekers to a holding centre in Malaysia in exchange for 4,000 refugees. The transfer of irregular migrants to Malaysia was intended to provide a significant disincentive to potential participants in mass arrivals. In August 2011, however, the Australian High Court struck down the agreement. To date, no further initiatives have been announced, and the Australian government has indicated its concern that the absence of offshore processing will lead to an increase in maritime arrivals.

Australia has also been promoting regional cooperation in Southeast Asia through the Bali Process, which it co-chairs with Indonesia. Both Australia and Canada value the Bali Process as it brings participants together to work on practical measures to help combat people smuggling, trafficking in persons and related transnational crimes in the Asia-Pacific region and beyond.

Should you require additional information, please do not hesitate to contact me at 613-949-6435 or Barbara Motzney, Director General, Border Policy and International Affairs Directorate, at 613-949-7260.

Paul MacKinnon

Enclosures: (2)

Prepared by: Joey Cloutier

MEETING WITH ROGER WILKINS
SECRETARY, ATTORNEY GENERAL'S DEPARTMENT

KEY MESSAGES

Intelligence Cooperation and Review of Intelligence Agency Powers

- Convey that the Canadian Government is exploring options to create "inter-agency review" of the Canadian security and intelligence community, and that we are very interested in the Australian review model, particularly the work of the Inspector General of Intelligence and Security.

- Convey an understanding that Australia is seeking to implement legislative changes to Australian Intelligence Agencies' powers, including to the domestic security agency's warrant regime, and that we are interested in learning more about the Australian plans.

Approaches to Countering Violent Extremism

- Explain that Sunni Islamist extremism remains the greatest threat to Canada and Canadian interests abroad, and will likely remain such for the foreseeable future.

- Note that a number of individuals in Canada and abroad are involved in terrorism related activities and we are increasingly concerned with:
    - Lone actor terrorists – individuals who act alone and outside any formal command structure, and whose actions and behaviour are difficult to predict and profile; and
    - Foreign-based extremist activities and the practice of terrorist groups recruiting and training Canadians to fight in foreign countries.

- With respect to the latter, we are aware of Canadians having travelled or attempted to travel from Canada to Somalia, the Afghanistan-Pakistan tribal areas, and Yemen to engage in terrorism-related activities.

- Note that radicalisation in prisons is also a growing concern in Canada, and that addressing it presents unique challenges.

- Explain that Canada is addressing the threat in a number of ways, including:
    - Coordination of intelligence and law enforcement;
    - Outreach to communities;
    - Research: through the Kanishka Project, Canada will invest $10 million over five years in research on pressing questions of terrorism, counter-terrorism, and violent extremism; and
    - Close relationships with international partners.

Cyber Security Cooperation

- Note that cyber security requires a whole-of-government approach to succeed, along with a strong international dimension.

- Convey your belief that the work the Australians are doing [redacted] towards cyber security links directly on the national effort we are leading here, both in the operational response to cyber incidents, but also to support law enforcement and national and international policy coordination.

- Note that there are many practical ways we can advance between our countries:

  - Indicate that there may be some practical things on CERT-to-CERT cooperation our officials can discuss, and we should have our officials pursue these; and

  - [redacted] real value in addressing some very complicated international issues.

Protection of telecommunications Infrastructures against Cyber Attacks

- Indicate that Canada takes national security very seriously and that a thriving telecommunications industry must fundamentally be a safe and secure one.

- Further indicate that this is particularly important as these networks are the backbone of our economy.

- Explain that Canada has in place the tools and mechanisms to identify, mitigate and address any risk to Canada's telecommunications sector, and that we work with our partners, like Australia, to better leverage knowledge, intelligence and expertise.

- Congratulate Australia on their massive National Broadband Network undertaking:
  - Ask how the Australians see the procurement process unrolling;
  - Ask whether the Australians expect to [redacted]
  - Ask what the Australians see as the key next steps and challenges as the telecommunications sector evolves, in the longer term.

s.15(1) - Int'l

Lawful Access

- Convey that Canada shares Australia's concerns that the capabilities of law enforcement and national security agencies not be lost as a result of developments in the area of technology and telecommunications.

- Indicate your understanding that Australian authorities are able to access information about subscribers from a service provider, without a warrant, and ask whether there were any criticisms from privacy advocates and if so, ask how the Government addresses them.

- Convey your understanding that Australia is expected to propose legislative amendments to ensure that vital investigative tools are not lost, and note that we will be following these developments closely and, in due time, would be interested in hearing how these amendments have advanced Australia's public safety objectives.

Migrant Smuggling

- Explain that the issue of migrant smuggling is a national security priority for our Government.

- Note that two migrant vessels arrived on Canada's west coast in 2009 and 2010.

- Explain that we currently have a Bill before Parliament that we believe will deter those who undertake human smuggling activities, and that will also create disincentives to potential irregular arrivals themselves.

- Convey Canada's appreciation for cooperation between our two countries in the key areas of intelligence, law enforcement and multilateral efforts to combat human smuggling.

For your meeting with:
Nicola Roxon, Attorney-General of Australia
On: Wednesday, June 13, 2012 (TBC), at

SECRET

DATE:

File No.:
RDIMS No.: 619913

MEMORANDUM FOR THE MINISTER

LUNCH WITH NICOLA ROXON, ATTORNEY-GENERAL OF AUSTRALIA

(Information only)

SUMMARY

You will be meeting with Nicola Roxon, the Attorney-General of Australia, on Wednesday, June 13, 2012, at 12:30 p.m. (TBC). The Attorney-General will be accompanied by Ms. Louise Hand, High Commissioner of Australia, and Bruce Soar, the Australian Deputy High Commissioner. You will be accompanied by...

The Australian High Commission has indicated that Attorney-General Roxon can be expected to discuss to discuss cyber security, organised crime and combatting terrorism.

A biography of Attorney-General Roxon is attached **(TAB A)**.

[redacted]

.../2

s.21(1)(a)

PUBLIC SAFETY RELATIONS

The Royal Canadian Mounted Police (RCMP) has a very good working relationship with the Australian Federal Police and the RCMP Liaison Officer (LO) in Kuala Lumpur covers Australia. During 2011, the RCMP posted a temporary LO to Canberra to support ongoing efforts to combat migrant smuggling. This temporary post ended in December 2011.

The Canadian Border Service Agency (CBSA) also has an LO in Canberra and an Intelligence Liaison Officer who is embedded in Australia's Department of Immigration and Citizenship. CBSA cooperates actively with Australia through the Border Five Conference, the Five Country Conference, Asia-Pacific Economic Cooperation, and the World Customs Organization.

ISSUES

Australia's 2011 Independent Review of the Intelligence Community

Prime Minister Gillard commissioned an independent review in December 2010, to take stock of the Australian intelligence community's performance and assess how well agencies are positioned to meet future challenges. Although the review was not prompted by any specific problem in the intelligence community, its timing meets a recommendation of the Inquiry into Australian Intelligence Agencies in 2004, that the intelligence agencies undergo further external review every five to seven years.

The review's principal overarching finding was that Australia's intelligence agencies are performing well with very good levels of cooperation, coordination and collaboration, and between the community and other government agencies. Australia's relationship with its Five Eyes partners was acknowledged as central to building its important national intelligence and security capability.

In addition, the review found that important technological and geopolitical challenges, underway for some time, have now reached a point of maturity. In particular, the review identified China and cyber security as major, emerging challenges for Australia, reconfirming views shared within the intelligence community.

.../3

In the absence of major issues that required significant improvement, some enhancements were suggested to current intelligence processes:

- Strengthening the evaluation of agency and overall Australian Intelligence Community (AIC) performance, and seeking a more evidence-based determination of intelligence priorities;
- Enhanced integration of intelligence missions to further streamline intelligence collection and analysis against the National Intelligence Priorities; and
- Continued improvement of practical cooperation between the AIC and the broader National Security Community agencies.

The vast majority of the review's recommendations were accepted by Government and work is already underway to consider and implement a range of specific proposals from the review. Legislative issues were also explored by the review, with no changes to the current arrangement recommended.

Cyber Security Cooperation with Australia

In November 2009, the *Australian Government Cyber Security Strategy* was announced. The Australian and Canadian strategies are well aligned, as both strategies focus on ensuring that:

- Citizens are aware of cyber risks and take steps to protect their identities, privacy and finances online;
- Partnerships are established to ensure vital systems and networks are resilient and operate securely; and
- Government ensures its information and communications technologies are secure and resilient.

In June 2011, the Government of Australia announced that it would draft a 'Cyber White Paper' to provide an integrated whole of government policy framework. It seeks to ensure that Australia can take full advantage of opportunities offered by the online environment while minimising risks and enhancing trust and confidence in online engagement. This paper [redacted] is expected to be publicly released soon.

In February 2012, [redacted]

.../4

s.13(1)(a)
s.15(1) -
Int'l

[redacted] Hungary will host the next International Cyber Conference in Budapest in October 2012, and it will likely feature Ministerial-level engagement, as was the case for the London Conference.

Migrant Smuggling

In 2010, more than 130 vessels carried over 6,500 migrants to Australian waters and in 2011, Australia received 69 vessels carrying over 4,500 migrants, primarily from the Middle East and South Asia.

To address this issue, Australia signed an agreement with Malaysia on July 25, 2011, pursuant to which Australia would send the next 800 mass-arrival asylum seekers to a holding centre in Malaysia in exchange for 4,000 Convention refugees. The transfer of irregular migrants to Malaysia was intended to provide a significant disincentive to potential participants in mass arrivals. On August 30, 2011, however, the Australian High Court struck down the agreement. To date, no further initiatives have been announced, and the Australian government has indicated its concern that the absence of offshore processing will lead to an increase in maritime arrivals.

Australia has also been promoting regional cooperation in Southeast Asia through the Bali Process, which it co-chairs with Indonesia. Both Australia and Canada value the Bali Process as it brings participants together to work on practical measures to help combat people smuggling, trafficking in persons and related transnational crimes in the Asia-Pacific region and beyond.

The proposed legislation will: make it easier to prosecute migrant smugglers and introduce mandatory minimum sentences for convicted migrant smugglers; make ship owners and operators liable for use of their ships in migrant smuggling; establish mandatory detention of irregular mass arrivals to allow for the determination of identity and admissibility of illegal migrants and any other investigations; and prevent migrants who are part of a smuggling operation from obtaining permanent resident status or bringing their family members to Canada for a period of five years; ensuring that the medical benefits received are not more generous that those received by the average Canadian; and revoking the refugee status of individuals who no longer require Canada's protection – for example, should they leave Canada to return to their country of origin or should country conditions change.

Canada also strengthened its operational cooperation with countries in South and Southeast Asia as well as Western Africa, in an effort to prevent and deter the activities of migrant smuggling groups from successfully launching another vessel destined to Canada.

Should you require additional information, please do not hesitate to contact me at 613-949-6435 or Barbara Motzney, Director General, Border Policy and International Affairs Directorate, at 613-949-7260.

Paul MacKinnon

Enclosure: (1)

Prepared by: Ian Smith-Windsor

BRIEFING NOTE FOR THE DEPUTY MINISTER

CYBER SECURITY

Background

[redacted] Enhancing domestic cyber security in India will benefit Canada and our allies. [redacted] In the international arena, as one of the key emerging economies and a leader within the Group of 77 developing countries (G-77), India can also play an influential role in the international debate on key cyber issues.

Canada has increased its engagement efforts with India on cyber security, including recent visits by Prime Minister Stephen Harper, Canada's National Security Advisor and Public Safety Canada's Senior Assistant Deputy Minister of National Security. A key outcome from the Prime Minister's state visit was a joint statement in which the two countries agreed to work closely together to improve cyber security and broaden their dialogue and cooperation on cyberspace policy.

International Cyber Issues

Two of the key cyber issues currently being debated internationally concern Internet governance and the Budapest Convention. [redacted]

Budapest Convention

The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the first and only international treaty to specifically deal with cybercrime. Some countries (Russia, China and many developing countries) have been reluctant to join the treaty, arguing that aspects of its core elements violate national sovereignty and are instead calling for a new United Nations (UN) cybercrime treaty. Recent reports in the Indian media have suggested that India may be looking to accede to the Budapest Convention. As India is a thought leader within the G-77, [redacted] o support the Budapest Convention.

Canada is an observer of the Council of Europe and contributed to the development of the treaty. The treaty was signed by Canada and its ratification is pending the enactment of legislative amendments contained in Bill C-30, the *Protecting Children from Online Predators Act.*

Internet Governance

The current day-to-day operations of the Internet are managed by a group of non-profit organizations, academics and engineers based primarily in the United States. While Canada and its allies strongly support this multi-stakeholder approach,) want greater state control over the Internet and the information transmitted over it.

This governance debate was front and centre at the recent World Conference on International Telecommunications (WCIT), organized by the International Telecommunications Union (ITU). The ITU is a UN body originally founded in 1865 to regulate telegrams and which today governs telephone communications between countries. At the WCIT, Russia, China and certain Arab states put forward modifications to the International Telecommunication Regulations (ITRs), some of which made reference to the Internet Prior to the conference, Canada and its allies made it clear that such modifications were unacceptable and therefore refused to sign the revised treaty.

A number of European countries and some developing countries, including India, also declined to sign, citing the need to first consult with home governments. India's reasons for not signing the treaty at the WCIT, however, are not entirely clear. In the past India had expressed strong support for an increased role for the UN in overseeing the Internet, but in recent months media reports have signalled a shift in favour of the status quo.

Areas for Possible Canada-India Collaboration

International organisations like the ITU appeal to many emerging and developing countries because they offer access to the expertise, facilities and resources that many of these countries lack to effectively address cyber threats. For example, the ITU recently formed a public-private partnership with the International Multilateral Partnership Against Cyber Threats (IMPACT), which includes the use of IMPACT's state of the art cyber facilities in Malaysia.

There are two areas where collaboration could be enhanced quickly and at relatively low cost:

- **Incident response and investigation** – The Canadian Cyber Incident Response Centre could share best practices and technical expertise with India's Computer Emergency Response Team through reciprocal site visits and exchanging contact information and products. This would enhance collaboration that has taken place on an infrequent basis to date. Similarly, the RCMP could share its expertise on cyber forensics with Indian law enforcement agencies.

s.15(1) - Int'l
s.21(1)(a)

- **Engagement with academia** – India and Canada could open a policy dialogue with academia to develop cyber security training programs and foster innovative research. This could focus on information exchange, including sharing academic papers, research and products, and participation in conferences and events hosted by each country.

Additionally, India is pursuing work on standards for cyber security. We would like to learn more about, India's efforts in this area will be especially important to Canada

s.15(1) - Int'l

CYBER SECURITY

KEY MESSAGES

Budapest Convention

- Express that Canada is a strong supporter of the Budapest Convention (on cybercrime), having signed and helped to negotiate the document in 2001.

- Note that some media reports indicated that India is exploring the possibility of joining the Budapest Convention.

[redacted]

Internet governance

- Comment that Canada supports the current multi-stakeholder model of Internet governance.

- Add that the current model of Internet governance is effective, inclusive, promotes competition, innovation and development for the social and economic benefit of all Internet users.

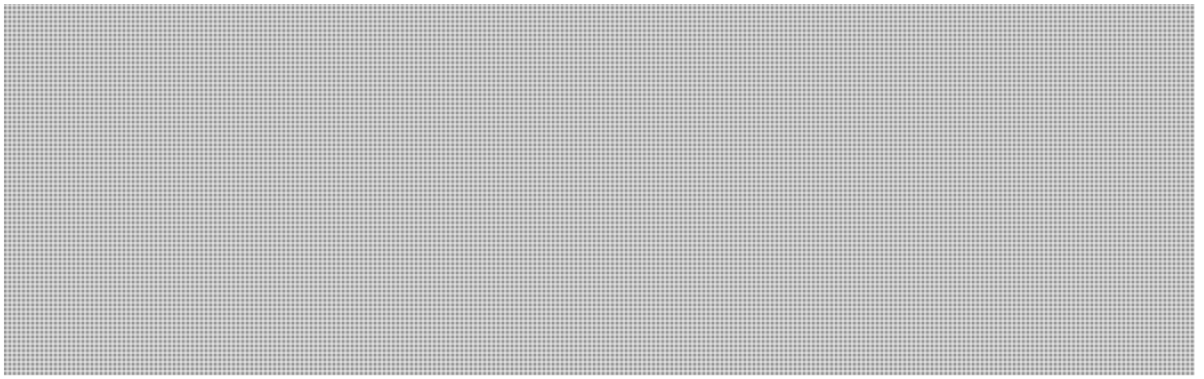
- Explain that these views account for Canada's refusal to sign the revised International Telecommunication Regulations at the World Conference on International Telecommunications in Dubai last month.

- Remark that although much of the revisions to the International Telecommunication Regulations accounted for the current and liberalised telecommunications environment, Canada believes that too many new provisions open the door for increased state control over the Internet.

[redacted]

Areas for Possible Canada-India Collaboration

- Note that Canada considers India to be one of its key cyber security partners.
- Highlight that officials from Public Safety Canada were in India last October and met with various representatives of the Government of India to discuss cyber security.
- Express that there are a number of areas where Canada and India could mutually benefit from working more closely together, such as cooperation between both countries' respective Computer Emergency Response Teams to exchange best practices and technical expertise.
- Add that a similar dialogue between law enforcement agencies working in cyber forensics could also be beneficial and this could be launched fairly quickly by Canada through the organization of reciprocal visits between the Royal Canadian Mounted Police and its Indian counterparts.
- Note the opportunity to work together in engaging with academia to develop training programs and foster innovative research.
- Comment that engagement with the private sector is an important element of *Canada's Cyber Security Strategy* and that Canada is currently working to define the role of government in securing cyber systems in the private sector.



s.21(1)(a)

BRIEFING NOTE FOR THE MINISTER

RESPONSIVE ISSUES

International Cyber Issues

Two of the key cyber issues currently being debated internationally concern Internet governance and the Budapest Convention.

Internet Governance

This was highlighted at the recent World Conference on International Telecommunications (WCIT), a two-week conference to update an international telecommunications treaty.

Canada is opposed to such efforts as they undermine the current Internet governance model where states, the private sector and civil society contribute to decision making.

A resolution annexed to the final text could be interpreted as giving the UN a greater role in managing the Internet. This was one of the many reasons Canada declined to sign the updated treaty

In Canada and developed countries, most critical infrastructure is owned and operated by the private sector.

In late 2010, Jordanian legislative efforts culminated with the passage of the *Information Systems Crimes Law*. This legislation addresses serious criminal activity conducted via the Internet but also includes law enforcement oversight provisions such as warrants and maintenance of law enforcement records.

Budapest Convention

The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the first and only international treaty to specifically deal with cybercrime. Some countries (Russia, China, Jordan and many developing countries) are reluctant to join the treaty, arguing that aspects of its core elements violate national sovereignty and are instead calling for a new UN cybercrime treaty.

Canada is an observer at the Council of Europe and contributed to the development of the treaty. The treaty was signed by Canada and its ratification is pending the enactment of legislative amendments contained in Bill C-30, the *Protecting Children from Online Predators Act.*

Public Safety Canada, through the Canadian Cyber Incident Response Centre, works on an incident by incident basis with international computer emergency readiness teams. This can include cooperation with regional incident response organizations.

Canadian Funding to United Nations Relief and Works Agency for Palestine Refugee in the Near East (UNRWA)

[redacted] Canadian funding to the United Nations Relief and Works Agency for Palestine Refuges in the Near East (UNRWA). As home to nearly two million Palestinian refugees, Jordan relies on UNRWA funding to support this population.

In 2009, CIDA stopped providing funds to UNRWA's general fund, which finances education, health and social services to Palestinian refugees in Jordan, Lebanon, Syria and the West Bank and Gaza. Since then, funding has been provided to food security programming in West Bank and Gaza, in line with Government of Canada development priorities. The announcement of this shift in funding provoked reactions from a number of countries, including Jordan. UNRWA's support to Palestinian refugees in Jordan is derived from the UNRWA's core services budget.

Canada recognizes the important role of UNRWA. Canada's contribution is determined annually based on a variety of factors, including alignment with current aid priorities and availability of resources. While Canada no longer provides funding to the general fund, we contributed $15 million to UNRWA's 2011 Emergency Appeal for West Bank and Gaza.

This funding helped deliver food aid to about 650,000 refugees in Gaza, helped support a school feeding program benefiting more than 200,000 children, and assisted with the creation of more than 82,000 jobs for almost 33,000 refugee families in the West Bank.

s.15(1) - Int'l

BRIEFING NOTE FOR THE MINISTER

CYBER SECURITY

Global Cyber Security Threats and Trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. Intelligence services and militaries are also increasingly supporting, both directly and indirectly, espionage activities which are intended to secure an economic advantage whether through stealing of trade secrets or research, or by interfering in negotiations.

Recognising the magnitude of the challenge, countries have started to pay more attention to cyber security issues and are taking steps to protect themselves. Since 2009, approximately 15 countries, including Australia, Canada, Germany, France, the Netherlands, South Korea, Russia, the UK, and the United States have each released a cyber security strategy.

United Kingdom: The UK updated its *National Cyber Security Strategy* in November 2011. The update included the following measures:

- A new national cyber security hub that will allow government and the private sector to exchange information on threats and responses;
- The establishment of a new Cyber Crime Unit within the National Crime Agency which is meant to be up and running by 2013;
- A new Joint Cyber Unit for the UK military;
- Have the Centre for the Protection for National Infrastructure (CPNI) take a more inclusive approach to defining critical infrastructure;
- Improve the GetSafeOnLine website (the UK equivalent of Canada's GetCyberSafe.ca public awareness campaign) and work with Internet service providers to develop a voluntary code of conduct to help people to determine if their computers have been compromised and what to do about it; and
- Continued emphasis on international dialogue, geared towards maintaining the momentum generated by the London Conference on Cyberspace held in November 2011.

Canada: Public Safety Canada's efforts under *Canada's Cyber Security Strategy* align well with many of the initiatives highlighted in the UK's strategy.

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the Royal Canadian Mountain Police's Integrated Cyber Crime Fusion Centre.

- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks.
- Canada's GetCyberSafe.ca website was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.

Public-Private Information Sharing

United Kingdom: the British government's engagement with the private sector is primarily driven by its intelligence agencies. The CPNI is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage.

Building on the work of the CPNI, in early September the UK formally launched their *Cyber Security Guidance for Business* program, which has released three tailored information products to help the CEOs of the 100 largest British companies address the cyber vulnerabilities of their organizations. Also in September, the UK government announced £3.8M in funding to create a Research Institute in the Science of Cyber Security based at University College London. This Institute is intended to bring together government, the UK signals intelligence agency and seven universities to develop new cyber security solutions, principally focused around cybercrime.

Canada: As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to modernize Canada's frameworks for information sharing accordingly. It may be useful to learn more about the UK's new national security hub for public-private information sharing,

Canada-UK Cooperation

United Kingdom: The UK with the support of like-minded countries, launched the London Conference on Cyberspace on November 1–2, 2011. This process is intended to specifically highlight the linkages between the various aspects of cybersecurity, namely that:

s.15(1) - s.21(1)(a)

- the current governance of the Internet, with a multi-stakeholder model that includes the private sector, has enabled incredible innovations and economic growth;
- going forward, the international community should focus on non-binding norms, which would set out the broad "rules of the road" for cyberspace; and
- existing international law, such as human rights law and the law of armed conflict, apply equally in cyberspace.

Underpinning this normative approach to cyberspace is the idea that no major structural changes to Internet governance or the international system are required to address new cyber issues.

The London Conference on Cyberspace was the first time that these issues were considered in a comprehensive way. It was hosted by the UK Foreign Minister William Hague, featured high-level participation (including from U.S. Vice President Joseph Biden), and brought together representatives from over 60 countries, the private sector and civil society. Hungary is hosting the next Conference in Budapest in October 2012, and it will likely feature similar prominent political engagement.

Canada: Canada has actively supported the UK in its efforts to sponsor norms for cyberspace that promote safe, predictable and consistent interactions while ensuring the Internet's accessibility and openness.

[redacted]

s.15(1) - Int'l (1)(b)

CYBER SECURITY

KEY MESSAGES

Global cyber security threats and trends

- Note that Canada and the United Kingdom have a strong history of working together to address cyber threats and improve our collective security.

- Highlight that the UK's recently updated national cyber security strategy is very compatible with Canada's, particularly its focus on addressing the economic dimension of cyber security.

Public-private information sharing

You may wish to:

- Inquire about the objectives of the "hub" for government and private sector information sharing referenced in the update to the UK's cyber security strategy and how this "hub" would work.

- Ask about the challenges faced by the UK in their efforts to share information to enhance the security of networks and systems.

Canada-UK cooperation

- Note that the Canadian Cyber Incident Response Centre (CCIRC) and its UK counterpart, the Protection for National Infrastructure (CPNI), have an excellent working relationship and routinely share information on malicious websites and computer viruses.

- Express your understanding that Canada strongly supports the UK at the policy level in promoting common interests and policy positions on cyber security.

UNCLASSIFIED

DATE:

File No.: 393309
RDIMS No.: 787149

MEMORANDUM FOR THE DEPUTY MINISTER

PUBLIC SAFETY INTERNATIONAL PRIORITIES FOR WHICH DEPUTY MINISTER ENGAGEMENT IS RECOMMENDED

cc: Lynda Clairmont

(Decision sought)

ISSUE

Recommendations for Deputy Minister (DM) engagements abroad to promote Public Safety (PS) priorities in Canada.

BACKGROUND

The transnational nature of many PS domestic security priorities means that the Department must engage with international partners and organizations to achieve its mission of building a safe and resilient Canada. The DM of PS can contribute greatly to the Department's mission by engaging internationally on several of PS's major priorities.

Further to my initial discussion with you, this memo proposes key trips for you to undertake in the coming year to 18 months, with a view to furthering several strategic priorities. The five visits suggested would support and build key relationships, and include your attendance at a major international cyber security meeting. Note that the international trips proposed are in addition to visits you may make to Washington, D.C. for meetings and events and that all suggestions are made subject to your availability and agreement.

Other Branches, most notably National Security, have been consulted on these recommendations. We have also taken into consideration potential travel by the Minister. His office has indicated his interest in travelling to Paraguay/Brazil and Saudi Arabia/Qatar this year. These are not trips that would necessitate DM accompaniment, and the following recommendations are made on that assumption.

PRIORITIES AND RECOMMENDATIONS

1. Sharing Best Practices and Furthering Common Interests With Like-Minded Allies

.../2

PS engages with allies to share intelligence, expertise, and information relevant to promoting the safety of our citizens. Our primary allies, the United States (U.S.), United Kingdom (UK), Australia, and New Zealand (NZ), along with Canada, established the "Five Eyes" community to facilitate intelligence sharing after World War II.

This group also known as the "Usual Five" has since expanded cooperation in a number of other areas, including policing and border management. Evidence of its ongoing importance includes U.S. plans to host the first U5 meeting of public safety Ministers in the summer of 2013.

The only bilateral agreement signed by the Minister of PS is with Israel and is called the "Canada-Israel Declaration of Intent" (DoI). Under the DoI, PS and Portfolio cooperation is structured into six robust working groups that address specific themes.

Australia and New Zealand, the United Kingdom, and Israel

Our relationships with Australia and NZ would benefit from increased PS engagement at a senior level. Canada and Australia have signed a Memorandum of Understanding to further cooperation on research and defence, and enjoy a strong relationship on law enforcement issues because of close cooperation between the Royal Canadian Mounted Police (RCMP) and the Australian Federal Police. NZ is also an important intelligence ally within the "Five Eyes" community, and Canada provided it with disaster assistance following the devastating 2011 earthquake in Christchurch. Recent engagements include a visit by Senior Assistant Deputy Minister Lynda Clairmont and Special Advisor Robert Gordon to advance cyber security issues. Establishing deeper senior connections with Australian and NZ Ministries and Agencies responsible for public safety is helpful to mitigate the national security and irregular migration threats to Canada from East Asia and the Pacific Region as well as to reaffirm our common approaches to cyber security and the combatting of transnational crime. As such, **we are proposing a visit to Australia and NZ as an early priority for you (Spring 2013).**

While the UK has received both the Minister and Deputy Minister of Public Safety in recent years, continued engagement with this ally is critical to realizing Public Safety's domestic security objectives, particularly concerning the advancement of cyber security, intelligence-sharing, and counter-terrorism efforts. A visit to the UK within the next six months is recommended, given the importance of this partner.

Finally, continued engagement with Israel is a pillar of the Government of Canada's (GoC) foreign policy and a commitment under the DoI. The objectives of your travel would be to emphasize the importance of the DoI; exchange views and best practices on other matters of mutual concern, such as terrorism and the countering of violent

.../3

extremism; and discuss the security situation in Israel and the surrounding region. As a PS delegation will be in Israel this fall for the next DoI meeting (which is not a DM-level engagement), **we propose that you visit Israel later, in Spring 2014.**

2. Engaging to Combat Illicit Drug-Trafficking and Transnational Criminal Organizations

Mexico

Illicit drug-trafficking and transnational criminal organizations pose a significant threat to Canadian public safety. Minister Toews has stated that the dangers of illicit drugs cannot be over-emphasized and are the roots of crime. Mexico is a primary source of narcotics trafficking to Canada, and successful engagement with Mexico is critical to the domestic security of Canada.

PS and its Portfolio engage Mexico on a variety of capacity-building and security-related activities. The RCMP has undertaken a number of capacity-building projects aimed at improving investigative techniques and police reform and professionalization; the Canada Border Services Agency has worked with Mexican border officials to strengthen customs collection and drug interdiction capabilities; and Correctional Service of Canada has shared best practices on corrections practices and reforms. The Department and Portfolio participate in annual security consultations with Mexico, have initiated a dialogue on information-sharing, and are working together to curb irregular migration. PS should engage at senior levels to demonstrate our commitment to this relationship.

In this regard, I am planning a visit to Mexico in mid-May, along with colleagues from the RCMP and CBSA, [redacted] Given the importance of our relationship, and that the Minister is unlikely to visit Mexico in the medium term, **it is recommended that you travel to Mexico to meet with your key counterparts in the Spring of 2014.** Consistent with the Canada-U.S. Beyond the Border commitments to improve hemispheric security through engagement with Mexico, your agenda would focus on what can be done to improve our mutual security and would be a helpful DM-level signal to note the importance that Canada attaches to Mexico.

3. Protect Canada's Cyber Security Interests

PS leads the GoC's international efforts with respect to national cyber security. Along with the U.S., UK, Australia, NZ, and Western European nations, [redacted]

.../4

s.15(1) - Int'l

PS has been an active participant in these conferences and its interventions have helped to shape the global cyber security regime in Canada's interest. PS's National Security Branch has committed to attending the next conference on this issue, with Senior Assistant Deputy Minister Lynda Clairmont scheduled to travel to Seoul, South Korea in October, 2013.

NEXT STEPS

The recommendations outlined in this memo would see you visit all Five Eyes countries by the end of this year, as well as attending the international cyber security conference, and travel to two other countries of key importance in the first part of 2014:

- Australia and New Zealand in Spring/early Summer 2013 (proposed month – June)
- The United Kingdom in Fall, 2013 (proposed month – September)
- South Korea in October, 2013
- Mexico in Spring, 2014
- Israel in Spring, 2014

If you notionally agree with these recommendations, we will work with your office to establish convenient dates for travel and develop relevant programs and briefing materials in consultation with the Department and Portfolio Agencies.

Should you require additional information, please do not hesitate to contact me or Jill Wherrett, Director General, Border Policy and International Affairs, at 613-949-7260.

Paul MacKinnon

s.15(1) - s.21(1)(a)

.../5

Session 5

15:30-17:00 - Focus Issue: Cyber security: Watch this space

Presenters will provide an overview of the scope and variety of cyber threats (political, economic, military) and their implications, and the U.S. policy/organizational response will be outlined.

You have been asked to introduce the two speakers for this event.

- Mr. Chris Painter, Coordinator for Cyber issues, U.S. State Department
- Mr. Bruce McConnell, Counsellor to the National Protection and Programs Directorate for the Deputy Under Secretary, Department of Homeland Security

Briefing material for this introduction is provided on the following page.

Public Safety Senior Assistant Deputy Minister Lynda Clairmont will have concluded cyber security meetings in Washington on the previous day

You will be provided with a briefing on the results of those meetings should the opportunity arise before the afternoon cyber session.

A brief overview of the Department's joint work with the U.S. on cyber security is attached for your information, including a copy of the *Joint Cyber Security Action Plan* recently announced between the Department of Homeland Security and Public Safety **(TAB 1)**.

For your additional reference, a recent cyber-conference speech by your colleague the Deputy Minister of Foreign Affairs is included **(TAB 2)** as well as several recent articles on cyber security issues **(TAB 3)**.

The biographies for Mr. Painter and Mr. McConnell are included **(TAB 4)**.

17:00-17:45 – GTFAD wrap-up – Co-chairs

The session will close with a wrap-up by co-chairs that will provide enough leeway for a timely return to the airport for the return flight.

INTRODUCTORY REMARKS
Session: *Cyber security – Watch this space*
15:30 -16:40

- Good afternoon everyone.

- Across Government, we have been working with our U.S. counterparts to deepen and enhance our already strong bilateral cooperation on cyber security. Many of you work closely with the U.S. Department of Defense, the National Security Agency, the Federal Bureau of Investigation (FBI), and the Department of Justice, just to name a few.

- My department has been working in close collaboration with the U.S. Department of Homeland Security (DHS) on a coordinated approach to cyber security. For example, we recently launched the *Cybersecurity Action Plan* as part of the Beyond the Borders initiative. The Action Plan sets out goals to increase integration across our cyber security activities, ranging from operational cooperation of our Computer Emergency Response Teams (CERTs) to coordinating and aligning our respective public awareness campaigns – the DHS' *Stop.Think.Connect* and PS' *GetCyberSafe*.

- But improving cyber security at home also means advancing our interests and values in the international arena. [redacted] are advocating for state control over cyberspace and the information transmitted over it. [redacted]

- Cyberspace did not grow to become fundamental to our lives and our economic prosperity by being closed and controlled. Our continued prosperity hinges on preserving the open nature of cyberspace. Canada and the U.S., together with our other allies, are fighting to maintain a secure, open and free cyberspace. Internationally we are calling for the continued use of the multi-stakeholder, norms-based approach to Internet governance that has served us well.

- Our two speakers this afternoon are good friends to Canada. We have been working closely together for some time. They have extensive experience in these and other cyber security and cyberspace issues. It is my pleasure to welcome – Mr. Christopher Painter and Mr. Bruce McConnell.

- Mr. Painter is well-known to many of us, both in his current role as the Coordinator for Cyber Issues at the U.S. Department of State and in his previous position as White House as Senior Director for Cybersecurity Policy in the National Security Staff. While at the White House he coordinated the development of the U.S.'s forthcoming international strategy for cyberspace and chaired many high-level interagency groups devoted to international and other cyber issues.

s.15(1) - Int'l

- Mr. Painter also has extensive domestic experience in cybercrime. As an Assistant U.S. Attorney, he led some of the most high profile and significant cybercrime prosecutions in the country. He then moved onto the Computer Crime and Intellectual Property Section of the U.S. Department of Justice and also served, for a short time, as Deputy Assistant Director of the FBI's Cyber Division.

- As I mentioned, DHS is one of Public Safety Canada's key partners. Mr. McConnell is the Cybersecurity Counselor to Deputy Under Secretary of the National Protection and Programs Directorate (NPPD) at the DHS.

- He and his team are leading the development of the DHS's overall cyber security strategy and the implementation of select high-priority Administration initiatives, like the National Strategy for Secure Online Transactions, the National Cybersecurity Public Awareness Campaign, the development of new cyber security authorities for DHS, and the coordination of cyber-related activities across DHS.

- Mr. McConnell also served on the 2008 Obama-Biden Presidential Transition Team, working on a variety of open government and technology issues. Prior to that he had founded McConnell International and Government Futures, a consultancy that provided advice in technology, business and government markets, and had served as Director of the International Y2K Cooperation Center.

- Mr. Painter, Mr. McConnell, I look forward to your presentations and your insights from an American perspective.

CYBER SECURITY ACTION PLAN BETWEEN PUBLIC SAFETY CANADA AND THE DEPARTMENT OF HOMELAND SECURITY

ISSUE

The Cyber Security Action Plan (**TAB A**) between Public Safety Canada and the Department of Homeland Security was released on October 26, 2012.

BACKGROUND

The Beyond the Border Action Plan identified two cyber security priorities. First, protect vital government and critical digital infrastructure of bi-national importance, and make cyber space safer for all our citizens by enhancing the already strong bilateral cyber security cooperation. This will better protect vital digital infrastructure inside and outside government and increase both countries' ability to respond jointly and effectively to cyber incidents.

Second, expand joint leadership on international cyber security efforts by improving engagement with third countries, especially in regard to multilateral forums.

To deliver on those priorities, PS and DHS jointly established the Cyber Security Action Plan. The Action Plan identifies the following four goals to improve engagement, collaboration, and information sharing at the operational and strategic levels with the private sector and in public awareness activities:

1. Enhanced cyber incident management collaboration between National Cyber Operations Centers;
2. Joint engagement and information sharing with the private sector;
3. Expand joint leadership on international cyber security efforts; and
4. Continued cooperation on ongoing cyber security public awareness efforts.

A detailed implementation plan that lays out the specific activities required to accomplish these goals is jointly being developed by PS and DHS. The implementation plan is intended to be a dynamic document and will be reviewed and updated on a regular basis.

A

Perimeter Security
and Economic
Competitiveness

Cybersecurity Action Plan

Between Public Safety Canada and the Department of Homeland Security

Public Safety Canada

Sécurité publique Canada

U.S. DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY ACTION PLAN BETWEEN PUBLIC SAFETY CANADA AND THE DEPARTMENT OF HOMELAND SECURITY

INTRODUCTION

Public Safety (PS) Canada and the Department of Homeland Security (DHS) are pursuing a coordinated approach to enhance the resiliency of our cyber infrastructure. The Cybersecurity Action Plan (the Action Plan) between PS and DHS seeks to enhance the cybersecurity of our nations through increased integration of PS' and DHS' respective national cybersecurity activities and improved collaboration with the private sector. This Action Plan represents just one of many important efforts between Canada and the United States to deepen our already strong bilateral cybersecurity cooperation.

As the Internet knows no borders, all countries have a responsibility to prevent, respond to, and recover from cyber disruptions and to make cyberspace safer for all citizens across the globe. Due to a shared physical border, Canada and the United States have an additional mutual interest in partnering to protect our shared infrastructure. This Action Plan aims to articulate a shared approach to fulfill PS' and DHS' vision of working together to defend and protect our use of cyberspace and to strengthen the resiliency of our nations. These efforts, combined, advance the objectives articulated by President Obama and Prime Minister Harper in the February 2011 declaration, *Beyond the Border: A Vision for Perimeter Security and Economic Competitiveness.*

This Action Plan outlines three goals for improved engagement, collaboration, and information sharing at the operational and strategic levels, with the private sector, and in public awareness activities, for activities conducted by PS and DHS. The Action Plan establishes lines of communication and areas for collaborative work critical to enhancing the cybersecurity preparedness of both nations. The Action Plan's goals and objectives are to be conducted in accordance with the June 2012 *Statement of Privacy Principles by the United States and Canada*. This Action Plan is intended to remain a living document to be reviewed on a regular basis and updated as needed to support new requirements that align to the Plan's key goals and objectives. It intends to support and inform current and future efforts to advance the goals of *Beyond the Border*, which ultimately seeks to enhance broad bilateral cooperation on cybersecurity efforts across both governments.

GOALS AND OBJECTIVES

1. Enhanced Cyber Incident Management Collaboration between National Cybersecurity Operations Centers

PS' Canadian Cyber Incident Response Centre intends to work jointly with DHS' United States Computer Emergency Readiness Team and Industrial Control Systems Cyber Emergency Response Team towards the following objectives:

1.1 Increase real-time collaboration between analysts by improving existing channels for remote communication and arranging in-person visits;

1.2 Enhance information sharing at all classification levels and collaborate on training opportunities, while promoting inter-agency coordination, as appropriate, as well as the proper protections for information, as outlined in the *Statement of Privacy Principles*;

1.3 Coordinate on cybersecurity incident response management, relating to defense, mitigation, and remediation activities and products, including with other public and private entities consistent with each country's laws and policies;

1.4 Align and standardize cyber incident management processes and escalation procedures; and

1.5 Enhance technical and operational information sharing in the area of industrial control systems security.

2. Joint Engagement and Information Sharing with the Private Sector on Cybersecurity

Due to the shared nature of critical infrastructure between Canada and the United States, PS and DHS intend to collaborate on cybersecurity-focused private-sector engagement for cybersecurity activities for which they are responsible through the following objectives:

2.1 Share engagement approaches for private sector;

2.2 Exchange and collaborate on the development of briefing materials for the private sector;

2.3 Jointly conduct private sector briefings;

2.4 Review approaches and align processes for private sector engagement through requests for technical assistance and non-disclosure agreements; and

2.5 Standardize protocols for sharing information.

3. Continued Cooperation on Ongoing Cybersecurity Public Awareness Efforts

Cybersecurity is a shared responsibility and everyone, including our citizens, has a role to play. With increased media attention devoted to cybersecurity incidents and with the continuing growth of electronic commerce and social media, it is imperative that citizens receive clear and trustworthy information on how to manage cyber threats to themselves and their families. Ensuring that government's cybersecurity awareness messages are consistent across our border helps to deliver that information effectively and consistently. PS Communications, the DHS Office of Public Affairs, and the National Protection and Program Directorate's Office of Cybersecurity and Communications (CS&C) intend to continue to work together as they:

3.1 Collaborate on public awareness campaigns (websites, social media activities, education material, etc.);

3.2 Collaborate on Cybersecurity Awareness Month (October); and

3.3 Share and coordinate messaging on issues of common interest.

GOVERNANCE OF THE JOINT ACTION PLAN

Senior officials within PS and CS&C intend to review and provide additional guidance in order to update this Action Plan on a quarterly basis. This Action Plan is intended to be a part of broader inter-governmental coordination across government agencies in both the United States and Canada.

2

The Budapest Conference on Cyberspace, 3-5 October 2012
PLENARY SESSION III: "Sharing knowledge for global challenges" –
Forum of International and Regional Organizations
Speaking Notes
October 5, 2012

Good morning Ladies and Gentlemen.
I am truly pleased to be here on behalf of the Government of Canada. As societies increasingly integrate information technologies into virtually all of what we do, the Internet has become an obviously critical space for human interactions and an engine of global economic growth and development, as it has been underlined eloquently in many different interventions during this important conference.

We know from our own Canadian experience, as a vast geographic space, that the Internet has been essential to our social and economic development, bringing the benefits of connectivity, learning and knowledge to all our communities, from our largest cities to remote communities in the Canadian Arctic in a cost-effective way. Sharing knowledge through the internet and social media allows us to build on the innovation of others, exponentially increasing the reach of our collective trajectory. Canada's experience is that working with international and regional organizations to share knowledge and our own hard-won lessons-learned affords much greater reach in the extension of these benefits beyond our borders.

As an example, at home, Health Canada is investing in "e-Health" initiatives, such as to enable First Nations health centres to have better access to e-health services, and it is similarly supporting such initiatives internationally, such as promoting health e-technologies through the Pan American Health Organization (PAHO). Through the Canadian International Development Agency (CIDA), our experience in implementing distance learning in rural areas has likewise been shared with partners that experience similar challenges, including in Mexico and India. The knowledge gained in overcoming these challenges is of mutual benefit. Most recently Foreign Minister Baird, in Cambodia earlier this summer, announced a $10 million ASEAN fund – a fund which will respond to ASEAN's top priority of advancing its connectivity agenda. We are now working with the ASEAN Secretariat to identify ASEAN-wide projects. These cooperative efforts greatly enhance the impact any one state or organization could have alone.

Beyond innovation and social development, we must recognize that information technology facilitates transparency, accountability and citizen engagement – key components of good governance. Both states and international organizations can use technology to great effect. The Open Government Partnership in which Canada participates and which many international and regional organizations support, uses cyberspace as a vehicle for transparency. Under this umbrella, initiatives such as the International Aid Transparency Initiative provide globally- accessible information on

international assistance flows to individuals and institutions alike - enhancing accountability between governments, international organizations and their citizens. Those involved in such partnerships can better track what assistance is being used for, and what it is achieving, helping us to ensure that each dollar goes as far as possible toward stated goals and to where it is most needed.

Finally, Internet-based platforms are also a tool for citizen engagement – strengthening the responsiveness of governments and international organizations to local needs. As part of our Open Government Action Plan, Canada is developing a new citizen engagement platform that will facilitate public consultations by federal organizations within Canada. Tools like these are also being used to great effect by international organizations to reach across borders and collectively address local challenges by connecting directly with stakeholders. Sharing our experiences and lessons learned in the use of these technologies would be of mutual benefit.

All of these benefits are lost if there is no access. We must work together to build capacity and disseminate knowledge to ensure all of these opportunities are more available. CIDA has been active in promoting internet and communications technologies for development in Africa and Asia and we have seen that the impacts of such technology can be life-changing. For example in Africa, information technology and mobile phones now provide weather and crop information to smallholder farmers, affording key inputs to their decision making and providing a vehicle for them to share their own knowledge with more distant neighbours and improve food security. We have been pleased to support efforts at the Organization of American States (OAS) to share best practices on cyber security and in the Americas, CIDA has also provided support over several years for scores of projects through the Institute for Connectivity of the Americas to promote enhanced connectivity. Canada's International Development Research Centre (IDRC) 's Information and Networks (I&N) program explores, in concert with developing country partners the positive and negative impacts of widespread access to mobile telephones and the Internet in developing countries, and is funding research in partner countries in areas such as "pro-poor" telecommunications policies, and media piracy challenges.

As we have already heard, the openness of cyberspace and our increasing reliance on information technologies bring with it challenges that must be overcome if we are to realize the full benefits of the knowledge-sharing platform that cyberspace provides. This essential openness is more than ever under threat, as some governments seek to censor, control and partition it in the name of national security. There are real concerns about malicious cyber activities which undermine national and individual security, economic prosperity, and free and open societies. These pressures are leading some governments to call for new international instruments, with the apparent aim of better securing cyberspace or more effectively combatting cybercrime.

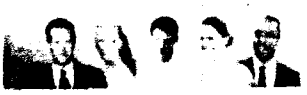
We should not allow the challenges to negate the overwhelming benefits that informational technologies can continue to provide. More control for security could easily result in fewer avenues for innovation and growth, and reduced opportunities for many. Greater centralization of governance could lead to reduced participation and fewer voices being heard, with technological advancements and growth decided by committee rather than being achieved through invention and creativity. In democratizing the Internet, we need to have more voices, not fewer. We cannot lose all that makes cyberspace so invaluable, and reject all the promise it holds, in an effort to protect it.

Let me state where I think our efforts need to go. As opposed to developing new international institutions to govern the Internet, we should work within the existing multi-stakeholder model that has served it so well. The business community, academics, non-governmental organisations, and Internet activities have made seminal contributions to the Internet's development, making it the incredible tool we have become so reliant on. The Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF) embody this multi-stakeholder approach. We should work within these institutions to ensure that the views of all stakeholders, including those of states, are reflected when discussing, debating, and deciding how the Internet should be governed.

International and regional organizations have a critical role as well and every organization should determine its value-added in this already-crowded field. The United Nations, the Organization for Security and Cooperation in Europe (OSCE) and the ASEAN Regional Forum (ARF) are exploring options for confidence and security building measures in cyberspace to reduce the risk of state conflict in this area. The UN Group of Governmental Experts, for example, is working hard to enunciate norms and principle for state behaviour and develop proposals for confidence building measures, including through the exchange of information. The OSCE and ARF are also working on confidence building measures, including commitments to information sharing, which are adapted to the needs and interests of their respective memberships. APEC works to develop and implement telecommunications policies in the Asia-Pacific region to foster economic development.

Canada intends to be active in these and other venues to bring together the widest possible support for a secure, prosperous and open cyberspace. We will work with our partners to promote a vision for the internet that maintains its essential character - the internet as an open and free network, not an over-regulated, censored and controlled cyberspace. We believe that this offers the best opportunity to maximise the economic, social and political benefits of cyberspace, now and for the future generations.
Thank you.

VANITY FAIR

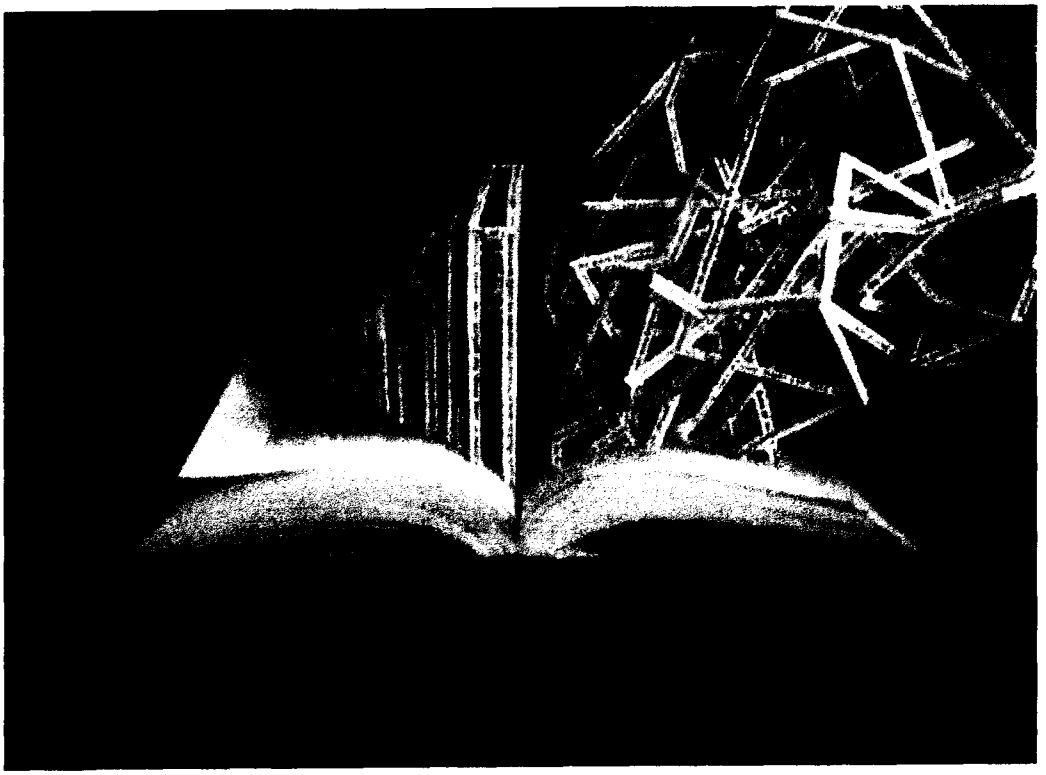


the magazine ▶ May 2012

World War 3.0

When the Internet was created, decades ago, one thing was inevitable: the war today over how (or whether) to control it, and who should have that power. Battle lines have been drawn between repressive regimes and Western democracies, corporations and customers, hackers and law enforcement. Looking toward a year-end negotiation in Dubai, where 193 nations will gather to revise a U.N. treaty concerning the Internet, Michael Joseph Gross lays out the stakes in a conflict that could split the virtual world as we know it.

By Michael Joseph Gross Illustration by Stephen Doyle



i. time bomb

In 1979 the Dubai World Trade Centre dominated the skyline of Dubai City, on the horn of the Arabian Peninsula. Today, the World Trade Centre looks quaint, like an old egg carton stuck into the ground amid a phantasmagoric forest of skyscrapers. But come December the World Trade Centre will once more be the most important place in Dubai City—and, for a couple of weeks, one of the more important places in the world. Diplomats from 193 countries will converge there to renegotiate a United Nations treaty called the International Telecommunications Regulations. The sprawling document, which governs telephone, television, and radio networks, may be extended to cover the

Internet, raising questions about who should control it, and how. Arrayed on one side will be representatives from the United States and other major Western powers, advocating what many call "Internet freedom," a plastic concept that has been defined by Secretary of State Hillary Clinton as the right to use the Internet to "express one's views," to "peacefully assemble," and to "seek or share" information. The U.S. and most of its allies basically want to keep Internet governance the way it is: run by a small group of technical nonprofit and volunteer organizations, most of them based in the United States.

On the other side will be representatives from countries where governments want to place restrictions on how people use the Internet. These include Russia, China, Brazil, India, Iran, and a host of others. All of them have implemented or experimented with more intrusive monitoring of online activities than the U.S. is publicly known to practice. A number of countries have openly called for the creation of a "new global body" to oversee online policy. At the very least, they'd like to give the United Nations a great deal more control over the Internet.

Mediating these forces in Dubai will be a man named Hamadoun Touré. Charming and wily, he is a satellite engineer who was born in Mali, educated in the Soviet Union, and now lives in Geneva. He serves as secretary-general of the U.N.'s International Telecommunication Union (I.T.U.).

Touré abjures pallid diplomatic doublespeak, instead opting for full-on self-contradiction that nonetheless leaves little doubt where his sympathies lie. In one breath Touré says, "The people who are trying to say that I.T.U. has an intention of taking over the management of the Internet simply do not know how the I.T.U. is functioning." In the next, noting that Internet users in America represent only a tenth of the total, he says, "When an invention becomes used by billions across the world, it no longer remains the sole property of one nation, however powerful that nation might be. There should be a mechanism where many countries have an opportunity to have a say. I think that's democratic. Do you think that's democratic?"

There is a war under way for control of the Internet, and every day brings word of new clashes on a shifting and widening battlefront. Governments, corporations, criminals, anarchists—they all have their own war aims.

In February, the Swedish Supreme Court refused to hear appeals from three founders of the Pirate Bay, the world's largest illegal file-sharing Web site, who had been sentenced to prison for copyright infringement. The same day, one of those men issued an online call to arms, urging users to abandon the entertainment industry: "Stop seeing their movies. Stop listening to their music.... Remix, reuse, use, abuse." Shortly after that, Google was discovered to have been secretly bypassing privacy settings on Apple iPhones and computers that use the Safari browser; the company was monitoring Web activity by people who believed they'd blocked such tracking. Around the same time, the European Union proposed that companies such as Google must obtain explicit consent from individuals for data collection; but these regulations would not take effect for years, by which point digital dossiers on almost every Internet user will have been bought and sold by marketers many times over. Meanwhile, the F.B.I. has been distributing "See something, say something" flyers to Internet-café owners in the U.S., warning that the use of certain basic cyber-security measures could be considered grounds for suspicion of possible terrorist activity. In response to the F.B.I.'s growing preoccupation with virtual insurgents, guerrilla hackers operating under the name Anonymous posted online an audio recording of F.B.I. and Scotland Yard officials discussing how to handle Anonymous attacks. Then Interpol, together with American and European authorities, busted 31 suspected

Anonymous hackers—including the one who covertly recorded that conference call—and an F.B.I. official declared victory over LulzSec, one of the most prominent Anonymous splinters, with the boast that "we're chopping off the head" of that faction.

The War for the Internet was inevitable—a time bomb built into its creation. The war grows out of tensions that came to a head as the Internet grew to serve populations far beyond those for which it was designed. Originally built to supplement the analog interactions among American soldiers and scientists who knew one another off-line, the Internet was established on a bedrock of trust: trust that people were who they said they were, and trust that information would be handled according to existing social and legal norms. That foundation of trust crumbled as the Internet expanded. The system is now approaching a state of crisis on four main fronts.

The first is sovereignty: by definition, a boundary-less system flouts geography and challenges the power of nation-states. The second is piracy and intellectual property: information wants to be free, as the hoary saying goes, but rights-holders want to be paid and protected. The third is privacy: online anonymity allows for creativity and political dissent, but it also gives cover to disruptive and criminal behavior—and much of what Internet users believe they do anonymously online can be tracked and tied to people's real-world identities. The fourth is security: free access to an open Internet makes users vulnerable to various kinds of hacking, including corporate and government espionage, personal surveillance, the hijacking of Web traffic, and remote manipulation of computer-controlled military and industrial processes.

There is no agreement about how any of these problems should be solved. There isn't even agreement on how to define the basic terms of debate. "Internet freedom," for instance, is the avowed objective not only of the U.S. secretary of state but also of WikiLeaks, which published hundreds of thousands of classified State Department diplomatic cables.

One way to think about the War for the Internet is to cast it as a polar conflict: Order versus Disorder, Control versus Chaos. The forces of Order want to superimpose existing, pre-digital power structures and their associated notions of privacy, intellectual property, security, and sovereignty onto the Internet. The forces of Disorder want to abandon those rickety old structures and let the will of the crowd create a new global culture, maybe even new kinds of virtual "countries." At their most extreme, the forces of Disorder want an Internet with no rules at all.

A conflict with two sides is a picture we're used to—and although in this case it's simplistic, it's a way to get a handle on what the stakes are. But the story of the War for the Internet, as it's usually told, leaves out the characters who have the best chance to resolve the conflict in a reasonable way. Think of these people as the forces of Organized Chaos. They are more farsighted than the forces of Order and Disorder. They tend to know more about the Internet as both a technical and social artifact. And they are pragmatists. They are like a Resistance group that hopes to influence the battle and to shape a fitful peace. The Resistance includes people such as Vint Cerf, who helped design the Internet in the first place; Jeff Moss, a hacker of immense powers who has been trying to get Order and Disorder to talk to each other; Joshua Corman, a cyber-security analyst who spends his off-hours keeping tabs on the activities of hackers operating under the name of Anonymous; and Dan Kaminsky, one of the world's top experts on the Internet's central feature, the Domain Name System.

Although they may feel a certain kinship with one another, they are not an organized group. Their main point of agreement is that the Internet has changed the world forever,

in ways we are only beginning to understand. They know that Order is impossible and that Disorder is unacceptable. They understand that the world is a messy place whose social arrangements come and go. But they are united in the conviction that what must be preserved and promoted at all costs is what the forces of Order and Disorder, in their very different ways, are both intent on undermining: the integrity of the Internet itself as a reliable, independent, and open structure.

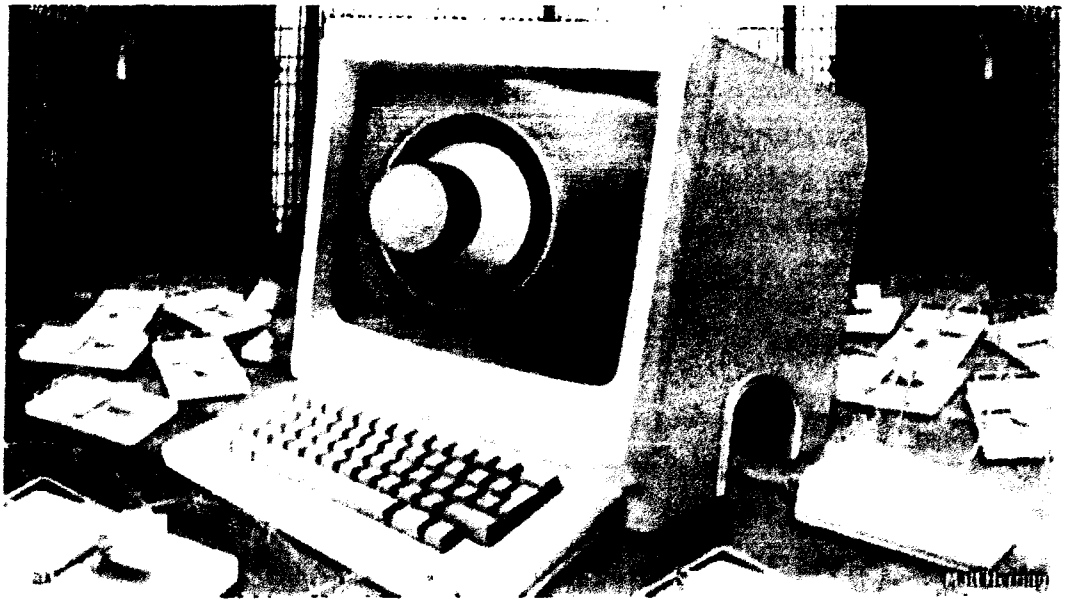
The Economist

Cyber warfare

Hype and fear

America is leading the way in developing doctrines for cyber-warfare. Other countries may follow, but the value of offensive capabilities is overrated

Dec 8th 2012 | from the print edition



EVEN as anxiety about *jihadi* terrorist threats has eased, thanks to the efforts of intelligence agencies and drone attacks' disruption of the militants' sanctuaries, fears over Western societies' vulnerability to cyber-assaults have grown. Political and military leaders miss no chance to declare that cyberwar is already upon us. America's defence secretary, Leon Panetta, talks of a "cyber-Pearl Harbour". A senior official says privately that a cyber-attack on America that "would make 9/11 look like a tea party" is only a matter of time.

The nightmares are of mouseclicks exploding fuel refineries, frying power grids or blinding air-traffic controllers. The reality is already of countless anonymous attacks on governments and businesses. These seek to disrupt out of malice, or to steal swathes of valuable commercial or security-related data. Some experts believe that such thefts have cost hundreds of billions of dollars in stolen R&D.

Many of these attacks are purely criminal. But the most sophisticated are more often the work of states, carried out either directly or by proxies. Attribution—detecting an enemy's fingerprints on a cyber-attack—is still tricky, so officials are reluctant to point the finger of blame publicly. But China is by far the most active transgressor. It employs thousands of gifted software engineers who systematically target technically advanced *Fortune* 100 companies. The other biggest offenders are Russia and, recently, Iran (the suspected source of the Shamoon virus that crippled thousands of computers at Saudi Arabia's Aramco and Qatar's RasGas in August).

America and its allies are by no means passive victims. Either America, Israel or the two working together almost certainly hatched the Stuxnet worm, found in 2010, that was designed to paralyse centrifuges at Iran's Natanz uranium-enrichment plant. The Flame virus, identified by Russian and Hungarian experts this year, apparently came from the same source. It was designed to strike at Iran by infecting computers in its oil ministry and at targets in the West Bank, Syria and Sudan.

Boring, not lurid

For all the hype, policies on cyber-warfare remain confused and secretive. The American government is bringing in new rules and a clearer strategy for dealing with cyber-threats. Barack Obama is said to have signed in October a still-secret directive containing new guidelines for federal agencies carrying out cyber-operations. It sets out how they should help private firms, particularly those responsible for critical national infrastructure, to defend themselves against cyber-threats by sharing information and setting standards.

The directive is partly a response to the stalling of cyber-legislation in the Senate. Republican senators argue that it imposes too great a regulatory burden on industry, which is already obliged to disclose when it is subject to a cyber-attack. It is also meant to govern how far such bodies as the

Department of Homeland Security can go in their defence of domestic networks against malware attacks.

The Pentagon is also working on more permissive rules of engagement for offensive cyber-warfare, for example to close down a foreign server from which an attack was thought to be emanating. General Keith Alexander heads both Cyber Command (which has a budget of $3.4 billion for next year) and the National Security Agency. He has often called for greater flexibility in taking the attack to the "enemy". The emergence of new cyber-warfare doctrines in America is being watched closely by allies who may follow where America leads—as well as by potential adversaries.

However, Jarno Limnell of Stonesoft, a big computer security firm, says that all levels of government in the West lack strategic understanding on cyber-warfare. So, although questions abound, answers are few. For example, it is not clear how much sensitive information about threats or vulnerabilities government agencies should share even with private-sector firms that are crucial to national security. Often the weakest link is their professional advisers, such as law firms or bankers who have access to sensitive data.

Almost all (roughly 98%) of the vulnerabilities in commonly used computer programmes that hackers exploit are in software created in America. Making private-sector companies more secure might involve a controversial degree of intrusion by government agencies, for example the permanent monitoring of e-mail traffic to make sure that every employee is sticking to security rules. Government hackers may also like to hoard such vulnerabilities rather than expose them. That way they can later create "backdoors" in the software for offensive purposes.

Also controversial is the balance between defence and attack. General Alexander stresses that in cyber-warfare, the attacker has the advantage. Mr Limnell says that, although America has better offensive cyber-capabilities than almost anybody, its defences get only three out of ten.

Setting rules for offensive cyber-warfare is exceptionally tricky. When it comes to real, physical war, the capability may become as important as air superiority has been for the past 70 years: though it cannot alone bring victory, you probably can't win if the other side has it.

China has long regarded the network-centric warfare that was developed by America in the late-1980s and copied by its allies as a weakness it might

target, particularly as military networks share many of the same underpinnings as their civilian equivalents. The People's Liberation Army (PLA) talks about "informationisation" in war, "weakening the information superiority of the enemy and operational effectiveness of the enemy's computer equipment". China's planning assumes an opening salvo of attacks on the enemy's information centres by cyber, electronic and kinetic means to create blind spots that its armed forces would then be able to exploit. Yet as the PLA comes to rely more on its own information networks it will no longer enjoy an asymmetric advantage. Few doubt the importance of being able to defend your own military networks from cyber-attacks (and to operate effectively when under attack), while threatening those of your adversaries.

But to conclude that future wars will be conducted largely in cyberspace is an exaggeration. Martin Libicki of the RAND Corporation, a think-tank, argues that with some exceptions cyber-warfare neither directly harms people nor destroys equipment. At best it "can confuse and frustrate...and then only temporarily". In short, "cyber-warfare can only be a support function" for other forms of war.

Four horsemen

Besides the cyber element of physical warfare, four other worries are: strategic cyberwar (direct attacks on an enemy's civilian infrastructure); cyber-espionage; cyber-disruption, such as the distributed denial-of-service attacks that briefly overwhelmed Estonian state, banking and media websites in 2007; and cyber-terrorism. Gauging an appropriate response to each of these is hard. Mr Limnell calls for a "triad" of capabilities: resilience under severe attack; reasonable assurance of attribution so that attackers cannot assume anonymity; and the means to hit back hard enough to deter an unprovoked attack.

Few would argue against improving resilience, particularly of critical national infrastructure such as power grids, sewerage and transport systems. But such targets are not as vulnerable as is now often suggested. Cyber-attacks on physical assets are most likely to use what Mr Libicki calls "one-shot weapons" aimed at industrial control systems. Stuxnet was an example: it destroyed perhaps a tenth of the Iranian centrifuges at Natanz and delayed some uranium enrichment for a few months, but the vulnerabilities it exposed were soon repaired. Its limited and fleeting success will also have

led Iran to take measures to hinder future attacks. If that is the best that two first-rate cyber-powers can do against a third-rate industrial power, notes Mr Libicki, it puts into perspective the more alarmist predictions of impending cyber-attacks on infrastructure in the West.

Moreover, anyone contemplating a cyber-attack on physical infrastructure has little idea how much actual damage it will cause, and if people will die. They cannot know if they are crossing an adversary's red line and in doing so would trigger a violent "kinetic" response (involving real weapons). Whether or not America has effective cyber-weapons, it has more than enough conventional ones to make any potential aggressor think twice.

For that reason, improving attribution of cyber-attacks is a high priority. Nigel Inkster, a former British intelligence officer now at the International Institute for Strategic Studies, highlights the huge risk to the perpetrator of carrying out an infrastructure attack given the consequences if it is detected. In October Mr Panetta said that "potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests."

He may be over-claiming. Given that cyber-attacks can be launched from almost anywhere, attribution is likely to remain tricky and to rely on context, motive and an assessment of capabilities as much as technology. That is one reason why countries on the receiving end of cyber attacks want to respond in kind—ambiguity cuts both ways. But poor or authoritarian countries attacking rich democratic ones may not have the sorts of assets that are vulnerable to a retaliatory cyber-attack.

The difficulty is even greater when it comes to the theft (or "exfiltration", as it is known) of data. For China and Russia, ransacking Western firms for high-tech research and other intellectual property is tempting. The other way round offers thinner pickings. In 2009 hackers from an unnamed "foreign

intelligence agency" made off with some 24,000 confidential files from Lockheed Martin, a big American defence contractor. As a result they could eavesdrop on online meetings and technical discussions, and gather information about the sensors, computer systems and "stealth" technology of the F-35 Joint Strike Fighter. This may have added to the delays of an already troubled programme as engineers tried to fix vulnerabilities that had been exposed in the plane's design. Investigators traced the penetrations with a "high level of certainty" to known Chinese IP addresses and digital fingerprints that had been used for attacks in the past. Less than two years later, China unveiled its first stealth fighter, the J-20.

Theft from thieves

As Mr Libicki asks, "what can we do back to a China that is stealing our data?" Espionage is carried out by both sides and is traditionally not regarded as an act of war. But the massive theft of data and the speed with which it can be exploited is something new. Responding with violence would be disproportionate, which leaves diplomacy and sanctions. But America and China have many other big items on their agenda, while trade is a very blunt instrument. It may be possible to identify products that China exports which compete only because of stolen data, but it would be hard and could risk a trade war that would damage both sides.

Cyber-disruption has nuisance value and may be costly to repair, but it can be mitigated by decent defences. Cyber-terrorism has remained largely in the imagination of film-makers, but would be worth worrying about if it became a reality. Stonesoft's Mr Limnell reckons that, though al-Qaeda and its offshoots show little sign of acquiring the necessary skills, they could buy them. Mr Libicki is more sceptical. Big teams of highly qualified people are needed to produce Stuxnet-type effects, which may be beyond even sophisticated terrorist groups. Also, the larger the team that is needed, the more likely it is to be penetrated.

The Obama administration's attempt to develop a more coherent—and perhaps less secret—doctrine of cyber-warfare is sensible so long as it is not just an excuse for hyping something that, as far as is known, has yet to kill anybody. The idea that offence beats defence is also suspect. If more attention were paid to fixing the security flaws in Western software, cyber-attackers would have fewer entry points. And more effort should be put into solving the attribution problem. Getting caught is a deterrent that state actors

take seriously. But given that the essence of cyber-warfare is ambiguity and uncertainty, gaining clarity and certainty will be exceptionally difficult. That makes policy both hard to construct and harder still to explain.

from the print edition | International

4

Christopher PAINTER

Coordinator for Cyber Issues, Department of State

Before being appointed Coordinator for Cyber Issues at the Department of State in February 2011, Mr. Painter served in the White House as Senior Director for Cybersecurity Policy in the National Security Staff. He coordinated the development of a forthcoming international strategy for cyberspace and chaired high-level interagency groups devoted to international and other cyber issues.

Mr. Painter began his federal career as an Assistant U.S. Attorney in Los Angeles where he led some of the most high profile and significant cybercrime prosecutions in the country. He subsequently helped lead the case and policy efforts of the Computer Crime and Intellectual Property Section in the U.S. Department of Justice and served, for a short time, as Deputy Assistant Director of the F.B.I.'s Cyber Division. Mr. Painter has represented the United States in numerous international fora, including Chairing the G8 High Tech Crime Subgroup since 2002. He has worked with dozens of foreign governments in bi-lateral meetings and has been a frequent spokesperson and presenter on cyber issues around the globe. He is a graduate of Stanford Law School and Cornell University.

Bruce W. McCONNELL

Cybersecurity Counselor to Deputy Under Secretary Philip Reitinger, National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security

On June 1, 2009 Bruce McConnell was appointed by Secretary Janet Napolitano to serve as Senior Counselor in the National Protection and Programs Directorate, U.S. Department of Homeland Security. McConnell serves as senior advisor on a host of strategic and policy matters related to NPPD and its components, with a particular focus on cybersecurity.

In May 2010, McConnell was tasked with leading the NPPD Cyber + Strategy Team. Under his leadership, McConnell's Cyber + Strategy Team is responsible for developing the overall cybersecurity strategy for DHS, aligned with the national strategy developed by the White House National Security Staff.

McConnell's Cyber + Strategy Team is leading implementation of select high-priority, Administration initiatives, such as the National Strategy for Secure Online Transactions, the National Cybersecurity Public Awareness Campaign, the development of new cyber security authorities for DHS, and the coordination of cyber-related activities across DHS.

Prior to DHS McConnell served on the Obama-Biden Presidential Transition Team, working on a variety of open government and technology issues. From 2000-2008 he created, built, and sold McConnell International and Government Futures, boutique consultancies that provided strategic and tactical advice in technology, business and government markets. Previously, McConnell was Director of the International Y2K Cooperation Center, where he coordinated regional and global critical information technology infrastructure organizations to promote information sharing and joint action, from 1999-2000.

McConnell was Chief of Information Policy and Technology in the U.S. Office of Management and Budget from 1993-1999, where he led the government-industry team that reformed U.S. encryption export policy, created an information security strategy for government agencies, redirected government technology procurement and management along commercial lines, and extended the presumption of open government information onto the Internet.

McConnell received an M.P.A. from the University of Washington and a B.S. from Stanford University.

Public Safety Canada | Sécurité publique Canada

Assistant Deputy Minister | Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

SECRET

DATE: MAR 1 2 2013
File No.: 393958
RDIMS No.: Dragon 5741

MEMORANDUM FOR THE DEPUTY MINISTER

MEETINGS WITH SENIOR OFFICIALS IN WASHINGTON, D.C., MARCH 14, 2013

(Information only)

ISSUE

You will travel to Washington, D.C., on March 13, 2013, to support Minister Toews at his bilateral meeting with Secretary Napolitano, on March 14, 2013, (material for this meeting has been sent to you under a separate cover). During your visit you will also be meeting with senior U.S. officials. These officials include: Nicholas J. Rasmussen, Principal Deputy Director of the National Counter-Terrorism Center; Deputy Attorney General James Cole; and Michael Daniel, Special Assistant to the President, Cybersecurity Coordinator.

The itinerary for your visit and a list of key contacts **(TAB 1-A)** are enclosed. You will be supported by me and by Heather De Santis, Counsellor (Public Safety) at the Canadian Embassy in Washington, D.C.

STRATEGIC OBJECTIVES

These three senior U.S. officials play key leadership roles in the areas of counter-terrorism, justice, and cyber security. These meetings represent a first opportunity for you to meet and build relationships with your U.S. counterparts. Speaking points for the meetings **(TAB 1-B)** are enclosed.

Nicholas J. Rasmussen, Principal Deputy Director, National Counter-Terrorism Centre (NCTC)

The NCTC has a broad mandate to lead the U.S. counterterrorism efforts by analyzing and integrating all terrorism intelligence, sharing information with key partners and conducting strategic operational planning for counterterrorism activities. The closest Canadian counterpart to NCTC is the Integrated Terrorism Assessment Center (ITAC).

.../2

Your meeting with Mr. Rasmussen represents an opportunity to:

[redacted]

Material to support you in this meeting is enclosed **(TAB 2-A)**.

Meeting with Deputy Attorney General James Cole

The mission of the Office of the Attorney General is to supervise and direct the administration and operation of the Department of Justice. The Department of Justice includes the Federal Bureau of Investigation, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, Bureau of Prisons and the Office of Justice Programs.

In the past, Deputy Ministers of PS have not met regularly with the Deputy Attorney General (apart from at the Cross Border Crime Forum (CBCF)). However, developing this relationship is important, both for managing PS/Justice-related issues and between CBCF meetings and in the context of the Beyond the Border Action Plan.

s.15(1) -
s.21(1)(a)

.../3

Your meeting with Deputy Attorney General Cole represents an opportunity to:

- Acknowledge the good working relationship between PS and US DoJ components including at the CBCF and in the implementation of Beyond the Border;

- During this meeting Mr. Rasmussen may raise other issues, they may include:
  -
  - Ratification of the Budapest Convention;

Material to support you in this meeting is enclosed **(TAB 2-B)**.

Meeting with Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator

Michael Daniel leads interagency development of national cybersecurity strategy and policy and oversees agency implementation of these policies. He is also responsible for the U.S. government's engagement with and partnerships with the private sector, non-governmental organizations, other branches and levels of government, and other countries.

Your meeting with Mr. Daniel represents an opportunity to:

- Note that Canada is equally grappling with these issues and highlight the extensive collaboration and good working relationship between Canada and the U.S. on cyber security issues, particularly the joint Cybersecurity Action Plan;

- Seek Mr. Daniel's views on how the Executive Order has been received in the business community and what legislative measures Congress is likely to take; and

.../4

s.15(1) -
s.21(1)(a)

- Note Canada's participation at the upcoming [redacted]

Material to support you in this meeting is enclosed (**TAB 2-C**).

Should you require additional information, please do not hesitate to contact me or Jill Wherrett, Director General, Border Policy and International Affairs at 613-949-7260.

Paul MacKinnon

Enclosures: (1)

Prepared by: Arjun Vinodrai

s.15(1) - Int'l

MEETING WITH DEPUTY ATTORNEY GENERAL JAMES COLE	
Cross Border Crime Forum	• Canada highly values bilateral collaboration fostered through the CBCF. Strengthening our cooperation on cross-border criminality issues is critical to enhancing public safety and security at both the domestic and regional levels. [redacted]
Beyond the Border Action Plan	• The collaboration between our officials to implement the Beyond the Border Action Plan allows us to enhance security at our perimeter, counter violent extremism, and improve intelligence on common threats. o We've been cooperating to counter violent extremism. It is helping increase our collective capacity to respond to this complex and multi-faceted issue. o Public Safety has been funding important research on CVE through the Kanishka program. We were pleased to have several researchers funded by your Department, as well as Homeland Security present at the opening conference in November 2012. o I also know that PS and RCMP officials were pleased to participate recently in the launch meeting of the National Institute of Justice Domestic Radicalization Program that your Department held here in Washington on February 7-8, 2013. [redacted] • We've also made progress made on the national security information sharing Beyond the Border action item. Some of the results that have been achieved through Canada-U.S. cooperation in this area include: [redacted] • It was also good to see that the Joint Statement of Privacy Principles was successfully launched last Summer. [redacted]
Canadian Release of Public Report on the Terrorist Threat	• We will release an annual public report on the terrorist threat. This report will be published in Spring 2013. • I am interested in your views on how the terrorist threat environment has evolved over the past year.

s.15(1) - Int'l

Reactive Only Issues	
Protections/Next Generation Pilot Projects	• [redacted] •
Cross Border Luring	[redacted]
Budapest Convention	• Canada is fully committed to the Budapest Convention. We are actively promoting it as the international standard to facilitate law enforcement cooperation and mutual legal assistance on cybercrime. • In 2012, the Government introduced Bill C-30 (the Protecting Children from Internet Predators Act), which included the required legislative amendments to allow Canada to ratify the Convention. While this Bill is no longer proceeding through our Parliamentary process we remain committed to the ratification of the convention.

s.13(1)(a)

s.15(1) - Int'l
s.21(1)(c)
s.21(1)(d)

MEETING WITH LISA MONACO DEPUTY NATIONAL SECURITY ADVISOR FOR HOMELAND SECURITY AND COUNTERTERRORISM	
Counter-Terrorism Issues	• As part of our commitment under Canada's Counter-terrorism Strategy, we intend to release a public report on the terrorist threat later this spring. I'm interested in your views in how the terrorist threat environment has evolved over the past year. • The public report addresses some key developments in 2012 including changes in the threat of international state-supported terrorism posed by Iran and Syria, the impact of the Syrian civil war, developments in Africa, and the state of al Qaida and its affiliates.
Beyond the Border Action Plan	• We are very pleased with the progress made on the joint threat assessments under The Beyond the Border Action Plan. [redacted] •
Reactive Only Issues	
Canadian involvement in recent attacks	• Recent high profile attacks in Bulgaria and Algeria allegedly involving Canadians raised public attention to the phenomenon of Canadians travelling overseas to participate in terrorist acts. • The Royal Canadian Mounted Police is investigating allegations of Canadian involvement in the recent attacks in Algeria and Bulgaria. • Proposed changes to the Criminal Code that seek to improve Canada's ability to address terrorist travel are currently before Parliament. • We understand that the United States has recently launched a National Strategy for Information Sharing and Safeguarding. • Our Government has launched an internal safeguarding initiative as well. This is an interdepartmental initiative to address the issues identified by our Allies and our own internal assessment of security and information protocols.

s.15(1) - Int'l

MEETING WITH MICHAEL DANIEL SPECIAL ASSISTANT TO THE PRESIDENT AND CYBERSECURITY COORDINATOR	
Cyber	• We value the close relationship we have with the United States on cyber security issues. • Cyber issues cross borders and coordinated action is required to address them. • I am pleased to see our collaboration deepening. I understand that, as part of the action plan on cyber security between my department and the Department of Homeland Security, we have had cyber incident handlers working side-by-side as part of an exchange. • We have also provided joint classified cyber security briefings to cross-border critical infrastructure sectors. • Internationally, we are working with U.S. officials and our Five Eyes partners to take more assertive positions to promote our shared cyber security interests. • [redacted] • We are particularly interested in the Executive Order and how it has been received in the business community. What has been the private sector's reaction and how are you engaging them? • [redacted] • [redacted] • My officials are looking forward to the upcoming [redacted] meeting [redacted] This will be an excellent opportunity to discuss issues [redacted]

s.15(1) - Int'l

1924

MEETING WITH DEPUTY ATTORNEY GENERAL JAMES COLE

ISSUE

You will be meeting with Deputy Attorney General (DAG) James Cole from 2:00 to 2:30 p.m. on Thursday, March 14, 2013 (biography at **TAB 2-A-1**). The meeting will take place at the U.S. Department of Justice, 950 Pennsylvania Avenue.

BACKGROUND

The Attorney General is the head of the Department of Justice and the chief law enforcement officer of the federal government. The Attorney General represents the U.S. in legal matters generally and gives advice to the President and to the heads of the executive departments of the government when requested. The mission of the Office of the Attorney General is to supervise and direct the administration and operation of the Department of Justice. The Department of Justice includes the Federal Bureau of Investigation, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, Bureau of Prisons, Office of Justice Programs, the U.S. Attorneys, and the U.S. Marshals Service.

The Deputy Attorney General is authorized to exercise all the power and authority of the Attorney General, except where such power or authority is prohibited by law from delegation or has been delegated to another official. The Deputy Attorney General advises and assists the Attorney General in formulating and implementing Departmental policies and programs and in providing overall supervision and direction to all organizational units of the Department.

TOPICS FOR DISCUSSION

Cross Border Crime Forum (CBCF)

The CBCF brings together Canadian and American senior law enforcement and justice officials, with a view to resolving cross-border law enforcement and justice policy and operational impediments. The Co-Chairs of the CBCF are the Minister of Public Safety, the Minister of Justice, the U.S. Secretary of Homeland Security, and the U.S. Attorney General. The last meeting was held in March 2012 in Ottawa.

[redacted]

[redacted]

Beyond the Border Action Plan (BTB)

As DAG Cole's Department is involved with a number of action items in the Beyond the Border Action Plan (BTB), you may wish to acknowledge the contribution of U.S. DOJ to the progress a number of items including: Privacy Principles and Countering Violent Extremism.

PS, along with Justice Canada, negotiated the Joint Statement of Privacy Principles with U.S. DOJ and the Department of Homeland Security. It was released on June 28, 2012. It is designed to guide and inform the sharing of personal information in specific initiatives and arrangements under the BTB. [redacted]

U.S. DOJ components are active in the working group that implements the BTB commitment to cooperate to counter violent extremism. This group is co-chaired by PS and DHS. In support of this work, PS and the RCMP recently participated in the launch meeting of the National Institute of Justice Domestic Radicalization Program on February 7-8, 2013, in Washington, DC.

U.S. DOJ components are also involved with PS-led action items related to joint threat assessment and cross-border intelligence and information sharing.

s.15(1) - Int'l

Protections/Next Generation Pilot Projects (Reactive Only)

The Beyond the Border Action Plan proposed that PS, the Royal Canadian Mounted Police, Justice Canada work with the U.S. Department of Homeland Security and the U.S. Department of Justice to deploy two "Next Generation" pilot projects by Summer 2012.

Next Generation pilot projects would create integrated cross-border teams to operate on land in the areas of intelligence, criminal investigations, and establish an intelligence-led uniformed presence between ports of entry. The pilot projects would be based on the proven cross-border policing approaches that were introduced in the marine context by Shiprider, and incorporate best practices and successes of other existing border law enforcement programs.

Canadian Release of Public Report on the Terrorist Threat

During your meeting, you may wish to note that the Government of Canada will soon be releasing its first public annual report on the terrorist threat. This report is expected to be published in Spring 2013 as part of Canada's Counter-Terrorism Strategy. The purpose of this report will be to better inform Canadians of the evolving domestic and international threat environment from a unique whole-of-government perspective. It is anticipated that the report will serve as an important publication for the security and intelligence community in their dialogue with Canadians and our international partners on terrorism. While raising this issue, you may wish to ask DAG Cole for views on how the terrorist threat environment has evolved over the last year.

s.15(1) - Int'l

Ratification of Council of Europe Convention on Cybercrime (Reactive Only)

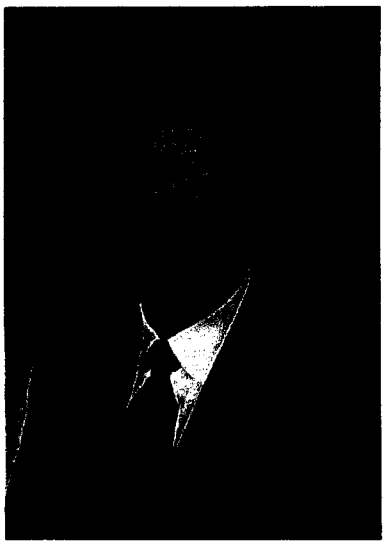
DAG Cole may be interested in knowing about Canadian plans to ratify the Council of Europe Convention on Cybercrime (Budapest Convention) following the February 2013 announcement that the Government of Canada would not pursue Bill C-30, the Protecting Children from Internet Predators Act. Among other things, this bill contained several changes to domestic legislation to ratify this Convention.

Canada signed the Convention in 2001 but needs to make several changes to domestic legislation in order to ratify it.

If this is raised, you could note that Canada remains a strong supporter of the Budapest Convention, and its ratification.

Tab 2A-7

James Cole, Deputy Attorney General



James Cole was sworn in as the Deputy Attorney General on Monday, January 3, 2011. Mr. Cole first joined the Department in 1979 as part of Attorney General's Honors Program and served for 13 years - first as a trial attorney in the Criminal Division, and later as the Deputy Chief of the Division's Public Integrity Section, the office that handles investigation and prosecution of corruption cases against officials, and employees at all levels of government. At Public Integrity Mr. Cole tried a number of notable cases, including prosecution of a U.S. District Judge, a member of Congress, and a federal prosecutor.

He entered private practice in 1992 and was a partner at Bryan Cave LLP from 1995 to 2010, specializing in white collar defense. He served as a court-appointed independent monitor to a large insurance company to establish and oversee corporate compliance programs and ensure it adhered to laws and regulations. He also counseled businesses on securities, regulatory, and criminal law issues.

While in private practice in 1995, Mr. Cole was tapped to serve as Special Counsel to the U.S. House of Representatives Committee on Standards of Official Conduct. In that role, he led an investigation into allegations that former House Speaker Newt Gingrich had improperly used tax-exempt money for partisan purposes and misled the Committee in its inquiry. His investigation led to a bipartisan resolution that was approved by an overwhelming majority of the full House, and resulted in a formal reprimand of Speaker Gingrich and a requirement that he pay penalties.

Mr. Cole has been a member of the adjunct faculty at Georgetown University Law Center, teaching courses on public corruption law and legal ethics, and has lectured at Harvard University's Kennedy School of Government. He is a former chair of the American Bar Association (ABA) White Collar Crime Committee and served as the Chair Elect of the ABA Criminal Justice Section. He received his B.A. from the University of Colorado and his J.D. from the University of California-Hastings.

Tab 2C

MEETING WITH MICHAEL DANIEL SPECIAL ASSISTANT TO THE PRESIDENT AND CYBERSECURITY COORDINATOR

ISSUE

You will be meeting with Michael Daniel Special Assistant to the President and the Cybersecurity Coordinator (biography at **TAB 2-C-1**). The meeting will take place from 4:00pm to 4:30pm at the Old Executive Office Building 1700 Pennsylvania Ave. NW, Washington DC.

BACKGROUND

In this position, Mr. Daniel leads interagency development of national cyber security strategy and policy, and he oversees agency implementation of those policies. He is also responsible for the federal government's engagement and partnerships with the private sector, non-governmental organizations, other branches and levels of government, and other countries.

- The President signed an Executive Order in February 2013, to improve the cybersecurity of critical infrastructure. The Executive Order includes measures to facilitate the U.S. Government's provision of classified and unclassified cyber threat information to critical infrastructure owners and operators; identify cyber systems of critical national importance; and establish voluntary baseline cybersecurity standards with incentives to encourage their adoption.
    - Executive Orders cannot create new authorities or new legal obligations. President Obama has called on Congress to pass comprehensive cyber security legislation. The White House has indicated that measures such as tax incentives and mandatory cybersecurity standards are required to secure U.S. networks.

- Cyber intrusions have significantly contributed to the loss of intellectual property and trade secrets. The White House has released a *Strategy on Mitigating the Theft of U.S. Trade Secrets*, which focuses on increasing diplomatic pressure on countries to address corporate espionage, enhancing law enforcement, trade sanctions and further domestic legislation.

- A number of recent high profile media reports have increased the visibility of cyber security. Several media outlets, including the *New York Times*, have admitted that their networks had been breached by Chinese hackers. The private network security company Mandiant released a report on February 19, 2013, claiming that the Chinese People's Liberation Army was responsible for at least 141 cyber intrusions across a number of industries since 2006. China has criticized the report, calling it "amateurish" and saying that its conclusions are "baseless."

CURRENT STATUS

In October 2012, Canada and the U.S. announced the *Cybersecurity Action Plan between the Department of Homeland Security and Public Safety Canada.* Since the Plan was announced, Canada and the U.S. have enhanced operational collaboration on cyber incident handling. For example, in February 2013, officials from the Canadian Cyber Incident Response Centre spent a week at the Department of Homeland Security's National Cybersecurity and Communications Integration Centre to work alongside their U.S. counterparts. Public Safety Canada and the Department of Homeland Security have also jointly provided cybersecurity briefings to cross-border critical infrastructure sectors, such as the financial and energy sectors, and coordinated public awareness efforts.

Canadian and U.S. officials share information on policy responses to shared cybersecurity concerns, such as mitigating risks posed by untrusted telecommunications equipment and efforts to have the Internet managed by governments instead of the private sector. This work is undertaken both bilaterally and with all Five Eye allies through the Ottawa 5.

The next [redacted] At the meeting, Canada will be represented by:

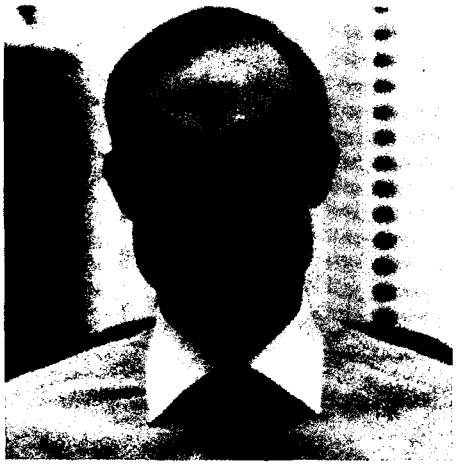
- Lynda Clairmont, Senior Assistant Deputy Minister, National Security (head of delegation);
- Bob Gordon, Special Advisor, Cybersecurity; and
- Michael Walma, Director of Policy and Planning and Cyber Coordinator at the Department of Foreign Affairs and International Trade.

[redacted]

s.15(1) - Int'l

Tab 2C-1

Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator



Michael Daniel is a Special Assistant to the President and the Cybersecurity Coordinator. In this position, Michael leads the interagency development of national cybersecurity strategy and policy, and he oversees agencies' implementation of those policies. Michael also ensures that the federal government is effectively partnering with the private sector, non-governmental organizations, other branches and levels of government, and other nations.

Prior to coming to the National Security Staff, Michael served for 17 years with the Office of Management and Budget (OMB). From September 2001 to June 2012, he served as the Chief of the Intelligence Branch, National Security Division, in a career Senior Executive Service position. This branch oversees the Intelligence Community (IC) and other classified Department of Defense programs. In this position, Michael played a key role in shaping intelligence budgets, improving the management of the IC, and resolving major IC policy issues. The branch also oversaw a variety of cross-cutting issues, including cybersecurity, counterterrorism spending, and information sharing and safeguarding.

Within OMB, Michael also served as an examiner in the National Security Division's Front Office supporting the Deputy Associate Director and in the Operations branch reviewing Navy and Marine Corps operational activities and overseas military operations such as Bosnia and Kosovo.

Since 2007, Michael has been heavily involved with Federal cybersecurity activities, starting with the Comprehensive National Cybersecurity Initiative. He has worked on cybersecurity funding issues in almost every budget since then and led an annual cross-cut review of Federal agencies' cybersecurity spending. He represented OMB on cybersecurity issues in the interagency policy process and worked with various Congressional committees and staff on cybersecurity issues. Finally, he has worked on tracking cybersecurity spending and the development of useful cyber performance metrics.

Originally from Atlanta, Michael received a Bachelor's in Public Policy from the Woodrow Wilson School at Princeton University. Subsequently, he obtained a Master's in Public Policy from the Kennedy School of Government at Harvard with a focus on International Affairs and Security. Michael also obtained a Master of Science in National Resource Strategy from the National Defense University's Industrial College of the Armed Forces in 2001.

Outside of work, Michael and his wife are raising two rambunctious boys. Michael also studies martial arts in the Chishin Ryu style with Dai Nippon Botoku Kai, a Norfolk-based karate association.

SCENARIO NOTE

HILL CALLS IN WASHINGTON, D.C.

General Overview

On March 14, 2013, in Washington, D.C., you will be conducting hill calls to meet with members of the United States Congress and Senate that sit on committees relevant to the Public Safety (PS) Portfolio. The meetings will be brief lasting from 15 – 30 minutes, allowing you to develop relations with key congressional and senate committee members. You will also be meeting with Lisa Monaco, recently appointed to the position of U.S. Deputy National Security Adviser for Homeland Security and Counterterrorism.

During these meetings, you will have an opportunity to discuss issues of mutual concern, including those relevant to the PS Portfolio, share ideas, and identify what you view as key threats to national security. You may also wish to explain some of the measures Canada is taking to counter these threats.

The meetings will also provide you with the opportunity to demonstrate that

Considerations

Suggested common speaking points for your meetings along with responsive speaking points can be found at (**TAB 3B**). These common and responsive speaking points will apply to each of your meetings. Overview details specific to Lisa Monaco and each of the members of Congress or Senate that you are meeting and their biographies can be found at (**TAB 3C**).

Potential Topics for Discussion

Relevant topics for discussion that you may wish to raise during your meetings include Beyond the Border, countering violent extremism, critical infrastructure, and cyber security. A brief description of each of these topics is included below and more detailed briefing notes on critical infrastructure and cyber security are included at (**TAB 3D**).

Topics for discussion that may be raised by the Congressmen during your meetings include the Detroit River International Crossing (DRIC), Keystone XL Pipeline, possible Canadian involvement in terrorism abroad, information sharing, and the Jeffrey Delisle espionage case. Responsive speaking points for each of these issues can be found after the common speaking points at (**TAB 3B**).

s.15(1) - s.21(1)(b)

Beyond the Border

[redacted] You may wish to explain the benefits of Beyond the Border and provide copies of the recent Beyond the Border implementation report to congressional members to demonstrate the progress that has been made.

[redacted]

Countering Violent Extremism

These meetings will provide an opportunity to reinforce Canada's commitment to countering violent extremism (CVE). You may wish to highlight how the *Beyond the Border Action Plan* has helped foster a productive ongoing Canada-U.S. relationship in efforts to counter violent extremism. Canada and the U.S. collaborate on a number of CVE issues, from strategic communications to the sharing of best practices and tools for law enforcement.

Critical Infrastructure

PS and DHS are very active in working together to enhance the resilience of cross border critical infrastructure and have made much progress under the Beyond the Border Action Plan. At the meeting you could highlight these successes and express PS's ongoing commitment to work with the United States [redacted]

Cyber Security

These meetings will provide an opportunity to highlight the extensive collaboration between Canada and the U.S. on cyber security issues, such as the *Cybersecurity Action Plan* between the

s.15(1) - s.21(1)(b)

Department of Homeland Security and PS, and increased operational collaboration on cyber incident handling. You could also emphasize Canada's ongoing commitment to investing in cyber security, given the considerable attention these issues have received in recent months.

COMMON SPEAKING POINTS

Beyond the Border

- A well-functioning Canada-U.S. border is integral to our shared security and the strength of both our economies.

- More than 200,000 people cross the border every day for business, pleasure, or to visit family. The U.S. is also Canada's most important export market, with trade supporting one in seven jobs in Canada.

- In turn, Canada is America's largest export market with $308.4 billion in U.S. exports to Canada in 2012 representing 19% of all U.S. exports for the year. This is larger than Mexico (14%), China (7%), Japan (5%), or the entire European Union (17%).

- At the same time, we also share a number of common threats to the security of our countries. The threat environment is constantly evolving, from cyber to terrorism, constantly challenging our ability to respond quickly and effectively.

- By moving forward with the Beyond the Border (BTB) Action Plan, the United States and Canada recognized their shared responsibility for the safety, security and resilience of both countries in an integrated and globalized world.

- We also recognized our long-standing trade relationship and committed to reduce impediments to the movement of people and goods between Canada and the U.S.

- For our integrated economies, BTB initiatives such as harmonizing and increasing trusted trader and traveler programs and low value shipment thresholds will facilitate and streamline the movement of goods and people across the border, and generate competitive advantages for North American businesses competing against overseas imports.

- For our shared border security, we will enhance the overall security of North America through joint threat and risk assessments and the continued growth of cooperative cross-border law enforcement programs, coupled with an entry-exit system and advanced passenger and cargo clearance programs.

[redacted]

s.15(1) -
s.21(1)(b)

Counter Terrorism

- Canada's Counter-Terrorism Strategy was launched in early 2012, with the four pillars of: prevent, detect, deny and respond to terrorism.

- The Strategy clearly details how our local, national and international efforts to address threats work together to protect Canadians and Canadian interests.

- The Strategy builds on our ongoing work with the U.S. through the Beyond the Border Action Plan on issues such as conducting joint threat assessments, countering violent extremism and enhancing information sharing.

Critical Infrastructure

- Public Safety Canada and the Department of Homeland Security have a longstanding partnership in the area of critical infrastructure resilience, including joint risk management activities and exercises.

- In particular, the success of the cross border Regional Resilience Assessment Program (RRAP) piloted in Maine – New Brunswick is a good example of the strong collaboration between our Departments and a key achievement under the Perimeter Security and Economic Competitiveness Action Plan.

- The RRAP brings together all levels of government with critical infrastructure owners and operators to assess resilience at a regional level. It features site assessments of vital assets and systems (e.g. nuclear power plants, bridges, border crossings) and focuses on identifying vulnerabilities, threats and the potential consequences of disruptions.

- I look forward to our continued collaboration, especially by building on the success of the pilot RRAP and expanding this initiative to other cross border regions.

Cyber Security

- We value the close relationship we have with the U.S. on cyber security issues. Cyber issues cross borders and coordinated action is required to address them.

- Since the release of Canada's Cyber Security Strategy in 2010, Canada has:
  - consolidated government IT systems to improve their security;
  - dedicated more resources to the Canadian Cyber Incident Response Centre;
  - taken an increasingly assertive role internationally, including at the United Nations; and
  - launched the GetCyberSafe.ca awareness campaign.

- We work very closely with our U.S. counterparts to jointly address cyber security issues. Through the *Cybersecurity Action Plan between the Department of Homeland Security and Public Safety Canada,* Canadian and U.S. officials have:
  - enhanced operational collaboration on cyber incident handling;
  - jointly provided cyber security briefings to cross-border private sector entities; and
  - coordinated public awareness efforts.

- We are particularly interested in the Executive Order and how it has been received in the business community.

RESPONSIVE SPEAKING POINTS

Detroit River International Crossing

- I understand that Transport Canada and the Canadian Embassy have asked to have substantive discussions with U.S. officials on options to fund the U.S. port of entry for the DRIC. However, these discussions have not yet occurred. In order to move forward with the project, it is critical that we resolve the uncertainty regarding the U.S. port of entry for this vitally important project.

- We are hopeful that a Presidential permit will soon be issued for the Detroit River International Crossing project.

Keystone XL Pipeline

- I understand the U.S. Department of State (DoS) recently released a Draft Supplemental Environmental Impact Statement (SEIS) on the Keystone XL pipeline project that concluded the pipeline will have little to no impact on U.S. greenhouse gas emissions.

- Our Government is looking forward to hearing a final decision on this approval process.

s.15(1) - Int'l

Possible Canadian Involvement in Terrorism Abroad

On suggestions that Canadian citizens were involved in terrorism abroad:

- I am aware of the recent media reports about alleged Canadian involvement in terrorist incidents in Algeria and Bulgaria.

- The Royal Canadian Mounted Police has deployed officers to Algeria and Bulgaria to investigate these allegations.

- We have a number of robust tools in place to address terrorism, both at home and abroad. This includes Canada's Counter-terrorism Strategy,

- Canada is also working closely with the U.S., under the Beyond the Border initiative, to enhance security at our perimeter, counter violent extremism and improve intelligence sharing on threats.

Information Sharing

- I think we can be very pleased with the progress made under the national security information sharing item of the Beyond the Border Action Plan.

-

-

Jeffrey Delisle Espionage Case

- National and allied intelligence is a fundamental national security tool and Canada remains committed to its protection.

- Mr. Delisle's unauthorized disclosure of secret information was intolerable, inexcusable and inconsistent with the integrity and loyalty that Canadians expect from their men and women in uniform.

- He not only violated Canada's trust, but also broke our laws, and has accordingly been sentenced to 20 years in prison as well as the requirement to pay restitution to the Canadian government. He has been released from the Canadian Armed Forces and his commission has been revoked.

- Our government has every confidence that this incident is not reflective of the characteristically impeccable performance and dedication of the men and women of the Canadian Armed Forces, and their commitment to safeguarding national interests.

Meeting with Congressman Patrick Meehan (Rep – Pennsylvania) from 1:45 p.m – 2:00 p.m.

Overview

Congressman Patrick Meehan represents Pennsylvania's 7th Congressional District and is currently serving his second term in Congress. He is a member of the Homeland Security Committee, on which he is the **Chairman of the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies**. Congressman Meehan also sits on the Oversight and Government Reform Committee, the Transportation and Infrastructure Committee and the House Ethics Committee. As a member of the Homeland Security Committee, Meehan has taken an active role in crafting a variety of national security policies, particularly regarding counter terrorism.

Cyber Security

The Congressman views **cyber security** as an urgent national security priority. In January 2013, he wrote a newspaper column on the growing threat of cyber-attacks in the United States. The column warns of threats to U.S. critical infrastructure citing recent cyber-attacks on U.S. banks by hacking groups that appear to be linked to the Iranian government. It also promises that the subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, which Meehan chairs, will be crafting a national strategy aimed at preventing attacks on American families and their bank accounts, health records, identities, and more.

Border Security

In July 2012, Congressman Meehan chaired a Subcommittee on Counterterrorism and Intelligence hearing held in Buffalo, NY on the implementation of the Beyond the Border Action Plan. Meehan stated in advance of the meeting that "*America's economy and national security depend on secure borders, free flow of goods and efficient travel for U.S. citizens. According to a 2011 Government Accountability Office report, only 32 of the 4,000 mile northern border with Canada are considered to have "an acceptable level of security." He added that he was looking forward to* hearing statements from federal and local officials on whether information sharing between U.S. and Canadian law enforcement and intelligence agencies is effectively addressing gaps in border security, facilitating commerce and travel, and protecting the United States from threats.

Sequestration

Leading up to the March 1, 2013 cut-off date for avoiding sequestration, Congressman Meehan's office indicated he desired to "avoid the sequester's arbitrary cuts," adding that the United States needs to address its spending problem "but the sequester's across-the-board cuts are not an ideal way to do it." Meehan stated that he favored replacing the arbitrary cuts with targeted spending reforms, but that it was up to the Senate to work out a deal because the House has already passed a plan to replace the sequester.

Keystone XL Pipeline

Meehan believes that the U.S. should support greater access to affordable sources of energy and was 1 of 110 members of Congress that signed a letter in May 2012 urging the immediate approval of the Keystone XL pipeline.

Terrorism

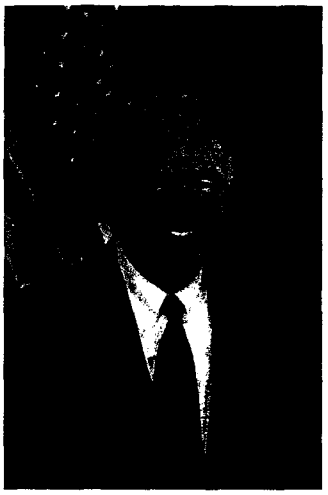
Congressman Meehan authored the *Weapons of Mass Destruction Intelligence and Information Sharing Act,* adopted by the House in May 2012. The bill would provide guidance for the Department of Homeland Security to engage in and support intelligence activities related to **chemical, biological, radiological, and nuclear (CBRN) threats** and to share timely intelligence and prevention tools with partners at the federal, state, and local levels. The bill is currently awaiting action in the Senate.

In spring 2012, Meehan traveled with a congressional delegation to the Middle East to assess the threat posed by Iran to the United States, the region, and global security. He has also been examining the emerging threat of the **Nigerian-based Islamist terror group Boko Haram.** Congressman Meehan's bill, the *Boko Haram Terrorist Designation Act* was accepted by the House as an amendment to the fiscal year 2013 *National Defense Authorization Act.* The bill tasks the Department of State to examine whether Boko Haram meets the criteria for designation as a terrorist group. It is awaiting action in the Senate.

Gun Trafficking

Meehan recently co-introduced the bipartisan *Gun Trafficking Prevention Act* of 2013. The Bill would make gun trafficking a federal crime for the first time and impose stronger penalties on so-called "straw purchasers" who acquire guns for convicted felons and other dangerous persons prohibited from owning firearms. The bill is currently being considered at the Committee level.

Congressman Patrick Meehan (Rep – Pennsylvania)



Congressman Patrick Meehan represents Pennsylvania's 7th Congressional District in the United States Congress. Currently in his second term in Congress, Meehan serves on the Oversight and Government Reform, Homeland Security, Transportation and Infrastructure, and House Ethics Committees. As a member of the Homeland Security Committee, Congressman Meehan was appointed Chairman of the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies.

Prior to his election to Congress, Meehan earned an impressive record as a prosecutor in Philadelphia. Meehan went on to be appointed by the President as the United States Attorney for the Eastern District of Pennsylvania, a position that made him the top federal prosecutor.

Meehan was sworn in just six days after the September 11, 2001 attacks. He immediately went to work combating the threat of terrorism. He set up an Anti-Terrorism Advisory Council (ATAC) to coordinate the region's response to the attacks. The ATAC became a national model for coordination among law enforcement agencies and ensured that critical information and intelligence on terrorist threats was disseminated to the appropriate federal, state and local law enforcement personnel.

During his tenure, the U.S. Attorney's Office in Philadelphia became a national leader in prosecuting corrupt government officials. Meehan helped to put behind bars some of the biggest names in Philadelphia's corrupt pay-to-play political culture, including former Philadelphia Treasurer Corey Kemp, Councilman Rick Mariano, and State Senator Vincent Fumo. Meehan earned praise from both sides of the aisle for his integrity and his commitment to rooting out political corruption.

Prior to his appointment as United States Attorney, Meehan served as the District Attorney of Delaware County. During this time, he successfully prosecuted several high-profile cases, including the murder trial of millionaire John DuPont. He also formed the Internet Crimes Against Children Task Force, a working group dedicated to protecting children from online predators.

A native of Cheltenham, Montgomery County, Meehan is a graduate of Bowdoin College and the Temple University School of Law. Prior to entering public service, Congressman Meehan spent two years as a referee in the National Hockey League. Meehan, his wife Carolyn, and their three sons live in Drexel Hill, Delaware County.

Meeting with Congresswoman Yvette Clarke (Dem – New York) from 4:30 p.m. – 5:00 p.m.

Overview

Congresswoman Yvette D. Clarke was first elected to Congress in November 2006 and represents the 9th Congressional District of New York. She is a member of the Homeland Security Committee, on which she is a **Ranking Member for the Subcommittee on Cybersecurity, Infrastructure Protection & Security Technologie**s and a member of the Subcommittee on Emergency Preparedness, Response & Communications.

Cyber Security

The Congresswoman is regularly briefed on cyber-attacks against the United States. Clarke contends that cyber-attacks are undermining computer systems in almost every sector of the U.S. economy and government. She has worked to develop public-private partnerships and to create a comprehensive strategy for protecting the United States against cyber-terrorism.

U.S. Sequestration

On U.S. sequestration, Clark has singled out cuts to airport security as one of her primary concerns. She believes cuts resulting from sequestration will present a serious risk to both airport staff and national security.

Keystone XL Pipeline

Clarke has not been a vocal opponent of the Keystone XL pipeline but did vote against a motion in the House to approve the Pipeline in April 2012.

Homeland Security (Emergency Management)

Having witnessed the horrors of 9/11 first-hand, Clarke has been a staunch advocate for homeland security policy. One of her first actions upon arriving in Congress in 2006 was to support the passage of a bill to implement the recommendations of the 9/11 Commission.

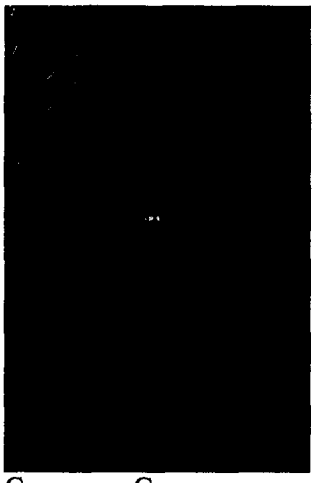
Emergency Management

In the area of emergency management, Clarke has worked with the Department of Health and Human Services to identify and fight new flu strains. She is also a strong advocate for municipal and state emergency responders, pushing for funding for "*state-of-the-art and reliable communications and safety equipment that is vital in responding to a domestic attack or natural disaster.*" During Clarke's first tenure in the House, she worked to secure New York City's bridges, tunnels, buses and trains under a program titled the *Securing the Cities Initiative*. The initiative culminated in a five-day, full-scale exercise that included thousands of first responders and law enforcement officers from 150 agencies in New York, New Jersey and Connecticut.

Caribbean Issues

A woman of Jamaican decent, Clarke is a strong supporter of capacity building in the Caribbean region. She has worked with the Caribbean Community (CARICOM), the Organization of American States (OAS) and the CARICOM Diplomatic Corps on a variety of capacity building programs in the areas of trade, security, economic development, and disaster preparedness.

Congresswoman Yvette Clarke (Dem – New York)



United States Congresswoman Yvette D. Clarke is a Brooklyn native whose roots are firmly planted in her Jamaican heritage. Clarke was first elected to Congress in November 2006 and represents the new Ninth Congressional District of New York. Prior to being elected to the U.S. House of Representatives, Clarke served on the New York City Council representing the 40th District in Brooklyn. She succeeded her pioneering mother, former City Council Member Una S. T. Clarke, the first African American woman and Caribbean American elected to Congress, making them the first mother-daughter succession in the history of the Council.

Currently in the 113th Congress, Clarke sits on the Committees of Homeland Security and Small Business. In the 111th and 112th Congress, Congresswoman Clarke served on several Committees including Education and Labor, Homeland Security and Small Business.

An unwavering champion for her native Brooklyn, she has worked with non-profit organizations, local community groups and appropriators to secure millions of dollars in essential federal support for the district. As a result, major institutions received funds, including the Brooklyn Academy of Music, the Brooklyn Botanic Garden, the Brooklyn Public Library, the Brooklyn Children's Museum, the Prospect Park Alliance and the New York State Department of Transportation (DOT).

A product of the New York City Public School System, Clarke graduated from Oberlin College and was a recipient of the prestigious APPAH/Sloan Fellowship in Public Policy and Policy Analysis. She currently resides in the neighborhood where she grew up, in the Flatbush section of Brooklyn.

Lisa Monaco, Deputy National Security Advisor for Homeland Security and Counterterrorism

In January, 2013, Lisa Monaco was selected to replace John Brennan as Deputy National Security Advisor for Homeland Security and Counterterrorism. Prior to replacing John Brennan, who himself was promoted to the Director of the Central Intelligence Agency, Monaco served as Assistant Attorney General for National Security beginning on July 1, 2011. Her previous assignment was as the Principal Associate Deputy Attorney General, where she was the Deputy Attorney General's primary advisor Prior to joining the Deputy Attorney General's office, Monaco was the chief of staff to FBI Director Robert S. Mueller. Monaco also served as special counsel to Director Mueller. Monaco initially joined the FBI on detail from the U.S. Attorney's Office for the District of Columbia.

From 2001 to 2007, Monaco served as a federal prosecutor. She was appointed to the Enron Task Force, serving as a co-lead trial counsel in the prosecution of five former executives of Enron Broadband Services. For her work on the Enron Task Force, Monaco received the Attorney General's Award for Exceptional Service, the Justice Department's highest award.

Monaco served as counsel to Attorney General Janet Reno from 1998 to 2001,

Before joining the department, Monaco clerked for the Honorable Jane R. Roth, U.S. Court of Appeals for the Third Circuit. She earned her J.D. from the University of Chicago Law School and her B.A. from Harvard University.

s.19(1)

RDIMS: 789853

Return to Table of Contents

Cyber Security

Background

Cyber security issues have received considerable attention in recent months in the United States (U.S.).

- The President signed an Executive Order in February 2013, to improve the cyber security of critical infrastructure. The Order includes measures to facilitate the U.S. Government's provision of classified and unclassified cyber threat information to critical infrastructure owners and operators; identify cyber systems of critical national importance; and establish voluntary baseline cyber security standards with incentives to encourage their adoption.
    - Despite this Executive Order, the President has called on Congress to pass comprehensive cyber security legislation, as Executive Orders cannot create new authorities or new legal obligations. The White House has indicated that further measures, such as tax incentives and mandatory compliance with cyber security standards, are required to secure U.S. networks.
- The White House has released a *Strategy on Mitigating the Theft of U.S. Trade Secrets*. As cyber intrusions have contributed to the loss of intellectual property and trade secrets, the Strategy aims to reinforce measures to mitigate and deter the theft of U.S. companies' trade secrets. This will be done by increasing diplomatic engagement, promoting voluntary best practices, enhancing domestic law enforcement action, improving domestic legislation, and raising awareness.
- Congress has struggled to pass comprehensive cyber security legislation due to an ideological divide among lawmakers: Republicans favour voluntary incentives and Democrats favour using regulatory authorities to set mandatory standards for the private sector. There is likely to be a renewed push this year in light of the President's calls for further action. The principal lawmakers engaged on cyber security are:
    - Representative Mike Rogers (Republican-Michigan);
    - Representative Dutch Ruppersberger (Democrat-Maryland);
    - Senator John D Rockefeller IV (Democrat-West Virginia); and
    - Senator Susan Collins (Republican-Maine).
- A number of recent high profile media reports have increased the visibility of cyber security. The *New York Times* recently admitted that its networks had been breached by Chinese hackers after having published an unflattering article on Chinese Premier Wen Jiabao. A few weeks later, the private network security company Mandiant released a report claiming that the Chinese People's Liberation Army (PLA) was responsible for at least 141 cyber intrusions across a number of industries since 2006.

The report was specific, revealing the tactics, techniques and procedures used by the PLA. China has criticized the report, calling it "amateurish" and saying that its conclusions were "baseless."

Current Status

Canada's Cyber Security Strategy is in its third year of implementation and aligns well with U.S. efforts in this area. Canada's cyber security achievements include:

- consolidating government IT systems to improve their security;
- clarifying the roles and responsibilities of federal departments and agencies;
- dedicating more resources to the Canadian Cyber Incident Response Centre;
- creating a Canadian Security Telecommunications Advisory Council to engage the telecommunications sector;
- launching the GetCyberSafe.ca awareness campaign; and
- passing anti-spam legislation.

In October 2012, Canada and the U.S. announced the *Cybersecurity Action Plan between the Department of Homeland Security and Public Safety Canada*. Since the Plan was announced, Canada and the U.S. have enhanced operational collaboration on cyber incident handling, jointly provided cyber security briefings to cross-border private sector entities, and coordinated public awareness efforts.

Canadian and U.S. officials also share information on policy responses to shared cyber security concerns, such as mitigating risks posed by untrusted telecommunications equipment and efforts to have the Internet managed by governments instead of the private sector. This work is undertaken bilaterally and with the remaining Five Eye allies (the United Kingdom, Australia, and New Zealand).

Considerations

[redacted]

Desired outcomes

- Highlight the extensive collaboration between Canada and the U.S. on cyber security issues, particularly the *Cybersecurity Action Plan between the Department of Homeland Security and Public Safety Canada.*
- [redacted]

BRIEFING NOTE FOR THE MINISTER

MEETING WITH PRINCE MOHAMMAD BIN NAYEF, MINISTER OF THE INTERIOR, SAUDI ARABIA

Issue

You will have a bilateral meeting with Prince Mohammad on Friday January 18, 2013, from 2:30 to 3:30 p.m., at your Hill Office. Prince Mohammad will be accompanied by Dr. Saad Al Jabri, Senior Security Advisor to the Minister of the Interior, and [redacted] Directorate. You will be supported at the meeting by your Chief of Staff, Andrew House, and Mike Theilmann, Acting Director International Affairs. Suggested key messages follow this note.

Public Safety Cooperation

Saudi Arabia is a tier one priority interest for Public Safety Canada. [redacted]

The **RCMP** manages a very positive bilateral operational relationship with its Saudi counterpart agencies through its liaison officer posted in Dubai, United Arab Emirates.

In October 2012, the RCMP provided the Saudi Ministry of the Interior with the Major Case Management software, "E&R III". Developed by the RCMP, the software facilitates the tracking, vetting and linking of information associated with complex and high-volume investigations. A number of Saudi law enforcement officers will attend training in the software at the Canadian Police College in February 2013.

The Saudi Ministry of the Interior has more than 500,000 employees and comprises a number of agencies and organizations, including those responsible for domestic security, counter-terrorism, police, corrections, special operations forces, and borders. The General Investigation Directorate is also part of the Ministry of the Interior, while the General Intelligence Presidency reports directly to the King.

s.15(1) - Int'l

Countering Violent Extremism

[redacted] a working group (the Contact Group) on counter-radicalization, which includes Saudi Arabia. The working group meets regularly to discuss issues related to countering violent extremism and radicalization.

Saudi officials believe the most effective way to avoid recidivism in prison in convicted terrorists is to fully reintegrate extremists into society. The Saudi government's de-radicalization program, which includes rehabilitation and post-release care, has received significant international attention. Since its inception, thousands of detainees have gone through the program. Key elements of the program include:

- Religious re-education, psychological counseling and vocational training;
- Government assistance to regain former employment or find new employment; and,
- Financial aid to cover post-release costs for housing, medical and dental care.

Consistent with Saudi beliefs and traditions, which emphasize family honour, the Saudi government works closely with families of detainees in the rehabilitation process. For example, detainees are released into custody of at least three family members, who sign pledges of responsibility for the detainee. Government officials also encourage unmarried detainees to marry, and will work with family members to identify suitable spouses (e.g. those who are not considered radical).

Canada's approach to countering violent extremism is situated within the *Prevent* pillar of Canada's Counter-Terrorism Strategy, launched in February 2012. The approach focuses on social cohesion and on building individual and community resilience to the threat of domestic terrorism.

Canada's approach is multi-faceted, holistic and involves a number of government departments and agencies. Activities include coordinated domestic intelligence aned law enforcement, and community outreach (including through the Cross-Cultural Roundtable on Security), as well as close relationships with bilateral (e.g. the U.S., U.K. and Saudi Arabia) and multilateral partners (e.g. the Global Counter-Terrorism Forum). Public Safety Canada is also active in countering violent extremism through its funding of the Kaniska Project.

Ministry of the Interior Modernization Program

[redacted]

s.13(1)(a)
s.15(1) - Int'l
s.19(1)

[redacted]

Regional Security

Mali. Following the March 22, 2012 coup d'état and the takeover of the northern two thirds of the country by rebels and terrorists, international efforts have focused on facilitating the restoration of democratic rule, supporting the re-establishment of government control in the north, and addressing the humanitarian crisis in the country.

On October 12, 2012, the UNSC adopted Resolution 2071 regarding the situation in northern Mali. The resolution paves the way for the creation by the UNSC of a UN stabilization mission in support of a regional African-led mission to Mali, which would authorize military deployment.

France, which has 6,000 citizens in Mali, was the first country to provide support to Malian forces. It launched a series of air strikes against rebel positions on January 11, 2013, and deployed 2,500 troops. On January 14, 2013, Prime Minister Harper announced that Canada will not have a direct Canadian military mission in Mali and will instead provide limited and clearly defined logistical support (deployment of a CC-177 aircraft) to assist the French government in transporting equipment and personnel to Mali. In addition to this logistical support, Prime Minister Harper added that Canada would continue to provide humanitarian aid and development assistance to the region to help alleviate the worsening humanitarian conditions in the region.

[redacted]

Syria. The situation in Syria is worsening and the most imminent threat is a humanitarian crisis prompted by an exodus of refugees, many of them Palestinians. It is believed that certain neighbouring countries would not welcome these refugees (e.g. Jordan). While Russia is still unwilling to support a UN Security Council on Syria,

[redacted]

[redacted]

Yemen. The instability in Yemen has been a concern of the international community for some time. Political turmoil connected to the "Arab Spring" has compounded these issues, and has led to further instability. Al Qaida in the Arabian Peninsula remains the country's most aggressive threat to international security. [redacted]

Iran. AQ-inspired Sunni extremists and individual or small group acts of terror [redacted] are the most formidable internal threat to the Iranian regime, while Israel remains its strongest external threat. Iran continues its role as a patron to terrorist groups such as Hizballah, Hamas, the Palestinian Islamic Jihad, and the Popular Front for the Liberation of Palestine – General Command. The August 15, 2012 cyber attack against Saudi Arabia's state oil company Aramco, which compromised more than 30,000 computers, [redacted]

Cyber Security Issues

Cyber Attack Against Aramco. On August 15, 2012, [redacted] the Saudi state-owned oil company's computers, unleashed a computer virus to initiate what is regarded as one of the most destructive acts of computer sabotage on a company to date. The virus erased data on three-quarters of Aramco's corporate computers – documents, spreadsheets, emails, files – replacing them with an image of a burning American flag. Media reports speculated that Iran was behind the attack, [redacted]

Internet Governance. The current day-to-day operations of the Internet are managed by a group of non-profit organizations, academics and engineers based primarily in the U.S. While Canada and its allies strongly support this multi-stakeholder approach, [redacted] want greater state control over the Internet and the information transmitted over it.

s.13(1)(a)
s.15(1) -
s.21(1)(b)

BRIEFING NOTE FOR THE MINISTER

MEETING WITH BARONESS PAULINE NEVILLE-JONES, SPECIAL REPRESENTATIVE TO BUSINESS ON CYBER SECURITY, UK CABINET OFFICE

Issue

You will be meeting with Baroness Pauline Neville-Jones, Special Representative to Business on Cyber Security, United Kingdom (UK) Cabinet Office.

There will not be a gift exchange.

Strategic Objectives

The recommended strategic objectives of your meeting are to:

- Obtain a better understanding of how the UK provides intelligence to private sector organizations, particularly in light of the UK's update to its *National Cyber Security Strategy*; and
- Convey the message that Canada and the UK face the same cyber threats [redacted]

Public-Private Information Sharing

United Kingdom: the British government's engagement with the private sector is primarily driven by its intelligence agencies. The Centre for the Protection for National Infrastructure (CPNI) is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage.

Building on the work of the CPNI, in early September the UK formally launched their *Cyber Security Guidance for Business* program, which has released three tailored information products to help the CEOs of the 100 largest British companies address the cyber vulnerabilities of their organizations. Also in September, the UK government announced £3.8M in funding to create a Research Institute in the Science of Cyber Security based at University College London. This Institute is intended to bring together government, the UK signals intelligence agency and seven universities to develop new cyber security solutions, principally focused around cybercrime.

Canada: [redacted] As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to modernize Canada's frameworks for information sharing accordingly. It may be useful to learn more about the UK's new national

security hub for public-private information sharing, [redacted]

Global Cyber Security Threats and Trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. Intelligence services and militaries are also increasingly supporting, both directly and indirectly, espionage activities which are intended to secure an economic advantage whether through stealing of trade secrets or research, or by interfering in negotiations.

Recognizing the magnitude of the challenge, countries have started to pay more attention to cyber security issues and are taking steps to protect themselves. Since 2009, approximately 15 countries, including Australia, Canada, Germany, France, the Netherlands, South Korea, Russia, the UK, and the United States have each released a cyber security strategy.

United Kingdom: The UK updated its *National Cyber Security Strategy* in November 2011. The update included the following measures:

- A new national cyber security hub that will allow government and the private sector to exchange information on threats and responses;
- The establishment of a new Cyber Crime Unit within the National Crime Agency which is meant to be up and running by 2013;
- A new Joint Cyber Unit for the UK military;
- Have the Centre for the CPNI take a more inclusive approach to defining critical infrastructure;
- Improve the GetSafeOnLine website (the UK equivalent of Canada's GetCyberSafe.ca public awareness campaign) and work with Internet service providers to develop a voluntary code of conduct to help people to determine if their computers have been compromised and what to do about it; and
- Continued emphasis on international dialogue, geared towards maintaining the momentum generated by the London Conference on Cyberspace held in November 2011 and the Budapest Conference held in October 2012.

Canada: Public Safety Canada's efforts under *Canada's Cyber Security Strategy* align well with many of the initiatives highlighted in the UK's strategy.

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the Royal Canadian Mountain Police's Integrated Cyber Crime Fusion Centre.
- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks.

s.21(1)(a)

- Canada's GetCyberSafe.ca website was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.

MEETING WITH BARONESS PAULINE NEVILLE-JONES, SPECIAL REPRESENTATIVE TO BUSINESS ON CYBER SECURITY, UK CABINET OFFICE

KEY MESSAGES

Public-private information sharing

You may wish to:

- Inquire about the objectives of the "hub" for government and private sector information sharing referenced in the update to the UK's cyber security strategy and how this "hub" would work.

- Ask about the challenges faced by the UK in their efforts to share information to enhance the security of networks and systems.

Global cyber security threats and trends

- Note that Canada and the United Kingdom have a strong history of working together to address cyber threats and improve our collective security.

- Highlight that the UK's recently updated national cyber security strategy is very compatible with Canada's, particularly its focus on addressing the economic dimension of cyber security.

BRIEFING NOTE FOR THE MINISTER

CYBER SECURITY

Global Cyber Security Threats and Trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. Intelligence services and militaries are also increasingly supporting, both directly and indirectly, espionage activities which are intended to secure an economic advantage whether through stealing of trade secrets or research, or by interfering in negotiations.

Recognising the magnitude of the challenge, countries have started to pay more attention to cyber security issues and are taking steps to protect themselves. Since 2009, approximately 15 countries, including Australia, Canada, Germany, France, the Netherlands, South Korea, Russia, the UK, and the United States have each released a cyber security strategy.

United Kingdom: The UK updated its *National Cyber Security Strategy* in November 2011. The update included the following measures:

- A new national cyber security hub that will allow government and the private sector to exchange information on threats and responses;
- The establishment of a new Cyber Crime Unit within the National Crime Agency which is meant to be up and running by 2013;
- A new Joint Cyber Unit for the UK military;
- Have the Centre for the Protection for National Infrastructure (CPNI) take a more inclusive approach to defining critical infrastructure;
- Improve the GetSafeOnLine website (the UK equivalent of Canada's GetCyberSafe.ca public awareness campaign) and work with Internet service providers to develop a voluntary code of conduct to help people to determine if their computers have been compromised and what to do about it; and
- Continued emphasis on international dialogue, geared towards maintaining the momentum generated by the London Conference on Cyberspace held in November 2011.

Canada: Public Safety Canada's efforts under *Canada's Cyber Security Strategy* align well with many of the initiatives highlighted in the UK's strategy.

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the Royal Canadian Mountain Police's Integrated Cyber Crime Fusion Centre.

- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks.
- Canada's GetCyberSafe.ca website was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.

Public-Private Information Sharing

United Kingdom: the British government's engagement with the private sector is primarily driven by its intelligence agencies. The CPNI is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage.

Building on the work of the CPNI, in early September the UK formally launched their *Cyber Security Guidance for Business* program, which has released three tailored information products to help the CEOs of the 100 largest British companies address the cyber vulnerabilities of their organizations. Also in September, the UK government announced £3.8M in funding to create a Research Institute in the Science of Cyber Security based at University College London. This Institute is intended to bring together government, the UK signals intelligence agency and seven universities to develop new cyber security solutions, principally focused around cybercrime.

Canada: As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to modernize Canada's frameworks for information sharing accordingly. It may be useful to learn more about the UK's new national security hub for public-private information sharing,

Canada-UK Cooperation

United Kingdom: The UK with the support of like-minded countries, launched the London Conference on Cyberspace on November 1–2, 2011. This process is intended to specifically highlight the linkages between the various aspects of cybersecurity, namely that:

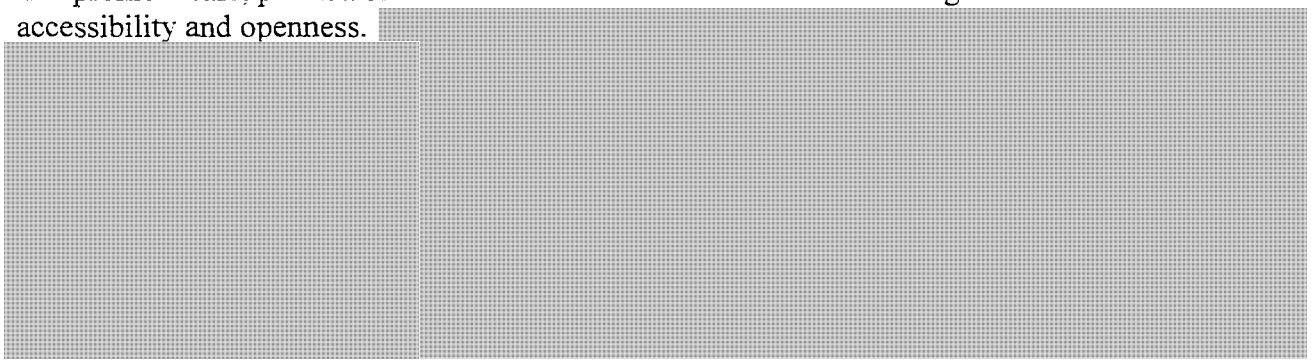
s.15(1) - Int(1)(a)

- the current governance of the Internet, with a multi-stakeholder model that includes the private sector, has enabled incredible innovations and economic growth;
- going forward, the international community should focus on non-binding norms, which would set out the broad "rules of the road" for cyberspace; and
- existing international law, such as human rights law and the law of armed conflict, apply equally in cyberspace.

Underpinning this normative approach to cyberspace is the idea that no major structural changes to Internet governance or the international system are required to address new cyber issues.

The London Conference on Cyberspace was the first time that these issues were considered in a comprehensive way. It was hosted by the UK Foreign Minister William Hague, featured high-level participation (including from U.S. Vice President Joseph Biden), and brought together representatives from over 60 countries, the private sector and civil society. Hungary is hosting the next Conference in Budapest in October 2012, and it will likely feature similar prominent political engagement.

Canada: Canada has actively supported the UK in its efforts to sponsor norms for cyberspace that promote safe, predictable and consistent interactions while ensuring the Internet's accessibility and openness.



s.15(1) - s.21(1)(b)

CYBER SECURITY

KEY MESSAGES

Global cyber security threats and trends

- Note that Canada and the United Kingdom have a strong history of working together to address cyber threats and improve our collective security.

- Highlight that the UK's recently updated national cyber security strategy is very compatible with Canada's, particularly its focus on addressing the economic dimension of cyber security.

Public-private information sharing

You may wish to:

- Inquire about the objectives of the "hub" for government and private sector information sharing referenced in the update to the UK's cyber security strategy and how this "hub" would work.

- Ask about the challenges faced by the UK in their efforts to share information to enhance the security of networks and systems.

Canada-UK cooperation

- Note that the Canadian Cyber Incident Response Centre (CCIRC) and its UK counterpart, the Protection for National Infrastructure (CPNI), have an excellent working relationship and routinely share information on malicious websites and computer viruses.

- Express your understanding that Canada strongly supports the UK at the policy level in promoting common interests and policy positions on cyber security.

BRIEFING NOTE FOR THE MINISTER

CYBER SECURITY ISSUES

Background

Global Cyber Security Threats and Trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. The ease of use of modern hacking tools makes it simple for activists to temporarily disrupt websites or cause other damage to networks. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. The hackers then craft emails or other messages that have been fabricated to trick the victim into downloading viruses or divulging details that would allow access to valuable information, such as intellectual property or credit card information. Foreign intelligence services and militaries are also capitalizing on states' dependence on networked infrastructure to conduct espionage activities or to support military operations.

Recognizing the magnitude of the challenge, countries have started to pay more attention to cyber security issues and are taking steps to protect themselves. Since 2009, approximately 15 countries, including Australia, Canada, Germany, France, the Netherlands, the Republic of Korea, Russia, the UK, and the US have each released a cyber security strategy.

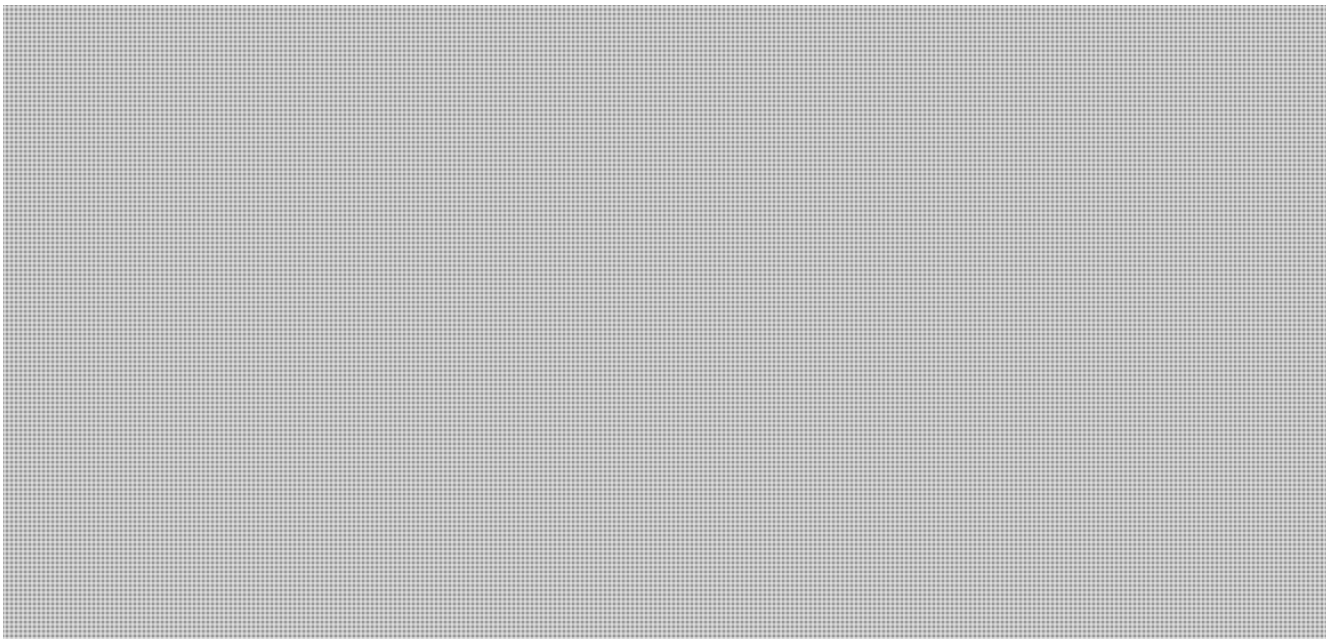
United Kingdom: The UK updated its *National Cyber Security Strategy* in November 2011. The update included the following measures:

- A new national cyber security hub that will allow government and the private sector to exchange information on threats and responses;
- The establishment of a new Cyber Crime Unit within the National Crime Agency which is meant to be up and running by 2013;
- A new Joint Cyber Unit which will develop military capabilities to give the UK comparative advantage in cyber space;
- An expanded role for the Centre for the Protection for National Infrastructure (CPNI) so that it will conduct outreach to sectors beyond what has been traditionally considered part of the national critical infrastructure;
- Improve the GetSafeOnLine website (the UK equivalent of Canada's GetCyberSafe.ca public awareness campaign) and work with Internet service providers to develop a voluntary code of conduct to help people to determine if their computers have been compromised and what to do about it; and,
- Continued emphasis on international dialogue, principally maintaining momentum generated by the London Conference on Cyberspace held in November 2011.

Canada: Public Safety Canada's efforts under *Canada's Cyber Security Strategy*'s align well with many of the initiatives highlighted in the UK's strategy:

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the RCMP's Integrated Cyber Crime Fusion Centre which was established per *Canada's Cyber Security Strategy*.
- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks; and,
- Canada's GetCyberSafe.ca website (equivalent to the UK's GetSafeOnline.org website) was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October in a manner similar to the UK's public outreach campaigns.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.



Clearer Understanding of Public-Private Information Sharing

United Kingdom: The UK has a unique interface with the private sector that is primarily driven by its intelligence agencies. The CPNI is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage. The advice under which these threats are addressed covers physical, personnel and information security, and includes cyber security.

Canada: As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to identify any gaps and modernize Canada's frameworks for information sharing accordingly. In this regard, it may be useful to learn more about the UK's new national security hub to facilitate public-private information sharing.

Canada-UK Cooperation

Cyber security is gaining sustained and high-level attention globally. As an indication of the importance placed on the issue by close allies,

The Internet has historically been managed through a public-private model that is coordinated by a non-profit corporation based in the US, namely the Internet Corporation for Assigned Names and Numbers (ICANN). However, there is a concerted international effort, to place governance of the Internet under United Nations control, as they see this as a venue that will be more amenable to their interests in increasing state power over the regulation and control of information. Further, these countries are advocating for international treaties to govern key aspects of cyberspace, such as cyber arms control and regulation over cyber security measures.

United Kingdom: The UK with the support of like-minded countries, launched a counter-narrative with the London Conference on Cyberspace on November 1–2, 2011. This narrative emphasizes that:

- the current governance of the Internet, with a multi-stakeholder model that includes the private sector, has worked well by enabling incredible innovations and economic growth;
- going forward, the international community should focus on non-binding norms, which would set out the broad "rules of the road" for interactions in cyberspace; and,
- existing principles of international law, such as human rights law and the law of armed conflict, apply equally in cyberspace.

Underpinning this normative approach to cyberspace is the idea that no major structural changes to Internet governance or the international system are required to address new cyber issues.

The London Conference on Cyberspace represented a major initiative: it was hosted by the UK Foreign Minister William Hague, featured high-level participation (including from US Vice President Joseph Biden), and brought together representatives from over 60 countries, the private sector and civil society. Hungary will host the next Conference in Budapest in October 2012, and will likely feature similar prominent political engagement.

s.13(1)(a)
s.15(1) - Int'l

Canada: Canada has actively supported the UK in its efforts to sponsor norms for cyberspace that promote safe, predictable and consistent interactions while ensuring the Internet's accessibility and openness. [redacted]

[redacted]

Canada is a signatory to, and has committed publicly to ratifying, the Council of Europe Convention on Cybercrime, also known as the "Budapest Convention." Key allies, including the UK and the US, view this as a key international agreement and are eager for Canada to complete its ratification process. The recently tabled Bill C-30 contains measures, including provision for data preservation orders, which would enable Canada to ratify the Budapest Convention.

s.15(1) - Int'l
s.21(1)(b)

Pages 223 to / à 225

are not relevant

sont non pertinentes

SCENARIO NOTE FOR THE MINISTER

LUNCH WITH SIR FRANCIS MAUDE,
MINISTER FOR THE CABINET OFFICE, CYBER SECURITY

Issue

You will attend lunch with Sir Francis Maude, Minister for the Cabinet Office, Cyber Security. The expected topics of conversation will include:

- International cyber governance, and approaches to global cyber security threats and trends;
- Canada-UK cooperation and common narrative on cyber security; and,
- Emergency management, community resilience, and civil contingencies.

A biography of Sir Francis Maude and key messages for the meeting follow this note.

There will not be a gift exchange.

Strategic Objectives

The suggested objectives of your meeting are to:

- Convey the message that Canada and the UK face the same cyber threats [redacted]
- Obtain a clearer understanding of how the UK provides intelligence to private sector organizations, particularly in light of the UK's November 2011 update to its *National Cyber Security Strategy*;
- [redacted]
- Exchange best practices on and gain an understanding of the UK's National Risk Register of Civil Emergencies the UK's support for prevention/mitigation and resilience; and,
- [redacted]

Role of Sir Francis Maude

As Minister for Cabinet Office, Sir Francis is responsible for the following issues:

- Public Sector Efficiency and Reform;
- UK Statistics;
- Civil Service issue;
- Government transparency;
- Civil Contingencies;
- Cyber security; and,
- Overall responsibility for Cabinet Office policy and the Department

s.21(1)(a)

RDIMS# 603082

With respect to his cyber security and civil contingencies responsibilities, Sir Francis is supported by the Office of Cyber Security and Information Assurance (OCSIA) and Civil Contingencies Secretariat (CCS), both located in the Cabinet Office.

Sir Francis chaired the panel on "Social Benefits of the Internet" at the London Conference on Cyberspace, November 1-2, 2011.

The Office of Cyber Security and Information Assurance

The OCSIA supports the Minister for the Cabinet Office, Francis Maude and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK.

The OCSIA, alongside the Cyber Security Operations Centre, works with lead government departments and agencies such as the Home Office, Ministry of Defence (MoD), the Government Communications Headquarters (GCHQ), the Communications-Electronics Security Group (CESG), the Centre for the Protection of National Infrastructure (CPNI) and the Department for Business, Innovation and Skills (BIS) in driving forward the cyber security program for the UK government and giving the UK the balance of advantage in cyberspace.

The Civil Contingencies Secretariat

The UK's lead agency for emergency management and resiliency issues is the Civil Contingencies Secretariat (CCS) located in the UK Cabinet Office. The CCS is responsible for all program management and policy development related to building resilience working in close cooperation with the devolved administrations of Scotland, Wales and Northern Ireland. The CCS is also responsible for coordinating the UK response to non-terrorist emergencies affecting the national interest. In a terrorist emergency with large-scale consequence management issues, the CCS is responsible for coordinating the recovery in concert, if necessary, with a lead department. The secretariat is led by a director, Christina Scott, who reports to the UK National Security Advisor to the Prime Minister. The director is supported by four deputy directors each of whom is responsible for one of the four divisions that comprise the CCS: Horizon Scanning and Response, Capabilities, Local Response Capability, and the Emergency Planning College

Controversy Regarding Sir Francis Maude and Emergency Preparedness

Critics of the UK government are accusing Sir Francis of sparking nation-wide panic over gasoline shortages because of his comments regarding a potential fuel-truck driver strike. In a television interview on March 27, 2012, Sir Francis suggested that "a bit of extra fuel in a jerry can in the garage is a sensible precaution to take", which is twice the official limit that can be safely stored in one container at a private home in the UK. Several Labour Members of Parliament have called for Sir Francis' resignation as Minister.

Canada's "72 Hour Be Prepared" approach does not recommend securing a reserve of gasoline.

Briefing notes on cyber security **(TAB 4L)** and emergency management **(TAB 4M)** are enclosed.

Sir Francis Maude
Minister for the Cabinet Office, Cyber Security

Francis was born in 1953. He was educated at Abingdon School, Corpus Christi College, Cambridge and the College of Law. He's married with five children; and lives at Dial Post.

Francis was elected as Member of Parliament for North Warwickshire in 1983 until 1992, during which time he was a PPS (1984-85); Government Whip (1985-87); Minister for Corporate and Consumer Affairs at the Department of Trade and Industry (1987-89); Minister of State at Foreign and Commonwealth Office (1989-90); and Financial Secretary to the Treasury (1990-92).

He lost his seat at the 1992 election, and in June that year was made a Privy Counsellor.

Francis was appointed a non-executive Director of ASDA Group Plc in July 1992. He was a Director of Salomon Brothers from 1992-93; a Managing Director of Morgan Stanley & Co Ltd 1993-97. Francis was Chairman of the Government's Deregulation Task Force from 1994-97.

In May 1997 Francis was elected to serve as Member of Parliament for Horsham.

In June 1997, he was appointed Shadow Secretary of State for Culture, Media and Sport. Francis was Shadow Chancellor of the Exchequer from June 1998 until February 2000 and from February 2000 to September 2001, he was Shadow Foreign Secretary. Francis then decided to spend a few years as backbencher, during which time he became Vice-Chairman of the All Party Parliamentary Group on AIDS.

In May 2005, Francis returned to the Front Bench when he was appointed Chairman of the Conservative Party. In July 2007, he was appointed Shadow Minister for the Cabinet Office and Shadow Chancellor of the Duchy of Lancaster.

Following the formation of the Coalition Government, Francis was appointed Minister for the Cabinet Office and Paymaster General.

RDIMS# 602079

LUNCH WITH SIR FRANCIS MAUDE

KEY MESSAGES

Cyber Security

Global Cyber Security Threats and Trends

- Note that cyber threats remain a significant concern to Canada. The range of threats is growing, encompassing hacker activities as well as criminal groups and state sponsored espionage.

[redacted]

- Highlight Canada's initiative to bring a large portion of our government departmental networks under the management of a single new organization called Shared Services Canada. This initiative is meant to reduce the contact points of our network to the internet, allow for better monitoring of what goes in and out, and improve security measures to protect Government of Canada systems.

Canada-UK Cooperation [redacted]

- Emphasize that Canada appreciates the international leadership and resolve shown by the UK in advancing a high level dialogue on norms and principles of behaviour for all stakeholders in cyberspace.

- Highlight that Canada strongly supports the UK in promoting common interests and policy positions on cyber security.

- Emphasize the importance of the October conference in Budapest, as the follow on from the London Conference on Cyberspace, as another key opportunity to influence the international discussion on cyber security and cyberspace generally.

- Note that our work on cyber security is one of the action items of the Canada-UK Joint Declaration, signed by our Prime Ministers on September 22, 2011.

- Underline that both Canada and the UK are working closely at the strategic level [redacted]

Clearer Understanding of Public-Private Information Sharing

- Inquire about the creation of a UK "hub" for government and private sector information sharing, the objectives for this hub, and how it would work.

- Inquire about the needs identified by the UK private sector and how the UK plans to respond to these needs.

- Inquire about the kinds of challenges the UK faces in sharing information with the private sector to enhance the security of networks and systems.

Emergency Management: Prevention/Mitigation

- Convey Canada's recognition of the importance of prevention/mitigation and resilience as key principles of effective emergency management. Building resilience and a culture of prevention at all levels helps maintain and enhance the safety and security of Canadians.

- Note that in response to the increasing intensity and diversity of severe weather events. Public Safety is working with other federal departments, provincial and territorial governments, and international colleagues to address the impacts on emergency management.

- Mention that the Government of Canada, in partnership with provincial and territorial governments is developing a new National Disaster Mitigation Program that aims to strengthen community resiliency.

- Convey our willingness to share information on the work on Canada's Platform for Disaster Risk Reduction, and extend an invitation to the U.K. to attend the next Annual National Roundtable of Canada's Platform, which will take place in Vancouver in October 2012.

BRIEFING NOTE FOR THE MINISTER

CANADA-UNITED ARAB EMIRATES RESPONSIVE ISSUES

Visa Requirement

United Arab Emirates (UAE) nationals require a visa to enter Canada. As of October 24, 2012, processing times for UAE nationals' temporary residence visa applications were 12 days for a visitor visa, seven weeks for a study permit and five months for a temporary work permit.

In 2009-2010, the UAE decided to pursue visa impositions on countries that had visa requirements for UAE nationals, including Canada. Based on a country visa review led by Citizenship and Immigration Canada in consultation with partners, including the Public Safety Portfolio, Canada decided to maintain its visa requirement due to safety and security issues.

Since late 2009, Canadians require a travel visa to transit through or visit the UAE (ranging from $165 for a short term single entry visa to $660 for a multiple entry visa),

Over 40,000 Canadians are living and working in the UAE, and over 135 Canadian businesses are located there, serving the region and beyond.

In 2012, to enhance the relationship between both countries, Ministers of Foreign Affairs John Baird and Sheikh Abdullah agreed on three actions:

- launch a Canada-UAE Business Council, which has been delivered;
- conclude a Nuclear Cooperation Agreement, which has been announced; and
- address the visa issues, which are still the subject of discussions between Canadian and UAE officials.

Citizenship Fraud

As of September 2012, approximately 150 Canadian citizens that have UAE as their place of birth were being investigated for citizenship fraud,

Cyber Security Issues

The UAE has actively advocated against Canadian positions in international venues on cyber security issues. Most recently, as chair of the World Conference on International Telecommunications (WCIT), the UAE led negotiations on the recently revised International Telecommunications Regulations, which Canada did not sign.

[redacted]

Canada's operating environment for cyber security varies significantly from the UAE. In the UAE critical infrastructure is largely under state control. [redacted] Canada views the current multi stakeholder model of Internet governance and an open Internet as being essential.

Public Safety Canada, through the Canadian Cyber Incident Response Centre, works on an incident by incident basis with international computer emergency response teams. This can include cooperation with regional incident response organizations or directly with the UAE Computer Emergency Response Team.

Budapest Convention. The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the first and only international treaty to specifically deal with cybercrime. Some countries (Russia, China and many developing countries) have been reluctant to join the treaty, arguing that aspects of its core elements violate national sovereignty and are instead calling for a new United Nations (UN) cybercrime treaty.

Canada is an observer at the Council of Europe and contributed to the development of the treaty. The treaty was signed by Canada and its ratification is pending the enactment of legislative amendments contained in Bill C-30, the *Protecting Children from Online Predators Act.*

Internet Governance. The current day-to-day operations of the Internet are managed by a group of non-profit organizations, academics and engineers based primarily in the United States. While Canada and its allies strongly support this multi-stakeholder approach, [redacted] want greater state control over the Internet and the information transmitted over it.

This governance debate was front and centre at the recent World Conference on International Telecommunications (WCIT), organized by the International Telecommunications Union (ITU). The ITU is a UN body originally founded in 1865 to regulate telegrams and which today governs telephone communications between countries. At the WCIT, Russia, China and certain Arab states, including the UAE, put forward modifications to the International Telecommunication Regulations (ITRs), some of which made reference to the Internet [redacted] Prior to the conference, Canada and its allies made it clear that such modifications were unacceptable and therefore refused to sign the revised treaty.

CANADA-UAE RESPONSIVE ISSUES

KEY MESSAGES

Visas

- Note that the Minister of Citizenship and Immigration Canada is responsible for visa, immigration and citizenship-related matters and that you will convey the UAE government message to him.
- Convey that the Government of Canada continues to welcome visitors, students, and temporary workers from the UAE.
- Convey that Canada continues to seek ways to improve its visa application process and to facilitate contact between our countries' officials.

Cyber Security Issues

- Note that in 2010, the Government of Canada released a cyber security strategy that focuses our efforts on securing Government systems, partnering to secure vital systems outside of the federal Government and helping to keep Canadians secure online.
- Convey that Canada is confident that supporting a safe and open Internet is in all of our interests.

BRIEFING NOTE FOR THE MINISTER

RESPONSIVE ISSUES

International Cyber Issues

Two of the key cyber issues currently being debated internationally concern Internet governance and the Budapest Convention.

Internet Governance

This was highlighted at the recent World Conference on International Telecommunications (WCIT), a two-week conference to update an international telecommunications treaty.

Canada is opposed to such efforts as they undermine the current Internet governance model where states, the private sector and civil society contribute to decision making.

A resolution annexed to the final text could be interpreted as giving the UN a greater role in managing the Internet. This was one of the many reasons Canada declined to sign the updated treaty In Canada and developed countries, most critical infrastructure is owned and operated by the private sector.

In late 2010, Jordanian legislative efforts culminated with the passage of the *Information Systems Crimes Law*. This legislation addresses serious criminal activity conducted via the Internet but also includes law enforcement oversight provisions such as warrants and maintenance of law enforcement records.

Budapest Convention

The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the first and only international treaty to specifically deal with cybercrime. Some countries (Russia, China, Jordan and many developing countries) are reluctant to join the treaty, arguing that aspects of its core elements violate national sovereignty and are instead calling for a new UN cybercrime treaty.

Canada is an observer at the Council of Europe and contributed to the development of the treaty. The treaty was signed by Canada and its ratification is pending the enactment of legislative amendments contained in Bill C-30, the *Protecting Children from Online Predators Act.*

Public Safety Canada, through the Canadian Cyber Incident Response Centre, works on an incident by incident basis with international computer emergency readiness teams. This can include cooperation with regional incident response organizations.

Canadian Funding to United Nations Relief and Works Agency for Palestine Refugee in the Near East (UNRWA)

[redacted] Canadian funding to the United Nations Relief and Works Agency for Palestine Refuges in the Near East (UNRWA). As home to nearly two million Palestinian refugees, Jordan relies on UNRWA funding to support this population.

In 2009, CIDA stopped providing funds to UNRWA's general fund, which finances education, health and social services to Palestinian refugees in Jordan, Lebanon, Syria and the West Bank and Gaza. Since then, funding has been provided to food security programming in West Bank and Gaza, in line with Government of Canada development priorities. The announcement of this shift in funding provoked reactions from a number of countries, including Jordan. UNRWA's support to Palestinian refugees in Jordan is derived from the UNRWA's core services budget.

Canada recognizes the important role of UNRWA. Canada's contribution is determined annually based on a variety of factors, including alignment with current aid priorities and availability of resources. While Canada no longer provides funding to the general fund, we contributed $15 million to UNRWA's 2011 Emergency Appeal for West Bank and Gaza.

This funding helped deliver food aid to about 650,000 refugees in Gaza, helped support a school feeding program benefiting more than 200,000 children, and assisted with the creation of more than 82,000 jobs for almost 33,000 refugee families in the West Bank.

s.15(1) - Int'l

UNCLASSIFIED

RESPONSIVE ISSUES

Key Messages

Cyber

- In 2010, the Government of Canada released a cyber security strategy which focuses our efforts on securing Government systems, partnering to secure vital systems outside of the federal Government and helping to keep Canadians secure online.

- Canada is confident that supporting a safe and open Internet is in all of our interests.

United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA) Funding

- UNRWA is a key humanitarian assistance partner. Canada recognizes the important role of UNRWA in meeting the humanitarian needs of Palestinian refugees.

- Canada's contribution is determined on a yearly basis on a variety of factors, including alignment with current aid priorities and availability of resources.

- In 2011, Canada contributed $15 million to UNRWA's 2011 Emergency Appeal for the West Bank and Gaza.

- That contribution helped deliver food aid to refugees in Gaza, supported a school feeding programme, and assisted with the creation of jobs for thousands of refugee families in the West Bank.

Pages 239 to / à 245

are not relevant

sont non pertinentes

Pages 247 to / à 254

are not relevant

sont non pertinentes

PACP meeting on

Progress made on OAG Report

Word count: 653 words

Duration: 6 to 6.5 minutes

Speechwriter: Janet Nuutilainen (998-7897)

Notes for Opening Remarks by

François Guimont
Deputy Minister of Public Safety

To discuss Public Safety's Management Action Plan in response to

Chapter 3 of the Fall 2012 Report of the Office of the Auditor General of Canada Protecting Canadian Critical Infrastructure Against Cyber Threats

Standing Committee on

Public Accounts

Ottawa, Ontario

March 2013

Check against delivery

- Thank you, Mr. Chair.

- I'm pleased to be here to discuss the progress that Public Safety Canada has made in response to Chapter Three of the *Fall 2012 Report of the Auditor General of Canada.*

- I am joined by (officials TBD)

- Mr. Chair, Canada and its allies face real and significant threats from persistent cyber intrusions aimed at trade secrets, sensitive business information and intellectual property.

- The cyber threat environment evolves quickly, and we must adapt to new vulnerabilities and methods for exploiting our systems.

- Moreover, cyber security is a pervasive challenge that involves virtually all government departments and agencies at all levels, international allies, industry partners and Canadians and their families.

- To address this challenge, Public Safety Canada is working closely with our domestic and international partners to monitor threats, provide support and guidance to private sector owners and operators, and coordinate the national response to cyber incidents when they occur.

- Together, we have launched site assessments of critical infrastructure sectors, delivered threat briefings to raise awareness among stakeholders, and developed partnerships with international cyber emergency response teams.

- Mr. Chair, my department has submitted our Management Action Plan, which outlines our progress and next steps to respond to the Auditor General's recommendations.

- The first recommendation was for Public Safety Canada to develop a public action plan with deliverables and timelines for *Canada's Cyber Security Strategy*.

- In fact, an implementation plan was developed prior to the launch of the *Strategy* in October 2010.

- But, given the sensitive, classified nature of the activities related to protecting government systems, it could not be released publicly.

- A public version of this plan has now been developed, and will be released in the coming weeks - TBD.

- It will communicate our progress more clearly to Canadians, and underscore the need for all Canadians, and owners and operators of vital systems, to do their part.

- The public implementation plan sets out an active, partnership-based approach to addressing cyber threats. It reflects our ongoing commitment to working closely with our international and domestic stakeholders, and with Canadians and their communities.

- We have also developed a horizontal performance measurement strategy, with input from key departments and agencies, to help us track progress made on our *Cyber Security Strategy*.

- The second recommendation was to bolster our critical infrastructure sector networks, and ensure that the right stakeholders are being engaged by Public Safety Canada and our Portfolio agencies.

- To date, my department has created a planning guide and risk management guide for critical infrastructure sectors. Both have been shared with our sector networks to help them develop risk management plans that are tailored to the needs of critical infrastructure owners and operators.

- We have also a launched site assessment program for these owners and operators, and we regularly coordinate threat briefings for our sector networks.

- Public Safety Canada is also working with lead federal departments and agencies to review the membership of the sector networks, and ensure that we are building partnerships with the full range of stakeholders.

- The Auditor General's third recommendation was to increase the capacity of the Canadian Cyber Incident Response Centre, or CCIRC.

- In response, CCIRC has expanded its operational hours to 15 hours a day, seven days a week onsite coverage, allowing it to cover the full business operating hours of its clients.

- It's important to note, however, that CCIRC experts are on call 24 hours a day, seven days a week, to deal with emergency situations.

- This on-call system is similar to those used by our international allies, including the United Kingdom.

- CCIRC has also taken steps to improve information sharing and dialogue with its partners, including launching an incident response pilot and establishing an online Community Portal.

- Mr. Chair, as you can see, much has been done to address the Auditor General's recommendations, but more work remains.

- And we are committed to ongoing efforts to secure Canada's cyber systems and critical infrastructure sectors.

- Thank you.

French speech:

PACP meeting on

Progress made on OAG Report

Word count: 628 words

Duration: 6 minutes

Speechwriter: Janet Nuutilainen (998-7897)

Notes pour le mot d'ouverture de

François Guimont
Sous-ministre de Sécurité publique Canada

sur le plan d'action de la gestion de Sécurité publique Canada en réponse au

Chapitre 3 du rapport d'automne 2012 du Bureau du vérificateur général du Canada – Protéger l'infrastructure canadienne essentielle contre les cybermenaces

Comité permanent des comptes publics

Ottawa (Ontario)

Mars 2013

Priorité au discours prononcé

- Merci, Monsieur le Président.

- Je suis heureux d'être ici présent pour faire état des progrès réalisés par Sécurité publique Canada pour donner suite au chapitre 3 du rapport d'automne 2012 du Bureau du vérificateur général du Canada.

- Je suis accompagné de (officials TBD)

- Monsieur le Président, le Canada et ses alliés sont confrontés à des menaces réelles et grandissantes, soit des cyberintrusions persistantes visant les secrets commerciaux, les données confidentielles des entreprises et la propriété intellectuelle du Canada.

- Or, le contexte des cybermenaces évolue rapidement, et nous devons faire face aux vulnérabilités et nous adapter aux nouvelles méthodes d'exploitation des systèmes.

-

- De plus, la cybersécurité est un défi omniprésent qui touche pratiquement tous les ministères et organismes de tous les ordres de gouvernement, de même que les alliés internationaux, les partenaires de l'industrie ainsi que les Canadiens et leurs familles.

- Pour faire face à ce défi, Sécurité publique Canada travaille étroitement avec les partenaires nationaux et internationaux dans le but de surveiller les cybermenaces, de conseiller et d'appuyer les propriétaires et exploitants du secteur privé et de coordonner l'intervention nationale advenant un cyberincident.

- Ensemble, nous avons effectué des évaluations sur les sites d'infrastructures essentielles, nous avons offert des séances d'information pour sensibiliser les intervenants aux menaces et nous avons établi des partenariats avec les équipes internationales d'intervention en cas d'urgence informatique.

- Monsieur le Président, mon ministère a présenté le Plan d'action de la gestion, lequel énonce les progrès réalisés et les étapes à suivre pour répondre aux recommandations du vérificateur général.

- La première recommandation demandait à Sécurité publique Canada d'établir un plan d'action public, ainsi que des résultats et des échéanciers pour la Stratégie de cybersécurité du Canada.

- En fait, un plan de mise en œuvre a été établi avant le lancement de la Stratégie en octobre 2010.

- Mais, compte tenu de la nature délicate et confidentielle des activités liées à la protection des systèmes gouvernementaux, le plan de mise en œuvre ne pouvait pas être rendu public.

- Une version publique du plan a été élaborée, et sera publiée au cours des prochaines semaines - TBD.

- Cette version viser à informer les Canadiens des progrès réalisés et à mettre l'accent sur la nécessité pour tous les Canadiens et les propriétaires et exploitants des systèmes essentiels de fournir leur part d'efforts.

- Le plan de mise en œuvre public établit une approche active et fondée sur les partenariats visant à faire face aux cybermenaces. Le plan témoigne de notre engagement continu à travailler en étroite collaboration avec nos partenaires internationaux et nationaux, ainsi qu'avec les Canadiens et leurs collectivités.

- Nous avons également élaboré une stratégie horizontale de mesure du rendement en collaboration avec les principaux ministères et organismes, laquelle nous aidera à déterminer les progrès réalisés dans le cadre de la Stratégie de cybersécurité du Canada.

- La deuxième recommandation visait à renforcer les réseaux d'infrastructures essentielles, et à veiller à ce que les intervenants appropriés soient consultés par Sécurité publique Canada et les organismes du Portefeuille.

- Jusqu'à présent, un guide de planification et un guide de gestion des risques pour les secteurs d'infrastructures essentielles ont été élaborés par mon ministère. Les deux guides ont été communiqués aux réseaux sectoriels, afin de les aider à élaborer des plans de gestion des risques adaptés aux besoins des propriétaires et exploitants d'infrastructures essentielles.

- Nous avons également lancé un programme d'évaluation des sites pour les propriétaires et exploitants, et nous organisons régulièrement des séances d'information sur les menaces à l'intention des réseaux sectoriels.

- Sécurité publique Canada travaille aussi avec les principaux ministères et organismes fédéraux pour revoir la composition des réseaux sectoriels et veiller à ce que des partenariats soient mis en place avec tous les intervenants.

- La troisième recommandation du vérificateur général proposait de renforcer la capacité du Centre canadien de réponse aux incidents cybernétiques ou le CCRIC.

- Pour donner suite à cette recommandation, le CCRIC a prolongé ses heures de travail pour fournir des services, à raison de 15 heures par jour, sept jours par semaine, dans le but de couvrir toutes les heures d'opération de ses clients.

- Il est cependant important de signaler que les experts du CCRIC sont mis en disponibilité 24 heures par jour, sept jours par semaine, pour faire face aux situations d'urgence.

- Ce système d'appels est similaire à ceux utilisés par nos alliés internationaux, notamment le Royaume-Uni.

- Le CCRIC a également pris les mesures requises pour améliorer l'échange d'information et le dialogue avec ses partenaires, notamment en lançant un projet pilote d'intervention en cas d'incident et en créant un portail en ligne pour la communauté.

- Monsieur le Président, comme vous pouvez le constater, beaucoup de travail a été accompli pour donner suite aux recommandations du vérificateur général, mais il reste encore un long chemin à faire.

- Et, nous tenons à poursuivre les efforts pour assurer la sécurité des systèmes cybernétiques et des secteurs d'infrastructures essentielles du Canada.

- Merci.

Key Messages

Public Safety Canada's Management Action Plan In response to *Chapter 3 of the Fall 2012 Auditor General Report*

Overarching

- The Auditor General's report recognizes the positive steps that Public Safety Canada has taken in recent years, and acknowledges the progress made since Public Safety Canada launched the cyber security and critical infrastructure strategies in 2010.

- We have, in fact, made significant progress, particularly in recent years, in the midst of an evolving threat environment.

- Like other countries, Canada is confronted by real and significant cyber threats, and while there is much work ahead of us, we are committed to working with our domestic and international partners to ensure continued progress.

- The Government of Canada is continuously working to enhance cyber security in Canada by identifying cyber threats and vulnerabilities, and by preparing for and responding to all types of cyber incidents to better protect Canada and Canadians.

Progress Highlights

- Public Safety Canada developed a public action plan for *Canada's Cyber Security Strategy* that will more clearly communicate to Canadians how progress is being achieved and underscore the need for all Canadians, and owners and operators of vital systems, to do their part.

- We have also developed a horizontal performance measurement strategy to allow us to track and report on progress made against our commitments in *Canada's Cyber Security Strategy*.

- As noted by the Auditor General, we have also developed longstanding partnerships with critical infrastructure sectors, including a National Cross Sector Forum that brings together representatives from all ten critical infrastructure sectors to identify priorities for collaborative action, such as raising awareness of cyber threats.

- Moving from partnerships to action, Public Safety Canada has launched a site assessment program for critical infrastructure sectors and published a *Risk Management Guide for Critical Infrastructure Sectors*.

- Most recently, Public Safety Canada developed a *Critical Infrastructure Planning Guide* and provided it to critical infrastructure sectors to strengthen our shared readiness to respond and recover swiftly when disruptions occur.

- The Canadian Cyber Incident Response Centre (CCIRC) has expanded its operational hours to 15 hours a day, seven days a week onsite coverage. However, it has 24/7 capacity. All of our private sector clients can reach CCIRC to get a quick response and support 24 hours a day through the Government Operations Centre.

- The CCIRC has also taken steps to improve information sharing and dialogue with its partners, including launching an incident response pilot and establishing an online Community Portal.

- CCIRC shares cyber threat and mitigation information on a daily basis with the private sector, other levels of Government, security partners and allies to ensure that Canada's vital systems and critical infrastructure are secure.

Detailed Messaging On Specific OAG Recommendations

***Recommendation 1:* PS should develop an interdepartmental action plan with deliverables and timelines for the Cyber Security Strategy (2010) to guide the implementation of the strategy and measure progress.**

- A detailed, classified implementation plan was developed and approved prior to the launch of *Canada's Cyber Security Strategy* in October 2010.

- But given the sensitive, classified nature of the activities related to protection of Government of Canada systems, it could not be released publicly.

- Public Safety Canada will release an unclassified action plan in order to communicate more clearly to Canadians how the progress is being achieved and to underscore the need for all Canadians, and owners and operators of vital systems, to do their part.

***Recommendation 2:* PS should ensure that all sector networks are fully established and operating as outlined in the national strategy and action plan for Critical Infrastructure so that they can be an effective tool in helping to secure critical infrastructure in order to deliver the objectives of the Cyber Security Strategy.**

- The Government of Canada has longstanding partnerships with critical infrastructure sectors, including energy, finance, and transportation – something the OAG has acknowledged.

- Since the 2010 announcement of the *National Strategy and Action Plan for Critical Infrastructure*, the Government has formalized these partnerships with the creation of networks for each critical infrastructure sector.

- These partnerships have helped the Government achieve significant progress in enhancing the resilience of Canada's critical infrastructure.

- As noted by the Auditor General, we have established a National Cross Sector Forum that brings together representatives from all ten critical infrastructure sectors to identify priorities for collaborative public-private sector action.

- Public Safety Canada has also taken significant risk management actions, including launching a site assessment program for critical infrastructure sectors and publishing a *Risk Management Guide for Critical Infrastructure Sectors.*

  Public Safety Canada developed a *Critical Infrastructure Planning Guide* and provided it to critical infrastructure sectors to strengthen our shared readiness to respond and recover swiftly when disruptions occur.

- Together with the private sector and first responder community, the Government of Canada is committed to sharing information on risks and threats to ensure that we are collectively prepared to address all threats to critical infrastructure, including cyber threats, terrorism, and natural disasters.

- In keeping with the OAG's recommendation, Public Safety Canada will continue to work with other federal departments and agencies to improve the sector networks and build partnerships with the private sector.

***Recommendation 3:* PS should increase the CCIRC's ability to maintain situational awareness of cyber threats to Canada's critical infrastructure and to increase the**

Centre's ability to communicate this information to critical infrastructure owners and operators.

- The Canadian Cyber Incident Response Centre (CCIRC) is the national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events for systems external to the Government of Canada.

- The Minister of Public Safety announced funding to expand CCIRC's operating capacity in October 2012. This funding specifically worked to:

    - Strengthen CCIRC's legal, policy and process foundations to ensure authority and capabilities are in place to deliver on CCIRC's assigned mandate;

    - Expand collaboration with internal and external partners to improve incident response across Canada; and

    - Strengthen analytical capability to improve mitigation advice and incident response for partners.

- CCIRC began operating 15 hours a day, 7 days a week on November 5th, 2012, to provide business hour coverage from coast to coast to coast.

- However, CCIRC has always had 24/7 capacity. All of our private sector clients can reach CCIRC to get a quick response and support 24 hours a day through the Government Operations Centre.

- CCIRC shares cyber threat and mitigation information on a daily basis with the private sector, other levels of Government, security partners and allies to ensure that Canada's vital systems and critical infrastructure are secure.

- CCIRC is responsible for providing authoritative advice and support, and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

- The Government of Canada will continue this cooperation to ensure that any risks to Canada's critical infrastructure are identified and addressed, for the benefit of all Canadians.

- Public Safety Canada has also:
    - Updated its mandate, policies and procedures to provide greater clarity to partners;
    - Introduced the Community Portal to facilitate communication and information exchange between CCIRC and its partners;
    - Established formal information-sharing agreements with CCIRC's main partners; and
    - Launched an incident response pilot to improve information-sharing among partners.

If asked about the finding that since 2001 "$780 M has been allocated to emergency management and other NS activities, including CI protection":

- It is important to be clear that while a portion of the $780M referenced by the OAG went directly to protecting critical infrastructure from cyber threats, a significant portion was committed to other important national security and emergency management areas. Specifically:

    - $20.9M over ten years went **directly** to policy and program work across several departments and agencies to protect critical infrastructure from cyber threats;

- $570M went to CSEC for a number of activities of national security importance – including the protection of government systems from cyber attacks. This is of great importance for the protection of Canadians and their information since the Government of Canada is the largest target for cyber attacks within our borders; and

- The remaining $190M supported a variety of activities not directly related to critical infrastructure, but still of national importance, across a number departments and agencies, ranging from marine security to emergency management training activities.

    - *If pressed on which departments received funding:*
        - That funding was distributed over the last decade to various departments, including: DND; Treasury Board; PWGSC; CSE; Finance; Industry Canada; NR Can; Transport Canada; CSIS; RCMP; Solicitor General; Justice

If asked for further details on the $570M allocated to CSEC:

- We cannot comment on specific operational activities of CSEC.

If pressed on GoC investments in own networks:

- We do not comment on specifics with respect to our classified systems.

If asked about the finding that Government information systems have been vulnerable to intrusion:

- Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. We take this responsibility seriously.

- Since the release of *Canada's Cyber Security Strategy*, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents.

- In 2011, we introduced the Government IT Shared Services initiative to transform the way government manages IT telecommunications, desktop computer services, data centres, IT security services and Internet access points.

If asked about media reports of incidents involving CCIRC responses:

- The Government of Canada, advised by its law enforcement and security agencies, is vigilant in monitoring any potential threats and has robust measures in place to address them.

- We do not comment on specific or potential threats. However, we can say that the Canadian Cyber Incident Response Centre (CCIRC) has 24/7 capacity. All of our private sector clients can reach CCIRC to get a quick response and support 24 hours a day.

- CCIRC shares cyber threat and mitigation information on a daily basis with the private sector, other levels of Government, security partners and allies to ensure that Canada's vital systems and critical infrastructure are secure.

- CCIRC is responsible for providing authoritative advice and support, and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

- Cyber threats evolve rapidly. The protection of Canada's cyber security is a shared responsibility. Successful implementation of Canada's Cyber Security Strategy depends on partnerships and information-sharing with other governments and industry to ensure the resilience of cyber systems vital to Canadian security and economic prosperity.

- The Government of Canada will continue this cooperation to ensure that any risks to Canada's critical infrastructure are identified and addressed, for the benefit of all Canadians.

If asked about the Mandiant report:

- The Government of Canada, advised by its law enforcement and security agencies, is vigilant in monitoring any potential threats and has measures in place to address them.

- While we will not comment on specific incidents for reasons of privacy and national security, we can say that threats to Canada, our businesses, governments and citizens from cyber espionage, organized crime and hackers are real.

- Canada fully supports the U.S. intention to protect itself from cyber theft, and our Government will likewise continue to take strong action to protect Canada's citizens and economy from cyber espionage.

- Successful implementation of Canada's Cyber Security Strategy depends on partnerships and information-sharing with other governments and industry to ensure the resilience of cyber systems vital to Canadian security and economic prosperity.

- The Government of Canada is committed to protecting Canada's cyber security. Cyber threats evolve rapidly, and it is essential that the Government of Canada, owners and operators of Canada's vital cyber systems, and even Canadians, work together to protect those systems and those who depend upon them. The protection of Canada's cyber security is a shared responsibility, and we all have a role to play.

- CCIRC is responsible for providing authoritative advice and support, and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

- CCIRC shares cyber threat and mitigation information on a daily basis with the private sector, other levels of Government, security partners and allies to ensure that Canada's vital systems and critical infrastructure are secure. They do this in full cooperation with national and international counterparts, including the United States.

- Canada is a close partner with the United States and acts in concert to protect the citizens, economies, and shared infrastructure of both our countries from cyber threats. We are committed to working together to protect vital cyber systems, to respond to and recover from any cyber disruptions, and to make cyberspace safer for all our citizens.

- In 2012, Canada and the United States signed a joint Cybersecurity Action Plan, a key commitment under the Beyond the Border Action Plan for Perimeter Security and Economic Competitiveness. The Plan enhances the already strong partnership and cooperation on cyber security matters between both countries, in order to ultimately better protect shared critical digital infrastructure and increase capacity to respond jointly and effectively to cyber incidents.

On communicating with the public:

- Our Government is committed to keeping Canada's cyber systems secure and to protecting Canadians online.

- Cyber Security Awareness Month is an initiative to engage online Canadians to take action, and to provide them with the information they need to protect themselves and their families.

- Government and business leaders promote Cyber Security Awareness Month each October to remind individuals how to protect themselves and to guard against cyber threats.

- We all have role to play when it comes to cyber security.

- *GetCyberSafe* is a key component of *Canada's Cyber Security Strategy*, the government's comprehensive response to the challenge of cyber security.

- *GetCyberSafe* provides Canadians with the information they need to protect themselves and their families against online threats.

- The website is a key component to the campaign – it provides tips and resources to help Canadians protect everything that's important to them. The link to the website is www.getcybersafe.gc.ca.

The 10 Critical Infrastructure Sectors:

Critical Infrastructure Sector	Federal Network Lead
Finance	Finance Canada
Energy and utilities	Natural Resources Canada
Manufacturing	Industry Canada
Transportation	Transport Canada
Health	Public Health Agency of Canada
Food	Agriculture and Agri-Food Canada
Water	Environment Canada
Government	Public Safety Canada
Safety	Public Safety Canada
Information and communication technology	Industry Canada

Public Safety Canada / Sécurité publique Canada

Questions and Answers

Public Safety Canada's Management Action Plan in response to Chapter 3 of the 2012 Fall Report of the Auditor General of Canada

Main Storylines

Why is CCIRC not operational 24/7?

CCIRC has always had 24/7 capacity. At all times, a Cyber Duty Officer is on call and reachable through the Government Operations Centre, which is staffed 24/7. All of our private sector clients can reach CCIRC and get a quick response. If the Cyber Duty Officer feels the incident warrants it, they can call CCIRC's staff back to the office, 24/7, every day.

CCIRC's primary role is to monitor the cyber threat environment and provide technical and strategic advice on cyber threats, as well as to coordinate a national response against cyber attacks, outside of federal government systems.

While CCIRC assists non-federal government entities, it's these entities that are ultimately accountable for protecting their own networks. The federal government cannot be responsible for the administration of all networks in Canada. Private companies and other levels of government all have a responsibility to keep their networks secure.

So having a person on call is a rational use of resources. This is a similar approach used internationally by allied countries like the UK to provide 24/7 coverage.

Over the past eight months, the Government Operations Centre has received 6 calls for CCIRC after hours. For each of those calls, the Government Operations Centre passed the request for assistance to the CCIRC employee on call and the request was handled appropriately. It would not be an effective use of taxpayers' money to have someone waiting at a desk by the phone for those six phone calls.

Over the past few months, we've made the after-hours service even easier to use by putting in direct contact features similar to what you would find in a call centre. After hours, a client calling CCIRC will get a message letting them know that if the matter is an emergency, they can press zero and the call is immediately directed to the CCIRC employee that is on-call.

As the Government announced, CCIRC extended its onsite hours to 15/7 starting on November 5, 2012. The purpose of this extension of hours is to ensure that our critical infrastructure clients, who are located in all time zones across the country, can reach CCIRC during their regular work days.

CCIRC is constantly evaluating its services and looking at how it should adjust its work to be more effective, while always assessing the nature of the threat.

How much funding has gone to cyber security? Where was it allocated?

Departments all across government have long been integrating cyber tools and cyber security into their operations. Every department has invested to protect their own systems. Key agencies and departments have made specialized investments for cyber security - a good portion of Communication Security Establishment Canada's (CSEC) budget is dedicated to securing networks and digital information. This investment is substantial, but detailing all funding to cyber security is a challenge for every country, since many of these investments in research, technical equipment, and capacity have multiple, interconnected uses and have only recently been caught up in the term "cyber security".

In terms of new and recent investments, the Government allocated an additional $90 million at the outset of *Canada's Cyber Security Strategy* across 9 departments and agencies. The lion's share of this funding went to the first pillar of the Strategy, securing Government systems.

The Government of Canada recently announced a further investment of $155 million over five years, going to the Treasury Board Secretariat, Shared Services Canada, and Public Safety Canada. The money to Public Safety was mostly funding for CCIRC to support 15/7 operations.

If pressed for further breakdown:

We cannot comment on internal security measures, nor can we disclose the exact breakdown of the $155M in funding for security reasons.

How was the $780 million referenced by Auditor General used?

Cyber security and critical infrastructure protection are shared responsibilities among federal departments/agencies, other levels of government, and the private sector.

For example, there is spending on cyber security by every federal department and agency, and in various emergency management and national security program areas.

It is important to be clear that while a portion of the $780M referenced by the OAG went directly to protecting critical infrastructure from cyber threats, a significant portion was committed to other important national security and emergency management areas. Specifically:

- $20.9M over ten years went directly to several departments and agencies to protect critical infrastructure from cyber threats;

- $570M over the last ten years went to CSEC to support a range of initiatives, including program integrity (modernizing computers, facilities and corporate services), research and development, as well as building capacity in foreign intelligence and cyber security. This includes the protection of government systems from cyber attacks; and

- The remaining $190M supported a variety of activities not directly related to critical infrastructure, but still of national importance, across a number departments and agencies, including emergency management training, business continuity planning, pandemic planning, continuity of constitutional government, marine security, emergency management exercises, counter-terrorism, creation of a liaison position with the U.S. Department of Homeland Security, development of an all-hazards warning system, enhancements to the Government Operations Centre, and development of the Federal Emergency Response Plan.

The report itself recognizes the positive steps that Public Safety Canada has taken in recent years, and it acknowledges that our Government has made progress since we launched our cyber security and critical infrastructure strategies in 2010.

We have made exceptional progress, particularly in recent years, in the midst of an evolving threat environment. If you look at where we stand today in terms of our critical infrastructure and cyber security, Canada is in a strong position.

If pressed on the $570M to CSEC:

CSEC does not provide funding details that might reveal its capabilities.

Why was only $20 million of the $780 million dedicated to cyber security for critical infrastructure? Why was CCIRC only recently given new funding?

If we look back to the early 2000's when funding was being allocated, there are two things to bear in mind.

First, the identified and current threats were different. 9/11 stressed the ability and willingness of terrorists to undertake physical attacks, so this is where essential work was focused on.

Second, the cyber threat was still evolving. For example, critical infrastructure operators have long had software to remotely control their industrial systems. These did not need major security features because they were all internal and not accessible from outside these companies.

Over the last number of years, as every business has become interconnected through the Internet, it has become possible to affect what once were only internal computer systems and software.

In short, I would say that funding has kept pace with the nature and evolution of national security threats to Canada.

Why can't Public Safety Canada compel critical infrastructure owners and operators to share information with CCIRC? What are regulatory implications or legal requirements for partners?

CCIRC works collaboratively with private sector partners by providing trusted value-added products and services, meaning that it relies on having a service in which organizations want to participate rather than forcing cooperation.

Further, sector networks are not regulatory entities. This also helps foster a trusted environment for all levels of government and industry to share information on threats and vulnerabilities. Because participation is voluntary, we actually see greater cooperation and better information sharing.

We have achieved significant progress with this approach, and risk management activities are underway, including security briefings and exercises.

Can you provide detail on the 2011 attacks on government systems? Why the delay in CSEC contacting CCIRC that is being reported in media? Have any other attacks on government systems taken place?

While I can't comment directly on specific incidents, I can say that generally, in the event of an attack on government systems, the lead agency with the technical abilities to respond is the Communication Security Establishment Canada. They have the tools and authority to mitigate an attack and provide a comprehensive response.

In the event of an incident, a department's Chief Information Officer and CSEC work closely together to determine the best response.

Where security concerns allow, CSEC does keep CCIRC informed so that any relevant information for critical infrastructure can be passed on to private sector stakeholders as required.

The U.S. recently warned against working with certain Chinese corporations. What is Canada doing with that warning?

We do not comment on specific or potential threats, but we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

And while we will certainly take all of the information we receive into consideration, the Government of Canada makes its own decisions on what is in the best interest of Canada.

The Government of Canada supports a prosperous and competitive telecommunications sector in Canada – however, a thriving telecommunications industry must be a safe and secure one.

So we regularly work with telecom companies to ensure that our telecommunications infrastructure is resilient and secure.

The Government of Canada will continue this cooperation to ensure that any risks to Canada's telecommunications sector are identified and addressed.

Are we safe?

Cyber security is an ongoing challenge for all countries, Canada included. To an extent we are all grappling with rapid changes in technology and an evolving world of threats. The Internet and modern communication technologies remain an incredible source of development, growth, prosperity, social connection, and well-being.

But over the last decade we've also seen the downside of our new interconnectedness. Criminal activity, new ways to steal state secrets and private information, cheaper and easier ways to disrupt or even destroy essential services and infrastructure.

While this reality is of concern, it is important to understand that the Government has pursued a balanced approach, where our actions to improve cyber security are proportional to the risks we face.

The Auditor General himself suggested that the only safe system is one which has no users.

Canada, like our allies, has striven to make sure that our pursuit of cyber security does not hinder the fundamental benefits we see from the Internet and modern telecommunications.

I believe we have struck that balance.

Yes, we need to continue our public awareness campaigns like Get Cyber Safe to help Canadians keep themselves safe online.

Yes, we need organizations like CCIRC to help critical infrastructure owners and operators protect the vital systems on which we depend.

Yes, governments need to continue to do their utmost to protect the classified and private information of citizens.

And yes, there are risks, and we need to continue to monitor and assess any potential cyber threats.

But - in no small measure thanks to the efforts we have in place - Canadians can have confidence in the safety and resilience of our country's digital information networks. .

How is the Government of Canada responding to the findings contained within the recent report from the U.S. cyber security firm Mandiant? What is the Government of Canada doing to protect Canada's critical infrastructure from the kind of cyber espionage Mandiant is warning about?

The Government of Canada, advised by its law enforcement and security agencies, is vigilant in monitoring any potential threats and has robust measures in place to address them. While we will not comment on specific incidents for reasons of privacy and national security, we can say that threats to Canada, our businesses, governments and citizens from cyber espionage, organized crime and hackers are real -- and we will continue to take strong action to protect Canada's citizens and economy.

Cyber threats evolve rapidly, and it is essential that the Government of Canada, owners and operators of Canada's vital cyber systems, and even Canadians, work together to protect those systems and those who depend upon them. CCIRC monitors potential cyber threats and advises the private sector on how to detect and defend themselves in the event of any cyber incident. CCIRC works directly with companies, providing them with frontline information on how to secure their systems and deal with potential threats. They do this in full cooperation with national and international counterparts, including the United States.

In terms of protecting joint, cross-border infrastructure, it's worth noting that in 2012, Canada and the United States signed a joint Cybersecurity Action Plan, a key commitment under the Beyond the Border Action Plan for Perimeter Security and Economic Competitiveness. The Plan enhances the already strong partnership and cooperation on cyber security matters between both countries, in order to ultimately better protect shared critical digital infrastructure and increase capacity to respond jointly and effectively to cyber incidents.

Roles in Cyber Security

Q: How are the cyber security roles of various cyber security agencies different? (CSEC, CCIRC, RCMP, CSIS, SSC, TBS, DND)

A. Many departments and agencies have a distinct role, according to their mandate, in delivering on our collective cyber security. They all work together, but each has a distinct and important contribution.

Public Safety Canada coordinates implementation of *Canada's Cyber Security Strategy* and the overall policy coordinator in addressing cyber risks.

Canadian Cyber Incident Response Centre is housed within Public Safety Canada, but has the distinct task of evaluating and providing mitigation advice on cyber threats to vital systems outside of the federal government and coordinating the national response to cyber security incidents.

The RCMP takes over when there is a suspected crime. They investigate suspected domestic and international criminal acts against Canadian networks and critical information infrastructure.

The Canadian Security Intelligence Service provides overall intelligence on national security issues. CSIS investigates threats to the security of Canada and advises government of such threats - including threats against critical information systems and infrastructure.

The Communications Security Establishment Canada is the technical cyber authority for the Government of Canada. CSEC detects and discovers threats, provides foreign intelligence and cyber security services, and responds to cyber threats and attacks against Government networks and information technology systems.

Shared Services Canada was created on August 4, 2011, to manage Government information technology (IT) infrastructure. This includes implementing IT security management across government systems.

The Treasury Board Secretariat sets government-wide direction and establishes priorities for securing government IT systems and networks. Working with the lead security agencies, it provides oversight of IT incident management, including post-mortem reviews and lessons learned.

The Department of National Defence provides cyber protection for its own military assets and undertakes cyber operations in military operations.

Q: Should Canada have a Cyber Czar?

A. While it might seem useful to have all cyber responsibilities brought together under one department, cyber security is a collective responsibility that is core to the operations of many areas of government: emergency management, critical infrastructure, law enforcement, national security and intelligence, and military operations.

Coordination of cyber activities is important, and that is why the Government has designated the Minister of Public Safety as the lead and coordinator of overall cyber security policy. As Canada's central point of contact on cyber security, we often work closely with the U.S. Cyber Czar.

Our model strikes the right balance by having departments work together and coordinate activity, but also allowing them to do what they need to deliver on their own mandates.

Q: What is the difference in the roles and mandates of CCIRC and CSEC?

A: The Communications Security Establishment Canada (CSEC) and CCIRC both have a role in cyber incident management, but they serve different clients.

As the technical cyber authority for Government of Canada networks, CSEC detects and analyses the impact of cyber security incidents that affect the confidentiality, integrity or availability of Government's own networks. CSEC provides mitigation advice to Government of Canada systems owners, as well as guidance and training to promote best IT security practices. CSEC shares cyber threat information and best practices with Public Safety Canada for further dissemination to other levels of government and the private sector where appropriate and where security concerns permit.

As Canada's computer security incident response team for non-government systems, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents.

CCIRC provides authoritative advice and support, and coordinates information sharing and incident response, in conjunction with its domestic and international partners to address high-level cyber security concerns.

Q: What is the role and relationship between CSEC and Shared Services Canada (SSC) now that the latter is leading the consolidation of federal government information technology and systems?

A: CSEC works closely with SSC to provide advice and guidance as part of the Governments Enterprise IT consolidation and transformation initiatives.

Q: What cyber security activities does CSEC conduct on systems outside the federal government?

A: CSEC can provide its unique expertise in collaboration with Public Safety Canada beyond federal networks when called upon to do so. This is a flexible arrangement depending on the situation, threat, and environment.

Q: Why did CSEC take over CCIRC's role?

A: CCIRC's role has been clarified to be outward facing, providing an essential service to public and private sector clients outside of the federal government.

While the two organizations communicate and cooperate with each other, this division of roles is clearer and more straightforward for critical infrastructure clients who need to have a clear point of contact with the federal government.

Q: The Auditor General's report indicates that there are information sharing issues between Communications Security Establishment Canada (CSEC) and Public Safety Canada. Could you please describe the nature of these information sharing issues?

A: As Canada's national cryptologic and signal intelligence agency, CSEC comes into contact with a variety of extremely sensitive information. They are - rightly - scrupulous in not only how they share information, but also in taking care in where and in what form it might be passed on. CCIRC and CSEC continue to develop closer working relationships through practical measures, like developing operating procedures to ensure that each understands how and in what circumstances information should be shared. As the Auditor General's report notes, CCIRC now has a staff member embedded part-time with CSEC to strengthen working relationships.

Q: We're told CSEC can provide its unique expertise in collaboration with Public Safety Canada *beyond* federal networks, on networks of interest to the Government -- what are these networks and how are they chosen?

A: The Government can issue direction to CSEC and have them volunteer services and expertise. This is a flexible situation depending on the situations, threat, and environment. For instance, we could say that today this includes the Government's own systems, critical infrastructure, and essential defence and security networks.

Cyber Security Strategy and Investments in Cyber Security

Q: Public Safety Canada has committed to providing a publicly available action plan on the Cyber Security Strategy – when can we expect this?

A: Treasury Board submissions and businesses cases were developed for *Canada's Cyber Security Strategy*. These documents detailed a series of actions that departments and agencies were to undertake to deliver on the strategy.

We did not release these because many activities were about the protection of federal government systems - it would have been, and continues to be inappropriate to release that kind of sensitive information.

For the remaining items, we agreed with the Auditor General to release an interdepartmental, public action plan.

Q. Where was the $90 million from the Cyber Security Strategy allocated?

A. The initial funding of $90 million was allocated to 9 departments across the three pillars of the Strategy – securing Government systems, partnering to secure vital cyber systems outside the federal Government, and helping Canadians to be secure online. The lion's share of funding went to pillar one, securing Government systems.

This funding was allocated across 9 departments and agencies:

- Communications Security Establishment Canada
- Public Safety Canada
- Royal Canadian Mounted Police
- Treasury Board Secretariat
- Public Works and Government Services Canada
- Department of Justice
- Department of Foreign Affairs and International Trade
- Canadian Security Intelligence Service
- Defence Research and Development Canada

Q. Where was the $155 million from the October 17, 2012 announcement allocated?

A. The Government of Canada announced additional cyber security funding of $155 million. This will deliver improved cyber security across the Government of Canada information technology infrastructure, improved capability for Government to respond to and recover from incidents on its systems, and improved training for Government cyber security professionals.

These funds will also allow Public Safety's Canadian Cyber Incident Response Centre (CCIRC) to expand its capabilities and extend its operating hours to 15 hours a day, 7 days a week.

The $155 million is focused on pillars 1 and 2 of the Strategy, securing government systems and partnering to secure vital cyber systems outside the federal Government.

The funds are allocated across four agencies:

- Communications Security Establishment Canada
- Treasury Board Secretariat
- Shared Services Canada
- Public Safety Canada

If pressed for further breakdown:

We cannot comment on internal security measures, nor can we disclose the exact breakdown of the $155M in funding for security reasons.

Q: When was the $155M approved? Why the delay in announcing?

A: The announcement of the increase in the Canadian Cyber Incident Response Centre's hours of operation to 15 hours a day, 7 days a week with on call service 24 hours a day took effect on November 5th, 2012. It is the element of this funding commitment that will be publicly apparent. The other expenditures within this announcement consist of a wide range of system and program upgrades that are largely internal to government. The funding announcement was scheduled for October 2012 in order to ensure that the increase in CCIRC's operating hours was widely publicized and as a demonstration of the government's ongoing commitment to cyber security during Cyber Security Awareness Month.

Q. What funding has CCIRC received?

A. Of the $155 million, CCIRC has received $13.4 million over 5 years. This enabled CCIRC to extend its hours of full operation to 15 hours a day, 7 days a week. CCIRC remains accessible to its clients 24 hours a day, 7 days a week, through on-call support.

The first $90 million allocation did not provide new funding for CCIRC to extend its operational capability.

Q: How do Canada's cyber security efforts compare to those of our allies – US, UK, AUS?

A: Canada was among the first half-dozen or so countries to draft a national cyber security strategy, and many others have followed since we released ours in 2010.

Cyber security is a global issue and many countries face similar challenges: protecting government systems, responding to the need to protect essential systems and services outside of the government, and helping to protect individual citizens from cyber crime.

While the responses vary a bit according to the circumstances of each country, *Canada's Cyber Security Strategy* is very similar to the strategies of our key partners like the U.S., UK, and Australia.

We are in regular contact with each of these countries on cyber security, so it is no surprise that we are well aligned.

Frankly, given how rapidly technology is evolving and how quickly the threat environment can change, it is no easy feat to keep pace with cyber security development.

That said, I believe that our efforts compare extremely well with those of our allies and that they would agree that we are making tremendous progress

Q: If cyber security is so important, why has the Government not invested more?

A. I would say that funding has kept pace with the nature of national security threats to Canada.

Canada's Cyber Security Strategy made clear that the Government would constantly be re-evaluating where to direct resources based on the kinds of threats Canada is facing.

This has always been the case. If we look back to the early 2000's, resources were being directed to counter terrorism in the face of threats such as we saw on 9/11.

The cyber threat was comparatively smaller. In the intervening years, we've seen a tremendous growth in cyber systems and connectivity to the Internet, as well as growing abilities among criminals and adversaries to take advantage of digital networks. As the threat environment evolved, so did the Government's response and the resources devoted to cyber security.

Q: Does Canada have a plan to deal with a major cyber incident?

A: Canada has an all hazards approach for responding to and managing incidents affecting Canada's national security, public safety, and economic prosperity. Cyber incidents are managed as part of this robust system.

Federal, provincial and territorial governments work together under the National Emergency Response System to ensure responses to major incidents of any type.

The Federal Emergency Response Plan ensures a coordinated federal response to emergencies, including critical infrastructure disruptions, where an integrated Government of Canada response is required.

Initiatives such as *Canada's Cyber Security Strategy* and the *National Strategy and Action Plan for Critical Infrastructure* have strengthened links between governments and private sector partners to ensure that incident response is coordinated across the public and private sectors.

Public Safety Canada is working with cyber security partners across Canada to develop a national cyber incident management plan that will clarify roles and responsibilities for incident response, where appropriate.

Q: In 2011, this Government introduced the Government IT Shared Services initiative to transform the way government manages IT telecommunications. Would you not agree that this is yet another example of our government making our information technology infrastructure more secure?

A: The creation of Shared Services Canada is a fundamental change in how government IT services will be managed, and will put in place a new and more efficient IT infrastructure.

A key feature of building this new system is that security will be a consideration in the very design of the network. It is much more difficult and costly to integrate security retroactively.

Practically speaking, this means limiting the number of individual connections to the Internet, better monitoring of network traffic, and more efficient patching and updates to systems. Overall, Government of Canada systems will be better protected.

CCIRC Activities, Responsibility, and Structure

Q: What is CCIRC?

A: The Canadian Cyber Incident Response Centre (CCIRC) is Canada's computer emergency readiness team, focused on vital systems outside of federal government networks.

CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents. It does this by providing authoritative advice and support, and coordinating information sharing and incident response.

CCIRC is *the* primary contact point into the Government of Canada for domestic and international partners for cyber incidents

Q: What are CCIRC's annual resources and number of employees?

A: The Canadian Cyber Incident Response Centre has 30 employees and its total budget for Fiscal Year 2012-13 is almost $3.1 million.

Q: How is the CCIRC structured?

A: CCIRC is divided three sections:

- *Operations Section*: Incident handlers that assists partners in identifying, mitigating, and managing cyber security incidents.
- *Technical Analysis Section*: Operates CCIRC's lab and provides technical analysis to support incident response and management.
- The *Operational Analysis and Support Section*: Builds and manages relationships with partners, and produces analytical reports to support organizations' operational and security decision-making.

Q. What actions does CCIRC take in the event of a cyber incident?

A: CCIRC's role varies depending on the scale and on the severity of the incident.

CCIRC has Standard Operating Procedures (SOPs) for each category of cyber incidents, including unauthorized access, malicious code, denial-of-service (DoS) attacks, improper usage, and phishing and targeted emails.

When a cyber incident occurs, CCIRC provides mitigation advice to the affected organization and any other available information that may be of help in the particular situation. The goal is to help the affected organization recover quickly and with minimal impact to its operations.

In the event of a major cyber incident with potential national or international repercussions, CCIRC would also coordinate a comprehensive response between federal departments and with the affected organizations in order to contain the cyber incident, and recover from it as quickly as possible.

Q. Are there any examples of CCIRC's prevention, mitigation, and response to cyber incidents, or potential cyber incidents?

A. Yes. Two examples are detailed below: CCIRC's response to the DNS Changer Malware and its SCADA lab project.

DNS Changer

The Domain Name System (DNS) Changer Malware was a massive online fraud that infected approximately four million of computers globally with malicious software. The FBI conducted a two-year investigation that eventually led to the arrests, but the infected computers were still being directed to a false Domain Name server. CCIRC became involved as the Canadian coordination agency following an international meeting held to plan for remediation of this global issue.

This issue took months of work and outreach to mitigate. Approximately 100,000 Canadian computers were potentially infected. CCIRC sent notifications to system owners of infected hosts in the Canadian critical infrastructure sectors and provided mitigation advice to Canadian stakeholders. CCIRC also led work with Canadian Internet Service Providers and with the Canadian Internet Registration Authority to identify and notify the victims. This close partnership led to the launch of the www.dns-ok.ca website in February 2012, which allowed visitors to check if their computer was affected.

This outreach was extremely successful: CCIRC observed a significant increase of activity on its website, with close to 55,000 single visits (English and French combined) to its page detailing the DNS Changer. Overall, these efforts reduced the number of infected computers in Canada by approximately 90%.

SCADA Lab Project

The Canadian Cyber Incident Response Centre (CCIRC), in partnership with Defence Research and Development Canada (DRDC) and other federal partners, has undertaken a research project to enhance what are called "supervisory control and data acquisition" or SCADA networks. These SCADA networks are computer controlled systems that monitor and control industrial processes, and are used by the private sector, academia as well as Canadian governments. The project we've undertaken is a collaborative effort combining the federal government's sophisticated equipment and technical expertise with the actual SCADA devices being provided by the private sector. Essentially the government is filling a gap by coordinating research with a long-term impact that no private sector user of these systems could undertake on their own.

The project has already produced results. CCIRC has published the Industrial Control Systems Security Best Practice Guide for use by both government and the private sector. This guide aims to help those involved in the design and operation of industrial control systems to understand the critical issues involved in securing these systems. It provides the reader with an overview of the challenges and threats facing owners and operators of industrial facilities and presents data from the study of real industrial control system security incidents. This guide has been distributed to key stakeholders in both official languages.

This is just one example of how CCIRC is continuing to build relationships with federal, provincial, and private sector organizations on a practical issue that is providing real value and is strengthening our collective security. We're looking to continue the project with DRDC to address another issue facing the private sector, namely the use of wireless technologies in conjunction with the industrial control systems being used today.

Q: Could you please outline the efforts Public Safety has made to date with respect to publicizing the existence of the Canadian Cyber Incident Response Centre (CCIRC)?

A: CCIRC's services and products are well known to IT professionals generally and across critical infrastructure sectors in particular. CCIRC's work has been the subject of briefs to a several critical infrastructure networks, as well as to the cross-sector network. Beyond this, CCIRC runs workshops across the country on specialized industrial control systems which have drawn attention from critical infrastructure operators. CCIRC is regularly asked to contribute or speak at IT security conferences across the country. Of course, CCIRC has a website and freely available products which gain a great deal of attention, such as the CCIRC information notes on major IT security issues like the DNS Changer malware.

CCIRC Hours of operation

Q: What are CCIRC's hours of operation?

A: CCIRC began their longer hours of operations, 15 hours per day, 7 days per week (15/7), on November 5, 2012.

This allows CCIRC to provide coverage to its partners during core business hours across the country.

CCIRC's hours of operation are now from 6:00 a.m. to 9:00 p.m., seven days a week. Between 9:00 p.m. and 6:00 a.m., a Cyber Duty Officer (CDO) is on standby to provide emergency incident response.

CCIRC Clients and Partners

Q: Who are CCIRC's partners?

A: CCIRC works with trusted partners including Canada's security and intelligence community, international allies, technology and security vendors, and experts within the global cyber security community. CCIRC's partners include municipal, provincial and territorial government, and public and private sector organizations.

Q: How does private sector report incidents to CCIRC?

A: Private sector partners can report to CCIRC in a number of ways and all have detailed contact information. These include e-mail, telephone (both local and via a 1-800 number) and using the CCIRC Community Portal.

Q: How many clients does CCIRC have?

A: In total, CCIRC has over 1400 points of contact. Of those, approximately 240 of them receive our products directly.

Q: What criteria are in place to be considered a CCIRC partner? Is there a vetting process?

A: A partner would be someone who is a technical point of contact that is part of a Canadian critical infrastructure sector.

Before adding them to their list of trusted partners, CCIRC performs a validation of this potential point of contact, mostly through open source research.

CCIRC also validates this point of contact's email address, ensuring it belongs to the right organization (and is hosted on the appropriate network), in addition to sometimes validating it through other already established contacts.

Q: How does CCIRC cooperate internationally?

A: CCIRC collaborates with a number of international partners.

A key partnership is with our counterpart in the United States' Department of Homeland Security, US-CERT.

CCIRC and US-CERT work together on a daily basis to share cyber threat and mitigation information, reduce cyber risks in both countries, and cooperatively develop cyber awareness products.

CCIRC also works on a near daily basis with our traditional allies in Australia, the United Kingdom, and New Zealand.

CCIRC is a member of the International Watch and Warning Network (IWWN) consisting of the five eyes countries, Japan and nine other European states.

CCIRC is a member of the Forum of Incident Response and Security Teams (FIRST), a group that consists of over 275 national and private sector computer security incident response teams.

Lastly, CCIRC works on an incident-by-incident basis with counterparts in countries across the globe to mitigate cyber risk to Canada.

CCIRC Products and Services

Q: Who receives CCIRC's products?

A: CCIRC releases its products through a distribution list made up of its trusted critical infrastructure partners, including all levels of governments, international partners, academe, and the private sector.

Q: Do private citizens or small businesses receive CCIRC products?

A: Private citizens and small businesses do not receive CCIRC products directly, but do have access to a number of them through CCIRC's website. Alerts, advisories, information notes and technical reports are posted online.

On occasion, due to the sensitive nature of the content, CCIRC will release one of these products directly to its critical infrastructure partners, and will not post it to its public website.

Q: What services does CCIRC provide?

A: CCIRC provides its partners with a number of services, including:

- Advising on how to detect and mitigate a cyber incident
- Coordinating the disclosure of cyber vulnerabilities
- Notifying victims of cyber incidents
- Coordinating requests to remove malicious code and/or content
- Analysing potentially malicious code

CCIRC also hosts and moderates a community portal for its partners which includes a repository of CCIRC's products, discussion groups, and allows for incident and malware submissions.

Attacks on and Threats to Government Systems

Q: What has the Government of Canada done to protect federal systems from cyber attacks? Is the Government of Canada ready for cyber attacks?

A: Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. We take this responsibility seriously. Enhanced security of government systems will better protect the private information of Canadians and Canadian businesses that are held there.

The Government of Canada understands that the cyber threats we face are evolving, and so strengthening cyber security is an ongoing journey – there is no end point.

Since the release of *Canada's Cyber Security Strategy* in 2010, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents:

- In 2011, we introduced the Government IT Shared Services initiative to transform the way government manages IT telecommunications, desktop computer services, data centres, IT security services and Internet access points. By consolidating our information technology infrastructure under Shared Services Canada, we are making our information technology infrastructure more secure.

- We have improved how we manage cyber incident response coordination and have clarified the roles and mandates for the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre to improve Canada's ability to identify, prevent and mitigate cyber security incidents.

The $155M in cyber security funding announced October 17, 2012, further secures government systems that deliver services to all Canadians and complements additional efforts under *Canada's Cyber Security Strategy* to protect Canadians from cyber threats.

Q: Can Canadians trust the government with their personal information?

A: Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. We take this responsibility seriously.

Since the release of the *Cyber Security Strategy*, the Government of Canada has been strengthening Canada's capacity to mitigate, detect and respond to cyber incidents.

In 2011, we introduced the Government IT Shared Services initiative to transform the way government manages IT telecommunications, desktop computer services, data centres, IT security services and Internet access points.

Enhanced security of government systems will better protect the private information of Canadians and Canadian businesses.

Q: How safe is Public Safety Canada's own network?

A: Public Safety Canada's network is accredited in accordance with Government of Canada policy and directives.

We have robust security safeguards based on these directives and industry best practices. We also work with Shared Services Canada and CSEC to continually monitor threats to our networks and take action to address any risks.

Q: What is CSEC doing to ensure that it is providing information in a timely fashion to partners, e.g., CCIRC, SSC, etc

A: CSEC routinely shares cyber threat information and mitigation advice with CCIRC at Public Safety.

CCIRC passes this information and advice on to other levels of government and the private sector.

Since 2011, CSEC has had standard operating procedures for sharing specific incident information and mitigation advice in a timely and secure manner to government IT security partners.

In addition, a CCIRC employee has also been integrated into CSEC's *Government of Canada Cyber Threat Evaluation Centre* (GC-CTEC) with full access to threat data.

Q: What is the biggest kind of threat to Canada - espionage, cyber crime, terrorism?

A. Canada faces a variety of threats directed towards different parts of our society.

Individual Canadians can be targets for cyber crime like identity theft or online fraud.

The Government is the target of state sponsored espionage.

The private sector is being targeted with corporate espionage, with the attendant the loss of trade secrets or economically valuable information.

Cyber terrorism is not something we have seen much of yet, but it is the likely next phase of cyber threats.

All these threats affect our security and prosperity. It would be impossible to say that one is more important than another.

In many ways the biggest challenge is that all these threats are inter-related and they are all constantly evolving.

The approach in *Canada's Cyber Security Strategy* is to establish an overall approach for the Government to coordinate its response to this complex environment and deal appropriately with all threats to our collective security.

Q: What kinds of attack are we seeing today?

A: Attacks today generally fall into four categories: denial of service, persistent attacks, website defacements, and attacks targeting the individual for profit.

Denial of Service (DOS or DDOS): This is an attempt to make a machine or network resource unavailable to its intended users. A common method is to

overwhelm the target machine with external communications requests so it cannot respond to legitimate traffic - essentially, a website or service is taken offline. Hundreds or thousands of individual computers are used to make these requests, and often all those computers have actually been taken over by a virus and are being remotely commanded to take part in the attack. These kind of threats need a quick response from CCIRC. Rapid response for such attacks is critical given that an entire business service could be stopped.

Persistent Attack: Sometimes called an "Advanced Persistent Threat", a persistent attack is a virus that sits on a computer or network for an extended time in order to allow an attacker ongoing access to a system. Often these are used for the purpose of espionage, but they can also be used to damage or disrupt a system: for instance, the Stuxnet virus was a persistent attack on an industrial control system. These attacks are designed to go unnoticed and so can be difficult to detect. The level of effort to eradicate this threat can be quite high requiring time and in-depth assessment of how long the attack has been active and what has been compromised.

Web Defacement: Attacks on a website that changes the visual appearance of the site. This is often the work of hackers who break into a web server and replace the hosted website with their own malicious one. This type of attack is usually used by politically motivated "hacktivists" to spread their messages.

Attacks for profit: Attacks for profit covers a range of activities typically used by cyber criminals: fraudulent emails, fake websites, viruses that log keystrokes. What they all have in common is the motive for quick profit, usually by deceiving an individual into giving up critical information such as bank details. Attacks for profit are by far the most pervasive threat on the Internet as they are relatively easy to undertake and offer quick gain for criminals. CCIRC consistently performs assessments of the tools and methods used by cyber criminals and provides advisories and warnings as necessary, or even direct mitigation help in large-scale cases such as the DNS Changer malware.

Two examples are:
Ransomware: Malware that restricts access to the computer system and demands a ransom be paid in order for that restriction to be removed.

Phishing Attacks: Attacks that attempt to acquire information such as usernames and credit card details by pretending to be a trustworthy source. Phishing emails contain links to websites that have been infected with malware.

On foreign threats and foreign investment

Q: Is China a cyber threat? What other countries are you concerned about?

A: The Government of Canada works closely with our allies on any threats to our security.

If there is a national security interest that would require the disclosure of specific threats, names or companies, that would be done in due course.*

At present we will not comment on specific or potential threats, but we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

**(From the Minister's press conference Oct 17, 2012.)*

Q: How do you respond to the US House Intelligence report, or to the ongoing warnings and media reports about foreign and specifically Chinese threats?

A: While we do not comment on specific or potential threats, we can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

The Government of Canada supports a prosperous and competitive telecommunications sector in Canada – however, a thriving telecommunications industry must be a safe and secure one.

That is why the Government of Canada is working to ensure that any risks to Canada's telecommunications sector are identified and addressed.

Q: Why doesn't Canada have its own agency to check the equipment that Canadian companies and public sector departments may be buying? *(asked at Oct 17 press conference)***?**

A: There is no stand-alone Government agency, either in Canada or the United States, to review all telecommunications equipment or software. There are third-party private sector firms that offer these services.
The Government of Canada works with Canadian telecommunications carriers, the provinces and territories, the critical infrastructure sectors, and with vendors to assess and mitigate possible risks to Canada's strategic telecommunications infrastructure and vital systems.

Informed by these assessments, private sector Canadian companies will demand the security assurances that they feel are warranted for the purchase of any equipment or software.

Q: Why doesn't Canada simply take the same measures as the US and Australia to prevent suspect companies from taking part in the Canadian market *(asked at Oct 17 press conference)*?

A: While we certainly consider what our allies are doing, we will make our own decisions, in the best interests of Canada and Canadians (from the Minister's Oct 17 press conference).

Q: Does the Investment Canada Act have strong enough security provisions to protect Canada's infrastructure against potential cyber-threats (asked at Oct 17 press conference)?

A: This Government is constantly working to strengthen Canada's cyber security. While we have a robust system in place, no legislative or technological framework alone can last indefinitely given the rapidly evolving nature of technology.

That said, we look at all possibilities to strengthen our security mechanisms to continue enhancing the safety and security of Canadians.

Q: What is the National Security Exception and why was it invoked for federal procurement?

A: The National Security Exception allows Canada to exclude a procurement from some or all of the obligations of the relevant trade agreements, where Canada considers it necessary to do so in order to protect its national security interests.

The National Security Exception has been invoked under Canada's domestic and international trade agreements in connection with procurements for Shared Services Canada related to email, network, telecommunications and data centre systems, infrastructure and services.

This is part of a Government of Canada strategy to create a secure, centralized communications infrastructure.

Critical Infrastructure Progress, Partnerships and Sector Networks

Q: What is Canada's approach to critical infrastructure protection, and why have there been delays?

A: Canada's critical infrastructure, such as the electricity grid, is interconnected and geographically dispersed throughout North American, from coast to coast and across the border.

The majority of Canada's critical infrastructure is owned by the private sector, and jurisdictional responsibility for our critical infrastructure sectors is shared among federal and provincial/territorial governments.

To move forward with an integrated approach among this large stakeholder community, in 2010, Public Safety Canada launched the National Strategy and Action Plan for Critical Infrastructure.

This strategy is our national game plan to ensure that we can respond and recover swiftly when disruptions occur. In particular, the strategy calls for the critical infrastructure sectors to assess risks, develop plans to address risks, and conduct exercises to ensure that our plans will be effective during a disruption.

Q: What is Public Safety Canada doing to address the Auditor General's recommendation on critical infrastructure?

A: Public Safety Canada has launched a review of the membership of the sector networks, in consultation with other federal departments and agencies. Based on these consultations, and in response to the Auditor General's recommendation, Public Safety Canada will provide guidance to lead federal departments and agencies on appropriate coverage for the sector networks by December 2013.

In follow-up to the Auditor General's report, we have already achieved significant progress toward strengthening the sector networks. Most recently, we have finalized a *Critical Infrastructure Planning Guide* and developed tools and guidance to support information sharing and risk management activities among the critical infrastructure community.

Q: What is the status of the critical infrastructure sector networks?

A: The OAG has acknowledged that we have longstanding partnerships with the private sector.

Since the 2010 announcement of the *National Strategy and Action Plan for Critical Infrastructure*, the Government has formalized our public-private sector partnerships with the creation of networks for each critical infrastructure sector. Each of these sector networks are up and running, and are undertaking risk management activities.

Public Safety Canada also established the National Cross Sector Forum, which brings together national leaders from each of the critical infrastructure sectors to set priorities and identify action items.

This National Cross Sector Forum meets annually and has been briefed on cyber threats during each meeting.

Cyber threat briefings have also been delivered to critical infrastructure sectors, including water, information and communications technology, transportation, safety, government, energy and finance.

In addition, Public Safety Canada and the Canadian Security Intelligence Service hosted a multi-sector meeting on cyber security in April 2012 to discuss cyber security. The next multi-sector network meeting will be in April 2013, and will again feature a cyber security briefing.

Public Safety Canada and the Royal Canadian Mounted Police have also co-hosted a series of Industrial Control Systems Cyber Security Workshops for critical infrastructure stakeholders across the country.

Q: How do the sector networks work? Are they all led by Government departments? Is there any way to ensure proper leadership and participation in the networks?

A: The purpose of the sector networks is to bring together the public-private sector stakeholders within each sector to share information and undertake risk management activities, such as risk assessments and exercises.

Each sector network has a lead federal department. For example, Finance Canada is responsible for the Finance Sector Network.

Public Safety Canada works closely with the lead federal departments to support partnership-building through the sector networks, and to encourage participation of stakeholders in risk management activities.

By delivering security briefings, doing site assessments, and conducting exercises, we are demonstrating value to the private sector for participation in the sector networks.

Q: Can you please speak to the positive steps the National Cross Sector forum continues to take in regard to risk management activities with partners across Canada?

A: Public Safety Canada hosted the inaugural meeting of the National Cross Sector Forum in December 2010, bringing together representatives from each of the critical infrastructure sectors. This Forum now meets annually to review progress and set priorities for collective action.

Under the National Cross Sector Forum, we have moved forward with a national approach to critical infrastructure risk management, including publication of a Risk Management Guide for Critical Infrastructure Sectors, and creation of a catalogue of risk assessment methodologies.

We are actively conducting site assessments of critical infrastructure facilities, and we have launched a project with the private sector to model interdependencies across the country. This project will tell us, for example, what the cascading impacts of a power disruption would be across sectors and jurisdictions.

The Office of the Auditor General (OAG) recognized a number of the positive steps that we have taken. The OAG pointed out that we have established a multi-sector network in April 2012, which brought together sector networks to discuss cyber security.

We also launched the Critical Infrastructure Gateway, which is a web-based portal to support active dialogue among critical infrastructure partners on best practices and risks and threats, including cyber threats.

In addition, we established the Critical Infrastructure Information Sharing Framework, which sets out processes to support information sharing among the critical infrastructure community and protect this information from inappropriate disclosure.

Q: In the AG's report, you stated that the Government has made progress in securing its systems and in building partnerships with the private sector. Can you elaborate in your view how we have done so?

A: Foremost, we are proud of our effective, longstanding partnerships with critical infrastructure sectors, including energy, finance, and transportation – something the OAG has acknowledged.

Since the 2010 announcement of the *National Strategy and Action Plan for Critical Infrastructure*, the Government has formalized these partnerships with the creation of networks for each critical infrastructure sector, and the establishment of the National Cross Sector Forum to review progress and set priorities.

The report also highlights several recent accomplishments in the area of critical infrastructure protection.

This includes the creation of a multi-sector network to discuss cyber security and share best practices, as well as the establishment of a web-based portal to support ongoing dialogue with our critical infrastructure partners.

We have also completed a Critical Infrastructure Information Sharing Framework to facilitate information exchange among stakeholders and protect this information from inappropriate disclosure. We are actively doing site assessments of critical infrastructure facilities, developing risk management tools and best practices, and conducting exercises to ensure that we will be ready when disruptions occur.

Q: Would it be helpful for this committee to undertake a study on critical infrastructure in Canada?

A: Critical infrastructure resilience is a shared responsibility among all levels of government and private sector owners and operators.

Given the integrated nature of critical infrastructure across jurisdictions, the scope of the study would need to involve significant participation of provinces and territories, which have extensive regulatory responsibilities for certain critical infrastructure sectors, such as health and water.

Recognizing that the private sector owns the majority of critical infrastructure in Canada, owners and operators would also need to be engaged.

Q: Jim Burpee, President and CEO of the Canadian Electricity Association, stated that: "*Through the National Strategy and Action Plan for Critical Infrastructure launched two years ago, all of the players are engaged and working together to address Canada's cyber security challengers.*" Can you describe some of the benefits of having a plan in place to pull together stakeholders so everyone is moving forward in the same direction?

A: The majority of our critical infrastructure is owned and operated by the private sector, and jurisdictional responsibility is shared among all levels of government. Our critical infrastructure is also interconnected – our first responders depend on secure transportation, which depends on secure communications technology, which in turn depends on reliable electricity.

The National Strategy and Action Plan for Critical Infrastructure is Canada's game plan for bringing the community together, including the private sector and all levels of government, to ensure that we can respond and recover quickly when disruptions occur.

This partnership model is consistent with international best practices, including the critical infrastructure programs in the United States and the United Kingdom, and Canada is leading the way through the National Cross Sector Forum and sector networks.

This model also recognizes that industry has the expertise and information that governments need to develop comprehensive plans to deal with the evolving threat environment. In turn, we are committed to bringing value to the partnership by providing timely and accurate information, and ensuring that industry is engaged as early as possible in risk management activities.

This approach leads to tangible benefits for all parties, including: greater understanding of the threat environment, improved ability to innovate and develop countermeasures, and swift response and recovery when disruptions occur.

Ultimately, these partnerships are helping to build a safer, more resilient Canada, that is attractive for investment, stimulates the economy, retains business, and improves the quality of life for Canadians.

Q: We know that Canada's critical infrastructure faces a diverse and evolving risk environment, including terrorism, cyber-attacks, pandemics, and natural disasters. Do you agree that the National Strategy and Action Plan for Critical Infrastructure launched in 2010 is committed to strengthening our ability to protect vital assets and systems such as electricity grids, transportation networks, financial systems and telecommunications, as well as our collective readiness to respond and recover from emergencies, attacks and disasters?

A: Agreed. The *National Strategy and Action Plan for Critical Infrastructure* recognizes that the key to protecting our critical assets and systems is collective action and an integrated approach among all levels of government and the private sector.

Our critical infrastructure strategy represents a shared, national commitment to building partnerships, sharing information, and undertaking risk management actions to help ensure that we can collectively respond and recover swiftly when disruptions occur.

Ten sector networks (finance, energy, transportation, information and communications technology, health, water, food, safety, government and manufacturing) have been established to move forward with identifying risks, developing plans to address risks, and validating these plans through exercises.

At the national level, the National Cross Sector Forum is co-chaired by the Deputy Minister of Public Safety and his provincial counterpart, and meets annually with

sector network representatives to discuss issues that cut across sectors, such as cyber security, and cross border collaboration.

Canada's approach to critical infrastructure has a number of competitive advantages. For example, our partnerships with the private sector are helping us to keep pace with the evolving threat environment and are helping us to innovate and adapt robust risk management practices.

Canada is also leading the global effort to protect critical infrastructure, including chairing the NATO Working Group on Critical Infrastructure and developing a Global Infrastructure Security Toolkit.

Q: What Critical Infrastructure sector networks remain to be established?

A: All of our critical infrastructure sector networks have been established.

Each of the sector networks is up and running, they have all held meetings, and are actively undertaking risk management efforts. These efforts include site assessments, standards development, and exercises.

The audit specifically notes that the sector networks are valuable forums for information sharing and collaboration on risk management, but that these sector networks are at various stages of maturity.

In addition, the audit notes that coverage of these sector networks should be expanded to include representatives from all industry groups that are considered critical infrastructure. In this context, the audit recommends that Public Safety Canada take action to ensure that the sector networks are fully established and operating as intended.

Q: What is your prioritization strategy for the establishment of these networks and when you expect to have completed this effort?

A: In keeping with the audit's recommendation, the Department will continue to work with lead federal departments and agencies to strengthen the sector networks and expand their coverage.

Recognizing that each sector is unique and that representation is not expected to be uniform across each of the critical infrastructure sectors, Public Safety Canada will provide guidance to lead federal departments and agencies on appropriate coverage for the sector networks by December 2013.

Q: What have been the challenges you have encountered along the way to establishing these networks?

A: The audit notes that most of Canada's critical infrastructure is owned by the private sector or is managed through other levels of government.

This mix of ownership and jurisdictions creates challenges in leading and coordinating stakeholders' efforts to protect critical infrastructure.

The audit also notes that critical infrastructure is geographically dispersed, throughout North America, spanning both Canada and the United Sates.

While we have achieved significant progress in our partnerships with the private sector, other levels of government and international allies, we also recognize that the collective attention and efforts of the entire critical infrastructure community will be required to protect Canada's vital assets and systems.

Q: Could you please describe the nature of the information Public Safety Canada is currently disseminating to the various critical infrastructure sectors and the frequency of this dissemination?

A: Public Safety Canada shares information with critical infrastructure sectors on a variety of topics, including pandemic planning, earthquake scenarios, natural disasters, national security threats, and cyber security. The information that we share covers the spectrum from best practices, suggested counter measures, planning guides, tools and templates, and risk and threat information.

We share information through security briefings to sector networks, and also through our Critical Infrastructure Gateway, which is our web-based portal for information sharing. The frequency of information dissemination varies, depending on when best practices are developed, when an incident happens, and when meetings occur. We are continuing to make efforts to ensure that we maintain ongoing dialogue with our critical infrastructure partners.

Q: What percentage of the time would you say the information you provide enables operators of critical infrastructure to prevent rather than simply react to the compromise of their systems

A: A significant amount of our information is directed toward identifying and addressing risks before disruptions occur. Examples include our risk management guide, risk assessment methodologies, and critical infrastructure planning guide.

Q: How do the current efforts you are making contribute to the ability of critical infrastructure operators to prevent compromise of their systems?

A: Our partnership model, based on the sector networks and the National Cross Sector Forum, ensures that we are constantly receiving feedback from critical infrastructure owners and operators. This feedback helps us to ensure that our efforts are meeting their needs and helping them to protect their vital assets and systems.

Q: In February 2011, Treasury Board Secretariat and Department of Finance computer networks were compromised in a cyber attack. Could you please identify the lead department responsible for cyber security in the finance sector?

A: Finance Canada is the lead federal department for the finance sector.

Q: Can you describe the current status of Public Safety engagement of and information sharing with this sector?

A: Public Safety Canada, in partnership with Finance Canada, is actively working with the finance sector. Most recently, for example, Public Safety Canada contributed geospatial analysis of critical infrastructure toward the finance sector's risk analysis activity that is presently underway.

On the STOP.THINK.CONNECT Partnership

Q: What is STOP.THINK.CONNECT?

A: STOP. THINK. CONNECT.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Anti-Phishing Working Group and National Cyber Security Alliance lead the effort to find a unified online safety message that could be adopted across public and private sectors.

Q: What are the benefits of this partnership?

A: This partnership will facilitate the alignment of both public awareness campaigns and provide citizens with consistent, reliable and important advice and tools to help increase personal online security. This partnership underscores our joint collaborative efforts and commitment to cyber security.

Q: What will Canadians see as a result of this partnership?

A: This new partnership builds upon the success of both public awareness campaigns by allowing us to align our efforts to reach a wider audience with consistent, reliable and important advice and tools to help increase personal online security.

Cyber security is an international issue, and we recognize that we cannot address cyber threats in isolation. Shared threats require shared solutions.

Q: Will GetCyberSafe change as a result of this partnership?

A: *Get Cyber Safe* will retain its branding. It will be enhanced over time with key messages and tools that are available through the partnership. GetCyberSafe is a key component of Canada's cyber security strategy, and is Canada's national campaign. A partnership with STOP.THINK.CONNECT compliments our efforts, leverages new tools and partners, and supplements the tools we develop to help broaden the reach of important messaging.

Q: Is there any funding attached to this partnership?

A: No.

On the U.S. Executive Order on Critical Infrastructure Cybersecurity

Q: The U.S. president recently signed a high-profile executive order to strengthen the cyber security of critical infrastructure. Has Canada undertaken any similar measures?

A: We work closely with our international allies, and the United States in particular, to secure our shared interests in cyberspace. We are aware of the recent announcements in the United States and are reviewing them. While we certainly consider what our allies are doing, we will make our own decisions, in the best interests of Canada and Canadians (from the Minister's Oct 17 press conference).

Q: The order calls for the development of baseline cyber security standards, procedures, and performance measurement metrics that critical infrastructure operators could voluntarily follow. Has Canada undertaken any similar measures?

A: Canada has a number of measures to strengthen the cyber security of critical infrastructure. CCIRC shares unclassified cyber threat information with Critical Infrastructure and though the National Cross Sector Forum, we engage with critical infrastructure owners and operators about cyber risks they face.

Q: The order expands efforts to provide classified cyber threat information to private sector entities. Has Canada undertaken any similar measures?

A: Public Safety Canada shares information with critical infrastructure sectors on a variety of topics, including pandemic planning, earthquake scenarios, natural disasters, national security threats, and cyber security. The information that we share covers the spectrum from best practices, suggested counter measures, planning guides, tools and templates, and risk and threat information. We share information through security briefings to sector networks, and also through our Critical Infrastructure Gateway, which is our web-based portal for information sharing. The frequency of information dissemination varies, depending on when best practices are developed, when an incident happens, and when meetings occur. We are continuing to make efforts to ensure that we maintain ongoing dialogue with our critical infrastructure partners. Note: this is the same answer from page 37 in the Q&A doc to a similar question.

Q: What is Canada doing about the recent DDoS activity targeting the financial sector?

A: The Government's approach to implementing *Canada's Cyber Security Strategy* is to use sector networks with critical infrastructure owners and operators to build the partnerships needed to secure systems. Critical infrastructure sector networks are forums for discussions and information exchanges among sector-specific industry stakeholders and governments. The Financial Sector network has proven to be a valuable forum for exchanging needed information to protect critical infrastructure, including facilitating discussions surrounding more recent DDoS activities.

Q: What is your engagement strategy to ensure Canada is providing full coverage to all organizations within the critical infrastructure community?

A: The Government's approach to implementing *Canada's Cyber Security Strategy* is to use sector networks with critical infrastructure owners and operators to build the partnerships needed to secure systems. Critical infrastructure sector networks are forums for discussions and information exchanges among sector-specific industry stakeholders and governments. Many of these Critical Infrastructure sector networks have proven to be valuable forums for exchanging needed information to protect critical infrastructure.

Q: What is the Government doing to increase visibility and awareness of CCIRC's services among the critical infrastructure community?

A: As part of CCIRC's goal to increase situational awareness among organizations and partners, CCIRC is involved with various speaking engagements and conferences with members of the critical infrastructure community. CCIRC has also recently developed and released a suite of professional products such as bi-weekly and quarterly operational summaries. These documents provide decision makers among the critical infrastructure community with relevant cyber information including products and services provided by CCIRC, noteworthy incidents, and trends. In addition, through the handling of daily cyber incidents, CCIRC will often reach out to partners and organizations to solicit useful information and build relationships. CCIRC continues to expand its contact list of organization members who receive our products and services. This will serve as one of CCIRC's main objectives in the upcoming year.

Q: What type of feedback is CCIRC receiving from its partners regarding its products and services? How often does it receive this feedback? How does this feedback contribute to the improvement of CCIRC's products and services?

A: CCIRC will often receive feedback from partners directly related to its products and services through emails and phone calls. CCIRC proactively chairs weekly meetings with its public and private sectors partners and these meetings serve as a proper forum for soliciting feedback related to CCIRC's products. All follow-up questions or concerns that arise from the distribution of CCIRC's products get tracked and directly feed into the improvement of CCIRC's products and services. Through the continual process of reviewing and updating its Standard Operating Procedures (SOP), CCIRC ensures that these improvements are followed by all incident handlers.

Q: Does CCIRC have standard operating procedures (SOP)? Are these SOPs reviewed and vetted to ensure CCIRC's products and services meet the needs of their partners.

A: To carry out CCIRC's mandate to prepare for, prevent and mitigate, respond to, and recover from cyber events affecting Canada's critical infrastructure sectors, approximately 70 SOPs have been created to fully define CCIRC's steps in both providing services to its clients, and producing awareness products. These SOPs are strictly followed by the CCIRC team and are available to all staff through CCIRC's internal portal. The SOPs are continually updated and reviewed to ensure accuracy and effectiveness.

Q: What measures and metrics are in place to ensure that tax payer resources being spent on cyber security are achieving results?

A: Under Public Safety Canada's leadership, all key departments and agencies have completed a horizontal performance measurement strategy which has been submitted to the Treasury Board Secretariat. That strategy will help the Government to measure and report on the progress made against commitments in the action plan. A component of the performance measurement strategy is the identification of key performance indicators for each activity under Canada's Cyber Security Strategy. Departments are now collecting performance data and will be reporting on the progress achieved by the end of the calendar year. Public Safety Canada is leading the development of a summative evaluation of *Canada's Cyber Security Strategy*, which will be completed in 2015.

On the Mandiant report on cyber espionage

Q: How is the Government of Canada responding to the findings contained within the recent report from the U.S. cyber security firm Mandiant?

A: While we are aware of the Mandiant report, we do not comment on specific or potential threats. We can say that the Government of Canada, advised by its law enforcement and security agencies, remains vigilant in monitoring any potential threats and has robust measures in place to address them.

Q: What is the Government of Canada doing to protect Canada's critical infrastructure from cyber espionage?

A: The Government of Canada is committed to protecting Canada's cyber security. Cyber threats evolve rapidly, and it is essential that the Government of Canada and owners and operators of Canada's vital cyber systems work together to protect those systems and the Canadians who depend upon them. The protection of Canada's cyber security is a shared responsibility.

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents. Its focus is the protection of vital systems outside of the federal government, including critical infrastructure, against cyber incidents.

CCIRC works with national and international counterparts to collect, analyze, and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals, critical infrastructure sectors and other related industries.

Product	Description
Cyber Flash	Flashes are time sensitive and describe an immediate or active security issue. They are used to raise awareness of recently identified cyber threats that may impact F/P/T/CI assets. Flashes are not publicly posted and are ideal for raising awareness and providing detection and mitigation advice, while avoiding unwanted publicity. Examples include: (1) Warnings of imminent threats against F/P/T/CI networks; (2) zero day vulnerability alerts; and (3) advance notification of important patches.
Daily Situation Report	This brief is a daily situation report, which includes: (1) events and actives that are currently being actionned by CCIRC; (2) publicly reported vulnerabilities and threats; (3) noteworthy news items; (4) information from international partners; and (5) a summary of CCIRC products. All events and activities are sanitized (i.e. made anonymous).
Weekly Technical Report	The weekly technical report is geared for the technical F/P/T/CI community. It is a summary of the past week's daily reports along with more technical information.
Information Note	Information notes are used to draw attention to: (1) changes in CCIRC policy or procedures; and (2) a significant cyber issue. Examples include: (1) notifications of new security tools; and (2) upcoming CCIRC events.
Technical Report	Technical reports explain the technical and operational details of a cyber event impacting F/P/T/CI networks.
Advisory	Advisories communicate security update information regarding vulnerable software. These vulnerabilities could possibly impact F/P/T/CI assets. As such, advisories may contain information describing the vulnerabilities and informing that updated software has now been made available by the vendor to correct these deficiencies.
Alert	An alert offers critical, time sensitive information and mitigation advice to trusted partners, and normally, the public. Alerts are used in circumstances where a vulnerability is being actively exploited on the Internet and no patch is available.
Statistics Report	This weekly statistics report provides an overview of notable cyber events, released CCIRC products, and details the activity on the CCIRC website in the past week.
Cyber Operational Summary	This bi-weekly report provides partners with cyber information that can support operational and security decision-making. It aims to raise awareness of Canadian cyber incidents seen by CCIRC, provides background information on CCIRC's technical products, and summarizes recently released Internet threat reports, and noteworthy news items.
Quarterly Operational Summary	This quarterly report provides partners with cyber information that can support operational and security decision-making in their organizations. It aims to raise awareness of Canadian cyber incidents seen by CCIRC, provide background information on CCIRC's technical products, and trend analysis.
Annual Report*	This annual status report will provide CCIRC's partners an overview of Canadian cyber incidents seen by CCIRC, and will also include background information on CCIRC's technical products, and trend analysis. **This report is in development.*

TALKING POINTS TO ADDRESS THE AUDITOR GENERAL OBSERVATIONS

OAG Observation	Key Messages
Between 2001 and 2009, the government made limited progress in its efforts to lead and coordinate the protection of Canada's critical infrastructure from cyber threats as these threats were rapidly evolving. Reference: Page 2	• The Auditor General's report recognizes the positive steps that Public Safety Canada has taken in recent years, and acknowledges the progress made since Public Safety Canada launched the cyber security and critical infrastructure strategies in 2010. • We have, in fact, made significant progress, particularly in recent years, in the midst of an evolving threat environment. • If we look back to the early 2000's, resources were being directed to counter terrorism in the face of threats such as we saw on 9/11. • The cyber threat was comparatively smaller. In the intervening years, we've seen a tremendous growth in cyber systems and connectivity to the Internet, as well as growing abilities among criminals and adversaries to take advantage of digital networks. As the threat environment evolved, so did the Government's response and the resources devoted to cyber security.
Seven years after the Canadian Cyber Incident Response Centre (CCIRC) was created to collect, analyze, and share cyber threat information among federal departments, provincial and territorial governments, and the private sector, many stakeholders are still unclear about the Centre's role and mandate. Reference: Page 2	• As Canada's computer security incident response team for non-government systems, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents. • CCIRC provides authoritative advice and support, and coordinates information sharing and incident response, in conjunction with its domestic and international partners to address high-level cyber security concerns. • CCIRC's services and products are well known to IT professionals and across critical infrastructure sectors. CCIRC provides regular briefings to critical infrastructure networks. In addition, CCIRC runs workshops across the country on specialized industrial control systems which have drawn attention from critical infrastructure operators, and CCIRC is regularly asked to contribute or speak at IT security conferences across the country. • Finally, CCIRC has a website and offers freely available products which gain a great deal of attention, such as the CCIRC information notes on major IT security issues.

OAG Observation	Key Messages
The Canadian Cyber Incident Response Centre (CCIRC) is still not operating on a 24-hour-a-day, 7-day-a-week basis, as originally intended. Reference: Page 2	• CCIRC has expanded its operational hours to 15 hours a day, seven days a week onsite coverage. This expanded capacity allows CCIRC to cover the full business operating hours of clients from coast-to-coast. • At all times, experts from CCIRC are available and on call 24 hours a day, seven days a week, to deal with emergency situations. This on-call system is similar to cyber incident response systems among international allies, including the United Kingdom.
Eleven years after the government said it would establish partnerships with other levels of government and with critical infrastructure owners and operators to help protect Canada's critical infrastructure, not all of the sector networks that facilitate these partnerships are fully established, and coverage is incomplete. This lack of progress limits Public Safety Canada's ability to communicate with critical infrastructure owners and operators. Reference: Page 2	• The Government of Canada has longstanding partnerships with critical infrastructure sectors, including energy, finance, and transportation – something the OAG has acknowledged. • Since the 2010 announcement of the *National Strategy and Action Plan for Critical Infrastructure*, the Government has formalized these partnerships with the creation of networks for each critical infrastructure sector. These partnerships have helped the Government achieve significant progress in enhancing the resilience of Canada's critical infrastructure. • To strengthen the sector networks, my department has created a planning guide and risk management guide for critical infrastructure sectors. Both have been shared with our sector networks to help them develop risk management plans that are tailored to the needs of critical infrastructure owners and operators. We have also a launched site assessment program for these owners and operators, and we regularly coordinate threat briefings for our sector networks. • In addition, Public Safety Canada is working with lead federal departments and agencies to review the membership of the sector networks, and ensure that we are building partnerships with the full range of stakeholders. By December 2013, officials will issue final guidelines on sector network membership. • As noted by the Auditor General, we have also established a National Cross Sector Forum that brings together representatives from all ten critical infrastructure sectors to identify priorities for collaborative public-private sector action. This National Cross Sector Forum meets annually and has been briefed on cyber threats during each meeting.

OAG Observation	Key Messages
Funding of $780 million was allocated for emergency management and other national security activities, including critical infrastructure protection. Reference: 3.19	• Cyber security and critical infrastructure protection are shared responsibilities among federal departments/agencies, other levels of government, and the private sector. • For example, there is spending on cyber security by every federal department and agency, and in various emergency management and national security program areas. • It is important to be clear that while a portion of the $780M referenced by the OAG went directly to protecting critical infrastructure from cyber threats, a significant portion was committed to other important national security and emergency management areas. Specifically: o $20.9M over ten years went directly to policy and program work across several departments and agencies to protect critical infrastructure from cyber threats; o $570M went to CSEC for a number of activities of national security importance – including the protection of government systems from cyber attacks. This is of great importance for the protection of Canadians and their information since the Government of Canada is the largest target for cyber attacks within our borders; and o The remaining $190M supported a variety of activities not directly related to critical infrastructure, but still of national importance, across a number departments and agencies, ranging from marine security to emergency management training activities.

OAG Observation	Key Messages
Public Safety Canada officials informed us that about $20.9 million of the remaining $210 million was directed toward cyber protection for critical infrastructure between 2001 and 2011. Reference: 3.21	• Funding has kept pace with the nature of national security threats to Canada. If we look back to the early 2000's when funding was being allocated, there are two things to bear in mind. • First, the identified and current threats were different. 9/11 had made clear the ability and willingness of terrorists to undertake physical attacks, so this is where essential work and funding was focused. • Second, the cyber threat was still evolving. For example, critical infrastructure operators have long had software to remotely control their industrial systems. These did not need major security features because they were all internal and not accessible from outside these companies. Over the last number of years, as every business has become interconnected through the Internet, it has become possible to affect what once were only internal computer systems and software. At the same time, Government has funding to implement *Canada's Cyber Security Strategy* so that we can continue to enjoy the social and economic benefits of cyber innovation.
The Department was not able to provide us with action plans, as none had been developed, with the exception of the National strategy and action plan for critical infrastructure.... In our opinion, the lack of action plans since the 2001 commitments for cyber security were announced has contributed to the overall lack of measurable progress. Reference: 3.23	• An implementation plan was developed prior to the launch of the *Strategy* in October 2010. • But, given the sensitive, classified nature of the activities related to protecting government systems, it could not be released publicly. • A public version of this plan has now been developed, and will be released in the coming weeks - TBD. • It will communicate our progress more clearly to Canadians, and underscore the need for all Canadians, and owners and operators of vital systems, to do their part.

OAG Observation	Key Messages
All 10 networks have sector risk profiles and lead departments identified, but 6 did not include representatives from all the industry groups that Public Safety Canada identified as key stakeholders. We also noted that while most have met, only 5 have included cyber security in their discussions. Reference: 3.32	• Public Safety Canada works closely with the lead federal departments to support partnership-building through the sector networks, and to encourage participation of stakeholders in risk management activities. • To address the Auditor General's findings, Public Safety Canada has launched a review of the membership of the sector networks, and will provide final guidance to lead federal departments and agencies by December 2013. • As noted by the Auditor General, these sector networks are valuable mechanisms for building public-private sector partnerships and facilitating risk management activities. For example, cyber threat briefings have been delivered to critical infrastructure sectors, including water, information and communications technology, transportation, safety, government, energy and finance. • The National Cross Sector Forum, which includes representatives from each of the 10 sectors, also receives annual cyber security briefings. In addition, Public Safety Canada and the Canadian Security Intelligence Service hosted a multi-sector meeting on cyber security in April 2012.
We noted that, during an incident where federal government systems were the target of hackers, CCIRC was not notified by the affected departments until more than one week after the intrusion was discovered, contrary to procedure. Reference: 3.48	• While I can't comment directly on specific incidents, I can say that generally, in the event of an attack on government systems, the lead agency with the technical abilities to respond is the Communication Security Establishment Canada. They have the tools and authority to mitigate an attack and provide a comprehensive response. • In the event of an incident, a department's Chief Information Officer and CSEC liaise to determine the best response. • CSEC does keep CCIRC informed so that any relevant information for critical infrastructure sectors can be passed on to our partners.

OAG Observation	Key Messages
We found that CSEC has not been consistently providing CCIRC with timely and complete information gained from its monitoring of government systems... This issue was to be resolved by the end of August 2011, but had not yet been resolved at the time of the audit. Reference: 3.49	• As Canada's national cryptologic and signal intelligence agency, CSEC comes into contact with a variety of extremely sensitive information. They are appropriately scrupulous in not only how they share information, but also in taking care in where and in what form it might be passed on. CCIRC and CSEC continue to develop closer working relationships through practical measures, like developing operating procedures to ensure that each understands how and in what circumstances information should be shared. • CSEC routinely shares cyber threat information and mitigation advice with CCIRC at Public Safety. • Since 2011, CSEC has had standard operating procedures for sharing specific incident information and mitigation advice in a timely and secure manner to government IT security partners. • In addition, as noted by the Auditor General's report notes, a CCIRC employee has also been integrated into CSEC's Government of Canada Cyber Threat Evaluation Centre (GC-CTEC) with full access to threat data.

OAG Observation	Key Messages
A lack of timely and relevant information and analyses affects the ability of critical infrastructure owners and operators to react to cyber-attacks that may cause disruptions Reference: 3.70	• As the Government has announced, CCIRC has extended its hours to 15/7 starting in November 2012. The purpose of this extension of hours is to ensure that our private and public sector clients, who are located in all time zones across the country, can reach CCIRC during their regular work days. • CCIRC works collaboratively with private sector partners by providing trusted value added products and services, meaning that it relies on having a service in which organizations want to participate rather than forcing cooperation. • We have achieved significant progress with this approach, and risk management activities are underway, including security briefings, and exercises. • While it is sometimes asked to provide timely mitigation information and warnings, CCIRC's primary role is to monitor and provide strategic and technical advice on cyber threats, as well as to coordinate national response against cyber attacks, outside of federal government systems. • CCIRC has taken steps to improve information sharing and dialogue with its partners, including launching an incident response pilot and establishing an online Community Portal.

Public Safety Canada | Sécurité publique Canada

MANAGEMENT ACTION PLAN

AUDITOR GENERAL'S REPORT, CHAPTER 3
PROTECTING CANADIAN CRITICAL INFRASTRUCTURE AGAINST CYBER THREATS

Recommendations	Management Implementation Actions	Lead	Timelines
(3.25). Public Safety Canada (PS) should develop an interdepartmental action plan with deliverables and timelines for Canada's Cyber Security Strategy (2010) to guide the implementation of the strategy and measure progress.	• Publicly release an action plan to guide the effective delivery of Canada's Cyber Security Strategy. • Complete the development of a horizontal performance measurement strategy (HPMS) to measure and report on the progress made against commitments in Canada's Cyber Security Strategy. • Implement the HPMS and request performance information annually from the departments and agencies involved in the implementation of the strategy.	Director General, National Cyber Security Directorate	• Winter 2013 • Completed • Ongoing
(3.37). Public Safety Canada should ensure that all sector networks are fully established and operating as outlined in the National strategy and action plan for critical infrastructure so that they can be an effective tool in helping to secure critical infrastructure in order to deliver the objectives of Canada's Cyber Security Strategy.	• Provide guidance to lead federal departments and agencies on appropriate coverage for sector networks, including: o Draft guidance based on the sector risk profiles by June 2013; and o Final guidance, based on feedback from the lead federal departments/agencies, by December 2013. • Work with lead federal departments to strengthen the sector networks by facilitating information sharing and providing tools to support risk management, including: o Planning guidance for critical infrastructure sectors; o Guidance for critical infrastructure sectors to conduct tabletop exercises; and o Development of a national profile of critical infrastructure.	Director General, Critical Infrastructure and Strategic Coordination	• December 2013 • December 2013

Recommendations	Management Implementation Actions	Lead	Timelines
(3.52). Public Safety Canada should increase the Canadian Cyber Incident Response Centre's ability to maintain situational awareness of cyber threats to Canada's critical infrastructure and to increase the Centre's ability to communicate this information to critical infrastructure owners and operators.	• Increase CCIRC's operational hours, and operational capacity and capabilities to enhance support for critical infrastructure and other partners. • Update CCIRC's mandate, and standard procedures and policies to provide greater clarity to internal and external partners. • Introduce CCIRC's Community Portal, create formal information-sharing agreements, and launch an incident response pilot to improve information sharing with partners. • Continue to deepen CCIRC's capabilities and expand its reach by working with lead sector departments to identify owners and operators of critical infrastructure.	Director General, National Cyber Security Directorate	• Completed • Completed • Completed • Ongoing

PLAN D'ACTION DE LA GESTION

RAPPORT DU VÉRIFICATEUR GÉNÉRAL, CHAPITRE 3
PROTÉGER L'INFRASTRUCTURE CANADIENNE ESSENTIELLE CONTRE LES CYBERMENACES

Recommandations	Mesures à mettre en œuvre par la direction	Responsables	Échéances
(3.25) Sécurité publique Canada (SP) devrait établir un plan d'action interministériel, prévoyant des produits à livrer et des échéanciers, afin d'orienter la mise en œuvre de la *Stratégie de cybersécurité du Canada* (2010) et de mesurer les progrès accomplis.	• Diffuser publiquement un plan d'action afin d'orienter la prestation efficace de la Stratégie de cybersécurité du Canada. • Élaborer une stratégie horizontale de mesure du rendement pour mesurer l'avancement des engagements de la *Stratégie de cybersécurité du Canada* et en faire rapport. • Mettre en œuvre la stratégie horizontale de mesure du rendement et demander tous les ans des renseignements sur le rendement aux ministères et aux organismes participant à la mise en œuvre de la stratégie.	Directeur général, Direction générale de la cybersécurité nationale	• Hiver 2013 • Terminé • En cours
(3.37) Sécurité publique Canada devrait s'assurer que tous les réseaux sectoriels sont pleinement établis et fonctionnent comme le prévoient la stratégie nationale et le plan d'action sur les infrastructures essentielles, afin qu'ils deviennent un outil efficace pour protéger l'infrastructure essentielle et atteindre les objectifs de la *Stratégie de cybersécurité du Canada*.	• Orienter les ministères et les organismes sur la couverture appropriée des réseaux sectoriels : o ébauche de l'orientation fondée sur les profils de risque des secteurs d'ici juin 2013; o orientation finale, fondée sur les commentaires des ministères et des organismes fédéraux responsables, d'ici décembre 2013. • Travailler avec les ministères fédéraux responsables en vue de renforcer les réseaux sectoriels en facilitant l'échange d'information et en fournissant les outils pour appuyer la gestion du risque, dont : o un guide de planification pour les secteurs des infrastructures essentielles; o des conseils afin que les secteurs des infrastructures essentielles puissent mener des exercices sur table.	Directeur général, Direction générale des infrastructures essentielles et de la coordination stratégique	• Décembre 2013 • Décembre 2013

Recommandations	Mesures à mettre en œuvre par la direction	Responsables	Échéances
(3.52) Sécurité publique Canada devrait renforcer la capacité du Centre canadien de réponse aux incidents cybernétiques à maintenir une connaissance de la situation relative aux cybermenaces qui pèsent contre l'infrastructure essentielle du Canada et à communiquer cette information aux propriétaires et aux exploitants d'éléments de l'infrastructure essentielle.	• Prolonger les heures d'activité du CCRIC, de même que sa capacité opérationnelle, afin de mieux soutenir les infrastructures essentielles et les autres partenaires. • Mettre à jour le mandat du CCRIC, de même que ses procédures et ses politiques normalisées, afin que ces éléments soient plus clairs pour les partenaires internes et externes. • Mettre en place le Portail de la communauté du CCRIC, établir des ententes officielles d'échange d'information et lancer un projet pilote d'intervention en cas d'incident dans le but d'améliorer l'échange d'information avec les partenaires. • Continuer à accroître les capacités du CCRIC et à étendre sa portée en travaillant avec les exploitants d'infrastructures essentielles.	Directeur général, Direction générale de la cybersécurité nationale	• Terminé • Terminé • Terminé • En cours

ANNOTATED MANAGEMENT ACTION PLAN

OAG Recommendation	Management Implementation Actions	Progress	Key Messages
Public Safety Canada (PS) should develop an interdepartmental action plan with deliverables and timelines for Canada's Cyber Security Strategy (2010) to guide the implementation of the strategy and measure progress.	Publicly release an action plan to guide the effective delivery of Canada's Cyber Security Strategy. **(Winter 2013)** Complete the development of a horizontal performance measurement strategy (HPMS) to measure and report on the progress made against commitments in Canada's Cyber Security Strategy. **(Completed)** Implement the horizontal performance measurement strategy and request performance information annually from the departments and agencies involved in the implementation of the strategy. **(Ongoing)**	The action plan and performance measurement strategy have been approved by ADM-Cyber. **(Completed: January 2013)** A communications strategy has been developed by Public Safety Canada Communications to support the release of the action plan. **(Completed: January 2013)** Minister Toews is writing to his colleagues to seek their final approval of the action plan by March 4, 2013. **(Underway)** Performance indicators have been developed and approved interdepartmentally at the Assistant Deputy Minister level and have been provided to TBS. **(Completed: October 2012)** Departments and agencies are actively collecting data against performance indicators in the performance measurement strategy. **(Underway)**	• A detailed, classified implementation plan was developed and approved prior to the launch of *Canada's Cyber Security Strategy* in October 2010. • But given the sensitive, classified nature of the activities related to protection of Government of Canada systems, it could not be released publicly. • A public version of this plan has now been developed, and will be released in the coming weeks - TBD. • It will communicate our progress more clearly to Canadians, and underscore the need for all Canadians, and owners and operators of vital systems, to do their part. • We have also developed a horizontal performance measurement strategy, with input from key departments and agencies, to help us track progress made on our *Cyber Security Strategy*.

.../2

OAG Recommendation	Management Implementation Actions	Progress	Key Messages
Public Safety Canada should ensure that all sector networks are fully established and operating as outlined in the National strategy and action plan for critical infrastructure so that they can be an effective tool in helping to secure critical infrastructure in order to deliver the objectives of Canada's Cyber Security Strategy.	Provide guidance to lead federal departments and agencies on appropriate coverage for sector networks, including: • Draft guidance based on the sector risk profiles. **(June 2013)** • Final guidance, based on feedback from the lead federal departments/agencies. **(December 2013)** Work with lead federal departments to strengthen the sector networks by facilitating information sharing and providing tools to support risk management, including: • Planning guidance for critical infrastructure sectors. (**December 2013**) • Guidance for critical infrastructure sectors to conduct tabletop exercises. **(December 2013)** • Development of a national profile of critical infrastructure. **(December 2013)**	Consultations are underway with lead federal departments/agencies to review membership of the sector networks, based on the sector profiles. **(Underway)** A *Critical Infrastructure Planning Guide* was developed to support the development of risk management plans for critical infrastructure sectors. **(Completed: December 2012)** A *Table Top Exercise in a Box* was developed to provide owners and operators with tools to test and validate their risk management plans. **(Completed: December 2012)** Development of a *National Profile of Critical Infrastructure* is underway. This document will identify and prioritize the most significant risks facing each critical infrastructure sector. **(Underway)**	• To strengthen Canada's sector networks, my Department has created a planning guide and risk management guide for critical infrastructure sectors. Both have been shared with our sector networks to help them develop risk management plans that are tailored to the needs of critical infrastructure owners and operators. • We have also a launched site assessment program for these owners and operators, and we regularly coordinate threat briefings for our sector networks. • Public Safety Canada is also working with lead federal departments and agencies to review the membership of the sector networks, and ensure that we are building partnerships with the full range of stakeholders. By December 2013, officials will issue final guidelines on sector network membership.

.../3

OAG Recommendation	Management Implementation Actions	Progress	Key Messages
Public Safety Canada should increase the Canadian Cyber Incident Response Centre's ability to maintain situational awareness of cyber threats to Canada's critical infrastructure and to increase the Centre's ability to communicate this information to critical infrastructure owners and operators.	Increase CCIRC's operational hours, and operational capacity and capabilities to enhance support for critical infrastructure and other partners. **(Completed)** Update CCIRC's mandate, and standard procedures and policies to provide greater clarity to internal and external partners. **(Completed)** Introduce CCIRC's Community Portal, create formal information sharing agreements, and launch an incident response pilot to improve information sharing with partners. **(Completed)** Continue to deepen CCIRC's capabilities and expand its reach by working with lead sector departments to identify owners and operators of critical infrastructure. **(Ongoing)**	CCIRC's operational hours have been expanded to cover Canada's business day from coast-to-coast-to-coast. **(Completed: November 5, 2012)** CCIRC's operational capacity and capabilities has been enhanced by: • Acquiring an advanced malware research and analysis system; **(Completed: July 2012)** • Building and integrating an industrial control system test bed; and **(Completed: March 2012)** • Deploying a National Cyber Threat Notification System. **(Ongoing)** The CCIRC's mandate has been updated. **(Completed: August 2012)** CCIRC's standard procedures and policies have been updated, including: • Updated Privacy Impact Assessment; **(Completed: July 2012)** • Developed standard operating procedures for CCIRC. (**Ongoing)** • Developed a Request for Technical Assistance agreement. **(Completed: January 2013)** CCIRC's community portal has been launched. **(Completed: October 2012)** CCIRC continues to undertake the creation of information sharing agreements with critical infrastructure partners. **(Ongoing)**	• In November, 2012, CCIRC expanded its operational hours to 15 hours a day, seven days a week onsite coverage, allowing it to cover the full business operating hours of its clients. • It's important to note, however, that CCIRC experts are on call 24 hours a day, seven days a week, to deal with emergency situations. • This on-call system is similar to those used by our international allies, including the United Kingdom. • CCIRC has also taken steps to improve information sharing and dialogue with its partners, including launching an incident response pilot and establishing an online Community Portal.

CYBER SECURITY

PROPOSED RESPONSE:

- **In 2010, the Government released *Canada's Cyber Security Strategy* as a statement of the priority placed on protecting citizens, businesses, and critical infrastructure from cyber security threats. Federal departments and agencies are working together to implement the Strategy by strengthening the security of federal systems and delivering programs and benefits to Canadians.**

- **Public Safety Canada has made the implementation of the Strategy a priority in our 2012-13 Reports on Plans and Priorities. Furthermore, we expect to begin reporting on progress made towards implementing the Strategy in our 2011-12 Departmental Performance Report.**

- **Supplementary Estimates A increases the amount of funding in 2012-13 for Public Safety Canada by an additional $3.0 million. A total of $9.5 million will be directed towards Public Safety Canada's efforts under *Canada's Cyber Security Strategy* in 2012-13.**

- **The additional funding identified in Supplementary Estimates A will enable Public Safety Canada to strengthen the Canadian Cyber Incident Response Centre's (CCIRC) operations, which include providing information and advice to private and public sector stakeholders on how to manage cyber security threats.**

- **The Government will continue to raise awareness through the *"Get Cyber Safe"* website, providing a trusted source of information on online risks and advice on how Canadians can protect themselves online.**

CYBER SECURITY

QUESTIONS AND ANSWERS:

Q1. Why is Public Safety Canada (PS) seeking $3.0 million through Supps A?

A1. Supplementary Estimates A includes additional funding of $31 million to four departments in 2012-13 to support the implementation of *Canada's Cyber Security Strategy*. The funding will be directed towards enhancements in the Government of Canada's cyber security infrastructure and related support mechanisms.

As part of Supplementary Estimates A, PS will receive $3.0 million, out of the total $31 million, in 2012-13 to support key activities in the areas of incident response and information sharing. More specifically, PS deliverables in 2012-13 are to:

- enhance the engagement and information sharing activities of the Canadian Cyber Incident Response Centre (CCIRC) with critical domestic and international stakeholders; and
- expand the operational service delivery hours of CCIRC, to provide service during business hours coast to coast to Canada's private and public sector stakeholders.

Dept/Agency (thousands)	2012-13	2013-14	2014-15	2015-16	Total (4 years)	Ongoing
PS	2,965	2,897	2,589	2,697	11,149	2,697

*** All figures are net of EBP and accommodations charges.

Q2. What progress has been made to date in implementing *Canada's Cyber Security Strategy*?

A2. Federal departments and agencies are implementing each of the three pillars of the Strategy: strengthening Government of Canada systems and networks; partnering to secure vital networks and systems outside of the federal Government; and helping Canadians be secure online.

In its efforts to further secure Government systems, the Government of Canada has made targeted investments to augment security measures on federal networks; reduced the number of Internet access points; and made amendments to the *Policy on Government Security*. In addition, the Government of Canada announced the creation of Shared Services Canada, which will reduce the overall number of data centres, streamline the Government's electronic network, save money and improve services to Canadians.

PS leads the federal effort to partner with other levels of government and the private sector to ensure that the integrity of information and services is maintained. We have strengthened our relationships with established partners, are expanding our outreach to additional sectors, and are bolstering the technical and operational capacity to enhance our advice and support to our stakeholders.

The Department is also leading efforts to help Canadians be secure online through activities such as increased public awareness as part of the *Get Cyber Safe* campaign.

Q3. What is the Government of Canada doing to protect systems that are the responsibility of provincial and territorial governments or the private sector?

A3. The Government of Canada is partnering with other levels of government and the private sector to advance shared priorities including the establishment of information sharing mechanisms. The Government of Canada is leveraging its resources to ensure that other levels of government and the private sector get the support they need, when they need it, including information, advice, access to tools and other support.

Q4. How does the Strategy help me if my computer becomes infected, hacked or compromised?

A4. The Government is also raising awareness directly with citizens through the *Get Cyber Safe* website, providing a trusted source of information about online risks and concrete advice on how Canadians can better protect themselves online.

CONTACTS:			
Prepared by Robert Dick, Director General, National Cyber Security Directorate	Tel. no. 613-990-2661	Approved by (ADM level only) Robert Gordon, Acting Senior Assistant Deputy Minister, National Security Branch	Tel. no. 613-949-7380 BB: [redacted]

s.19(1)

CYBER SECURITY

PROPOSED RESPONSE:

- **Public Safety Canada made the implementation of *Canada's Cyber Security Strategy* a priority in its 2012-13 Report on Plans and Priorities. The Department reported on initial milestones made in implementing the Strategy in our recently released 2011-12 Departmental Performance Report.**

- **Public Safety Canada is working to implement responses to the recommendations outlined by the report of the Office of the Auditor General. Namely, the Department is:**
  - **preparing to release an interdepartmental action plan;**
  - **strengthening critical infrastructure sector networks; and**
  - **enhancing the Canadian Cyber Incident Response Centre.**

- **The Government of Canada announced $155 million in additional funding over five years to support the implementation of *Canada's Cyber Security Strategy*. This funding supports efforts to strengthen federal cyber infrastructure and extends the Canadian Cyber Incident Response Centre's hours to 15 hours a day, 7 days a week.**

- **The Government of Canada and the United States recently announced a *Cybersecurity Action Plan between Public Safety Canada and the Department of Homeland Security*. This joint action plan enhances cooperation on cyber incident management between Canada and the U.S. to better protect shared critical digital infrastructure and improve coordination of responses to cyber incidents.**

- **The Government will continue to raise awareness through the *"Get Cyber Safe"* website, providing a trusted source of information on online risks and advice on how Canadians can protect themselves online.**

QUESTIONS AND ANSWERS:

Q1. What progress has been made to date in implementing *Canada's Cyber Security Strategy*?

A1. Federal departments and agencies are implementing each of the three pillars of the Strategy: strengthening Government of Canada systems and networks, partnering to secure vital networks and systems outside of the federal Government, and helping Canadians be secure online.

In its efforts to further secure Government systems, the Government of Canada has made targeted investments to augment security measures on federal networks, reduced the number of Internet access points, and made amendments to the *Policy on Government Security*. The Government of Canada created Shared Services Canada, which will reduce the overall number of data centres, streamline the Government's electronic network, save money and improve services to Canadians.

PS leads the federal effort to partner with other levels of government and the private sector to ensure that the integrity of information and services is maintained. We have strengthened our relationships with established partners, are expanding our outreach to additional sectors, and are bolstering the technical and operational capacity to enhance our advice and support to our stakeholders.

The Department is also leading efforts to help Canadians be secure online through activities such as increased public awareness as part of the *Get Cyber Safe* campaign. In October, which is *Cyber Security Awareness Month,* the Minister of Public Safety made a number of announcements highlighting federal cyber security efforts.

Q2. What is Public Safety Canada (PS) doing to respond to the recommendations outlined in the fall 2012 Report of the Office of the Auditor General?

A2. PS is currently coordinating the release of the public action plan among federal departments and agencies responsible for activities under the Strategy.

The Department is continuing to work with lead federal departments and agencies to strengthen sector networks, share information with stakeholders, including cyber information, and provide tools to support each sector's respective risk management efforts. Given the varied needs and representation of each critical infrastructure sector, the Department has committed to provide guidance on appropriate coverage for sector networks by December 2013.

The Government recently announced additional funding of $155 million over five years to support objectives under *Canada's Cyber Security Strategy*. This funding includes an additional $13 million over five years to expand the capacity of the Canadian Cyber Incident Response Centre (CCIRC). The Department has also taken steps to clarify CCIRC's mandate and operations which will enable it to improve its service delivery to Canada's critical infrastructure sectors.

Q3. What is the Government of Canada doing to protect systems that are the responsibility of provincial and territorial governments or the private sector?

A3. The Government of Canada is partnering with other levels of government and the private sector to advance shared priorities including the establishment of information sharing mechanisms. The Government of Canada is leveraging its resources to ensure that other levels of government and the private sector get the support they need, when they need it, including information, advice, access to tools and other support.

Q4. How does the Strategy help me if my computer becomes infected, hacked or compromised?

A4. The Government is also raising awareness directly with citizens through the *Get Cyber Safe* website, providing a trusted source of information about online risks and concrete advice on how Canadians can better protect themselves online.

CONTACTS: Prepared by	Tel. no.	Approved by (ADM level only)	Tel. no.
Robert Dick, Director General, National Cyber Security Directorate	613-990-2661	Lynda Clairmont, Senior Assistant Deputy Minister, National Security Branch	613-990-4976

CYBERSÉCURITÉ

RÉPONSE PROPOSÉE :

- **Sécurité publique Canada a fait de la mise en place de la *Stratégie nationale de cybersécurité* une priorité dans son Rapport sur les plans et les priorités 2012-2013. Des représentants du Ministère ont présenté un rapport sur les réalisations initiales associées à la mise en œuvre de la Stratégie dans le Rapport ministériel sur le rendement 2011-2012, publié récemment.**

- **Sécurité publique Canada travaille à donner suite aux recommandations formulées dans le rapport du Bureau du vérificateur général. Notamment, le Ministère déploie actuellement des efforts pour :**
  - **préparer un plan d'action interministériel;**
  - **renforcer les réseaux sectoriels des infrastructures essentielles;**
  - **améliorer le rendement du Centre canadien de réponse aux incidents cybernétiques.**

- **Les représentants du gouvernement du Canada ont annoncé un financement supplémentaire de 155 millions de dollars sur cinq ans pour appuyer la poursuite de la mise en œuvre de la *Stratégie nationale de cybersécurité*. Ce financement appuie les efforts visant à renforcer les infrastructures cybernétiques essentielles fédérales et à prolonger les heures d'ouverture du Centre canadien de réponse aux incidents cybernétiques afin qu'il mène ses opérations 15 heures par jour, 7 jours par semaine.**

- **Des représentants du gouvernement du Canada et des État-Unis ont récemment annoncé l'adoption du Plan d'action en matière de cybersécurité entre Sécurité publique Canada et le département de la Sécurité intérieure. Ce plan d'action conjoint améliore la collaboration en matière de gestion des incidents cybernétiques entre le Canada et les États-Unis afin de mieux protéger les infrastructures numériques essentielles partagées et d'améliorer la capacité de coordonner l'intervention en cas d'incident cybernétique.**

- **Le gouvernement continuera de sensibiliser la population à l'aide du site Web « Pensez cybersécurité », une source fiable de renseignements sur les risques associés à Internet et de conseils sur la façon dont les Canadiens peuvent se protéger en ligne.**

QUESTIONS ET RÉPONSES

Q1. Quels progrès ont été réalisés jusqu'à maintenant dans le cadre de la mise en œuvre de la *Stratégie nationale de cybersécurité*?

R1. Les ministères et organismes fédéraux s'affairent à mettre en place chacun des trois piliers de la Stratégie : renforcement des systèmes et des réseaux du gouvernement du Canada; établissement de partenariats en vue d'assurer la protection des réseaux essentiels et des systèmes à l'extérieur du gouvernement fédéral; appui aux Canadiens afin de les aider à se protéger sur Internet.

Dans le cadre des efforts qu'il déploie pour protéger davantage ses systèmes, le gouvernement du Canada a fait des investissements ciblés afin d'accroître les mesures de sécurité dans les réseaux fédéraux, il a réduit le nombre de points d'accès à Internet et il a modifié la Politique sur la sécurité du gouvernement. Le gouvernement du Canada a créé Services partagés Canada, qui réduira le nombre de centres de données, harmonisera le réseau électronique du gouvernement, économisera de l'argent et améliorera les services offerts aux Canadiens.

Sécurité publique Canada dirige les efforts du gouvernement fédéral visant à établir des partenariats avec d'autres ordres de gouvernement et le secteur privé pour s'assurer de maintenir l'intégrité de l'information et des services. Nous avons renforcé nos relations avec les partenaires établis, et nous élargissons nos activités de sensibilisation au sein d'autres secteurs, en plus d'accroître la capacité technique et opérationnelle en vue d'améliorer les conseils et l'appui que nous offrons aux intervenants.

Le Ministère dirige aussi les efforts visant à aider les Canadiens à se protéger sur Internet en menant des activités permettant, entre autres, de sensibiliser davantage la population, dans le cadre de la campagne « Pensez cybersécurité ». En octobre, le *Mois de la sensibilisation à la cybersécurité*, le ministre de la Sécurité publique a fait plusieurs annonces soulignant les efforts du gouvernement fédéral en matière de cybersécurité.

Q2. Que fait Sécurité publique Canada pour répondre aux recommandations faites dans le rapport du Bureau du vérificateur général publié à l'automne 2012?

R2. Sécurité publique Canada coordonne actuellement la publication du plan d'action public parmi les ministères et organismes fédéraux chargés de mener les activités conformément à la Stratégie.

Le Ministère continue de collaborer avec les principaux ministères et organismes fédéraux pour renforcer les réseaux sectoriels, échanger l'information avec les intervenants, y compris l'information sur la cybersécurité, et fournir des outils permettant d'appuyer les efforts de gestion du risque de chaque secteur. En raison des divers besoins et de la variété de représentants de chaque secteur des infrastructures essentielles, le Ministère s'est engagé à formuler des conseils sur la couverture appropriée des réseaux sectoriels d'ici décembre 2013.

Les représentants du gouvernement ont récemment annoncé un financement additionnel d'une valeur de 155 millions de dollars sur cinq ans pour appuyer l'atteinte des objectifs énoncés dans la *Stratégie nationale de cybersécurité*. Ce financement comprend un investissement additionnel de 13 millions de dollars sur cinq ans pour accroître la capacité du Centre canadien de réponse aux incidents cybernétiques. Le Ministère a aussi pris des mesures pour préciser le mandat du Centre et la nature de ses opérations, ce qui lui permettra d'améliorer la prestation de ses services dans les secteurs des infrastructures essentielles au Canada.

Q3. Que fait le gouvernement du Canada pour protéger les systèmes dont sont chargés les gouvernements provinciaux et territoriaux ou le secteur privé?

R3. Les représentants du gouvernement du Canada établissent des partenariats avec les autres ordres de gouvernement et le secteur privé pour atteindre les priorités communes, y compris l'établissement de mécanismes d'échange d'information. Le gouvernement du Canada tire profit de ses ressources pour s'assurer que les autres ordres de gouvernement et le secteur privé reçoivent l'appui dont ils ont besoin, au moment opportun, notamment des renseignements, des conseils et un accès à des outils et à d'autres mesures de soutien.

Q4. Comment la Stratégie m'aidera-t-elle si mon ordinateur est infecté, piraté ou compromis?

R4. Le gouvernement sensibilise aussi la population directement à l'aide du site Internet « Pensez cybersécurité », qui représente une source fiable d'information au sujet des risques sur Internet et de conseils concrets sur la façon dont les Canadiens peuvent mieux se protéger en ligne.

PERSONNES-RESSOURCES Rédigé par Robert Dick, directeur général, Direction générale de la cybersécurité nationale	Tél. : 613-990-2661	Approuvé par (au niveau du SMA seulement) Lynda Clairmont, sous-ministre adjointe principale, Secteur de la sécurité nationale	Tél. : 613-990-4976

CYBER SECURITY

PROPOSED RESPONSE:

- **Main Estimates increases the amount of national security funding in 2013-2014 for Public Safety Canada's cyber security activities by an additional $2.4 million to the program area. This funding will enable the Department to increase the operational capacity and capabilities of the Canadian Cyber Incident Response Centre to better assist Canada's critical infrastructure sectors in detecting, deterring, mitigating and responding to cyber security threats.**

- **In October 2012, the Government announced $155 million in additional funding to support the implementation of *Canada's Cyber Security Strategy*. This funding supports efforts to strengthen federal cyber infrastructure and extends the Canadian Cyber Incident Response Centre's onsite hours to 15 hours a day, 7 days a week. The Canadian Cyber Incident Response Centre continues to provide emergency access to staff 24 hours a day, 7 days a week.**

- **Since extending onsite business hours to 15 hours a day, 7 days a week, in November 2011, the Canadian Cyber Incident Response Centre has received zero cyber incident reports from domestic partners outside those hours.**

- **In October 2012, Canada and the United States publicly announced a *Cybersecurity Action Plan between Public Safety Canada and the Department of Homeland Security*. This joint action plan enhances operational collaboration between Canada and the U.S. to better protect shared critical digital infrastructure and improve the coordination of responses to cyber incidents.**

- **The Government continues to raise awareness through the *"Get Cyber Safe"* website, providing a trusted source of information on online risks and advice on how Canadians can protect themselves online.**

QUESTIONS AND ANSWERS:

Q1. Why is Public Safety Canada (PS) seeking $2.4 million through 2013-2014 Main Estimates?

A1. The Main Estimates for 2013-14 includes additional funding of $36.9 million to the Communications Security Establishment Canada, Treasury Board Secretariat, Public Safety Canada and Shared Services Canada to enhance cyber security infrastructure and support mechanisms. For reasons of internal security we cannot comment on the breakdown.

As part of 2013-14 Main Estimates, PS will receive $3.5 million, out of the total $36.9 million, to support key activities in the areas of incident response and information sharing. The Main Estimates identify $2.4 million as part of national security branch expenditures, while additional funding is directed towards accommodations, internal services and employee benefit plans.

Q2. What is PS doing to respond to the recommendations outlined in the fall 2012 Report of the Office of the Auditor General?

A2. PS will release a public Cyber Security Action Plan which will outline the Government's efforts to enhance cyber security and serve as a guide for implementation activities under the Strategy.

The Department continues to work with lead federal departments and agencies to strengthen sector networks, share information with stakeholders and provide tools to support each sector's respective risk management efforts, including, a *Critical Infrastructure Planning Guide* and a *Table Top Exercise guide*. Given the varied needs and representation of each critical infrastructure sector, the Department has committed to both provide guidance on appropriate coverage for sector networks and develop a national profile of critical infrastructure by December 2013.

The Government recently announced additional funding of $155 million over five years to support objectives under *Canada's Cyber Security Strategy*. This funding includes an additional $13 million over five years to expand the onsite coverage for of the Canadian Cyber Incident Response Centre (CCIRC) to 15 hours a day, 7 days a week, with emergency access to staff 24 hours a day. The Department also:

- updated CCIRC's mandate, procedures and policies to provide greater clarity to stakeholders;
- introduced CCIRC's Community Portal, created formal information sharing agreements and launched an incident response pilot to improve information sharing with partners; and
- continues to deepen CCIRC's capabilities and expand its reach with critical infrastructure owners and operators.

Q3. What progress has been made to date in implementing *Canada's Cyber Security Strategy*?

A3. Federal departments and agencies are implementing each of the three pillars of the Strategy: strengthening Government of Canada systems and networks, partnering to secure vital networks and systems outside of the federal Government, and helping Canadians be secure online.

In its efforts to further secure Government systems, the Government of Canada has made targeted investments to augment security measures on federal networks, reduced the number of Internet access points, and made amendments to the *Policy on Government Security*.

PS leads the federal effort to partner with other levels of government and the private sector to ensure that the integrity of information and services is maintained. We have strengthened our relationships with established partners, are expanding our outreach to additional sectors, and are bolstering the technical and operational capacity to enhance our advice and support to our stakeholders. For example, in October 2012, the Minister of Public Safety announced the release of a Cybersecurity Action Plan with the United States Department of Homeland Security to enhance:

- operational collaboration between national cyber security operations centres;
- joint engagement and information sharing with the private sector on cyber security; and
- cooperation on ongoing cyber security public awareness efforts.

The Department is also leading efforts to help Canadians be secure online through activities such as increased public awareness as part of the *Get Cyber Safe* campaign.

CONTACTS:			
Prepared by Robert Dick Director General, NCSD	Tel. no. 613-990-2661	Approved by DG Robert Dick Director General, NCSD	Tel. no. 613-990-2661

CYBERSÉCURITÉ

RÉPONSE PROPOSÉE :

- **Le Budget principal des dépenses prévoit une augmentation au secteur de programme de 2,4 millions de dollars du montant du financement accordé à la sécurité nationale en 2013-2014 pour les activités liées à la cybersécurité de Sécurité publique Canada. Ce financement permettra au Ministère de renforcer la capacité opérationnelle et les moyens d'action du Centre canadien de réponse aux incidents cybernétiques, et ce, dans le but de mieux aider les secteurs des infrastructures essentielles du Canada à détecter les cybermenaces, à les prévenir, à les atténuer et à intervenir le cas échéant.**

- **En octobre 2012, le gouvernement a annoncé 155 millions de dollars en financement additionnel visant à appuyer la mise en œuvre de la Stratégie de cybersécurité du Canada. Il s'agit d'un financement qui vise à favoriser les efforts déployés pour renforcer les infrastructures cybernétiques fédérales et à prolonger les heures d'ouverture du Centre canadien de réponse aux incidents cybernétiques afin qu'il mène ses opérations 15 heures par jour, 7 jours par semaine. Le Centre canadien de réponse aux incidents cybernétiques continue d'offrir un accès d'urgence aux employés 24 heures par jour, 7 jours par semaine.**

- **Depuis qu'il a prolongé ses heures d'ouverture en date de novembre 2011, le Centre canadien de réponse aux incidents cybernétiques n'a reçu aucun rapport de cyberincident de ses partenaires nationaux en dehors de ces heures.**

- **En octobre 2012, le Canada et les États-Unis ont annoncé publiquement le Plan d'action sur la cybersécurité entre Sécurité publique Canada et le département de la Sécurité intérieure. Ce plan**

d'action conjoint permet d'améliorer la collaboration opérationnelle entre le Canada et les États-Unis dans le but de mieux protéger l'infrastructure numérique essentielle partagée et d'améliorer la coordination des réponses aux incidents cybernétiques.

- **Le gouvernement continue d'accroître la sensibilisation par l'intermédiaire de son site Web intitulé : « Pensez cybersécurité », qui constitue une source d'information fiable sur les risques en ligne et qui fournit aux Canadiens des conseils sur les façons de se protéger en ligne.**

QUESTIONS ET RÉPONSES

Q1. Pourquoi Sécurité publique Canada demande-t-il 2,4 millions de dollars dans le Budget principal des dépenses de 2013-2014?

R1. Le Budget principal des dépenses de 2013-2014 prévoit un financement additionnel de 36,9 millions de dollars accordé au Centre de la sécurité des télécommunications Canada, au Secrétariat du Conseil du Trésor, à Sécurité publique Canada et à Services partagés Canada pour améliorer l'infrastructure de cybersécurité et les mécanismes habilitants. Pour des raisons de sécurité, nous ne pouvons faire aucun commentaire sur l'allocation précise des fonds.

Dans le cadre du Budget principal des dépenses de 2013-2014, SP recevra 3,5 millions de dollars, sur les 36,9 millions de dollars au total, qui l'aideront à la réalisation d'activités clés dans les domaines de la réponse aux incidents et de l'échange d'information. Le Budget principal des dépenses prévoit 2,4 millions de dollars pour les dépenses du Secteur de la sécurité nationale, tandis que le financement supplémentaire est axé sur les installations, les services internes et les régimes d'avantages sociaux des employés.

Q2. Que fait SP pour donner suite aux recommandations formulées dans le rapport du Bureau du vérificateur général publié à l'automne 2012?

R2. SP publiera un plan d'action sur la cybersécurité, qui mettra en évidence les efforts que déploie le gouvernement pour améliorer la cybersécurité et qui servira de guide pour la mise en œuvre des activités prévues par la Stratégie.

Le Ministère continue de travailler de concert avec les principaux ministères et organismes fédéraux afin de renforcer les réseaux sectoriels, d'échanger de l'information avec les intervenants et de fournir des outils permettant d'appuyer les efforts de gestion du risque de chaque secteur, notamment au moyen d'un Guide de planification sur les infrastructures essentielles et d'un Guide des exercices sur table. En raison de la représentation et des besoins variés de chacun des secteurs des infrastructures essentielles, le Ministère s'est engagé à fournir des directives sur la couverture appropriée des réseaux sectoriels et à élaborer un profil national des infrastructures essentielles au plus tard en décembre 2013.

Le gouvernement a récemment annoncé un financement additionnel de 155 millions de dollars sur cinq ans visant à favoriser l'atteinte des objectifs prévus par la Stratégie de cybersécurité du Canada. Ce financement comprend 13 millions de dollars supplémentaires sur cinq ans pour prolonger à 15 heures par jour, 7 jours par semaine, les heures d'ouverture du Centre canadien de réponse aux incidents cybernétiques, avec un accès d'urgence à des employés 24 heures par jour. Le ministère de la Sécurité publique a également :

- mis à jour le mandat, les procédures et les politiques du Centre pour aider les intervenants à mieux comprendre son rôle;
- lancé le portail de la communauté du Centre, mis en place des ententes officielles d'échange d'information et lancé un projet pilote d'intervention en cas d'incidents pour améliorer l'échange de renseignements avec les partenaires;
- continué à améliorer les moyens d'action du Centre et d'en élargir les services aux propriétaires et exploitants d'infrastructures essentielles.

Q3. Quels progrès ont été réalisés jusqu'à maintenant dans le cadre de la mise en œuvre de la Stratégie nationale de cybersécurité?

R3. Les ministères et organismes fédéraux s'affairent à mettre en place chacun des trois piliers de la Stratégie : renforcement des systèmes et des réseaux du gouvernement du Canada; établissement de partenariats en vue d'assurer la protection des réseaux essentiels et des systèmes à l'extérieur du gouvernement fédéral; appui aux Canadiens afin de les aider à se protéger sur Internet.

Dans les efforts qu'il déploie pour sécuriser davantage les systèmes gouvernementaux, le gouvernement du Canada a fait des investissements ciblés afin d'améliorer les mesures de sécurité sur les réseaux fédéraux, réduit le nombre de points d'accès Internet et apporté des modifications à la Politique sur la sécurité du gouvernement.

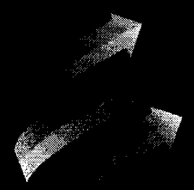
SP dirige les efforts fédéraux visant à établir des partenariats avec d'autres ordres de gouvernement et le secteur privé pour faire en sorte que l'intégrité de l'information et des services soit maintenue. Nous avons renforcé notre relation avec les partenaires établis, nous travaillons à établir des contacts avec d'autres secteurs et nous renforçons notre capacité technique et opérationnelle afin

d'améliorer les conseils et le soutien que nous apportons à nos intervenants. Par exemple, en octobre 2012, le ministre de la Sécurité publique a annoncé la publication du Plan d'action sur la cybersécurité avec le département de la Sécurité intérieure des États-Unis, qui vise à améliorer :

- la collaboration sur le plan opérationnel entre les centres nationaux des opérations de cybernétique;
- l'engagement conjoint et l'échange d'information en matière de cybersécurité avec le secteur privé;
- la collaboration en ce qui a trait aux activités de sensibilisation du public à la cybersécurité.

Le Ministère dirige les efforts déployés pour aider les Canadiens à se protéger en ligne par l'entremise d'activités, notamment la sensibilisation accrue du public dans le cadre de la campagne Pensez cybersécurité.

PERSONNES-RESSOURCES : Rédigé par : Robert Dick Directeur général Direction de la cybersécurité nationale	Numéro de téléphone 613-990-2661	Approuvé par le DG Robert Dick Directeur général Direction de la cybersécurité nationale	Numéro de téléphone 613-990-2661



Perimeter Security and Economic Competitiveness

Sécurité du périmètre et compétitivité économique

Cybersecurity Action Plan

Between Public Safety Canada and the Department of Homeland Security

Public Safety Canada

Sécurité publique Canada

CYBERSECURITY ACTION PLAN BETWEEN PUBLIC SAFETY CANADA AND THE DEPARTMENT OF HOMELAND SECURITY

INTRODUCTION

Public Safety (PS) Canada and the Department of Homeland Security (DHS) are pursuing a coordinated approach to enhance the resiliency of our cyber infrastructure. The Cybersecurity Action Plan (the Action Plan) between PS and DHS seeks to enhance the cybersecurity of our nations through increased integration of PS' and DHS' respective national cybersecurity activities and improved collaboration with the private sector. This Action Plan represents just one of many important efforts between Canada and the United States to deepen our already strong bilateral cybersecurity cooperation.

As the Internet knows no borders, all countries have a responsibility to prevent, respond to, and recover from cyber disruptions and to make cyberspace safer for all citizens across the globe. Due to a shared physical border, Canada and the United States have an additional mutual interest in partnering to protect our shared infrastructure. This Action Plan aims to articulate a shared approach to fulfill PS' and DHS' vision of working together to defend and protect our use of cyberspace and to strengthen the resiliency of our nations. These efforts, combined, advance the objectives articulated by President Obama and Prime Minister Harper in the February 2011 declaration, *Beyond the Border: A Vision for Perimeter Security and Economic Competitiveness.*

This Action Plan outlines three goals for improved engagement, collaboration, and information sharing at the operational and strategic levels, with the private sector, and in public awareness activities, for activities conducted by PS and DHS. The Action Plan establishes lines of communication and areas for collaborative work critical to enhancing the cybersecurity preparedness of both nations. The Action Plan's goals and objectives are to be conducted in accordance with the June 2012 *Statement of Privacy Principles by the United States and Canada*. This Action Plan is intended to remain a living document to be reviewed on a regular basis and updated as needed to support new requirements that align to the Plan's key goals and objectives. It intends to support and inform current and future efforts to advance the goals of *Beyond the Border*, which ultimately seeks to enhance broad bilateral cooperation on cybersecurity efforts across both governments.

GOALS AND OBJECTIVES

1. Enhanced Cyber Incident Management Collaboration between National Cybersecurity Operations Centers

PS' Canadian Cyber Incident Response Centre intends to work jointly with DHS' United States Computer Emergency Readiness Team and Industrial Control Systems Cyber Emergency Response Team towards the following objectives:

1.1 Increase real-time collaboration between analysts by improving existing channels for remote communication and arranging in-person visits;

1.2 Enhance information sharing at all classification levels and collaborate on training opportunities, while promoting inter-agency coordination, as appropriate, as well as the proper protections for information, as outlined in the *Statement of Privacy Principles*;

1.3 Coordinate on cybersecurity incident response management, relating to defense, mitigation, and remediation activities and products, including with other public and private entities consistent with each country's laws and policies;

1.4 Align and standardize cyber incident management processes and escalation procedures; and

1.5 Enhance technical and operational information sharing in the area of industrial control systems security.

2. Joint Engagement and Information Sharing with the Private Sector on Cybersecurity

Due to the shared nature of critical infrastructure between Canada and the United States, PS and DHS intend to collaborate on cybersecurity-focused private-sector engagement for cybersecurity activities for which they are responsible through the following objectives:

2.1 Share engagement approaches for private sector;

2.2 Exchange and collaborate on the development of briefing materials for the private sector;

2.3 Jointly conduct private sector briefings;

2.4 Review approaches and align processes for private sector engagement through requests for technical assistance and non-disclosure agreements; and

2.5 Standardize protocols for sharing information.

3. Continued Cooperation on Ongoing Cybersecurity Public Awareness Efforts

Cybersecurity is a shared responsibility and everyone, including our citizens, has a role to play. With increased media attention devoted to cybersecurity incidents and with the continuing growth of electronic commerce and social media, it is imperative that citizens receive clear and trustworthy information on how to manage cyber threats to themselves and their families. Ensuring that government's cybersecurity awareness messages are consistent across our border helps to deliver that information effectively and consistently. PS Communications, the DHS Office of Public Affairs, and the National Protection and Program Directorate's Office of Cybersecurity and Communications (CS&C) intend to continue to work together as they:

3.1 Collaborate on public awareness campaigns (websites, social media activities, education material, etc.);

3.2 Collaborate on Cybersecurity Awareness Month (October); and

3.3 Share and coordinate messaging on issues of common interest.

GOVERNANCE OF THE JOINT ACTION PLAN

Senior officials within PS and CS&C intend to review and provide additional guidance in order to update this Action Plan on a quarterly basis. This Action Plan is intended to be a part of broader inter-governmental coordination across government agencies in both the United States and Canada.

CYBER SECURITY

PROPOSED RESPONSE:

- **The Government released *Canada's Cyber Security Strategy* in 2010 as a clear statement of the priority we place on protecting our citizens, our businesses, and our critical infrastructure from online threats. The Government continues to deliver on its commitments as laid out in the Strategy.**

- **Because the Strategy envisions coordinated action across government, a number of federal departments and agencies have been actively working to implement their respective elements. For instance, Industry Canada has established Canada's Spam Reporting Centre through our Government's Anti-Spam Legislation. Federal departments and agencies continue to strengthen the security of federal systems and deliver programs and benefits to Canadians.**

- **Among the concrete benefits the Strategy is providing is the Canadian Cyber Incident Response Centre (CCIRC), which is on the frontline in protecting our critical infrastructure from cyber threats. CCIRC monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with specific cyber threats.**

- **The Government is also raising awareness directly with citizens through *Get Cyber Safe* campaign, which provides a trusted source of information about online risks and provides concrete advice on how Canadians can better protect themselves online.**

QUESTIONS AND ANSWERS:

Q1. What progress has been made to date in implementing *Canada's Cyber Security Strategy*?

A1. Federal departments and agencies have been undertaking activities to implement each of the three pillars of the Strategy, which include strengthening Government of Canada systems and networks, partnering to secure vital networks and systems outside of the federal Government, and helping Canadians be secure online.

In its efforts to further secure Government systems, the Government of Canada has made targeted investments to augment security measures on federal networks, complemented by a reduction of Internet access points and amendments to the Policy on Government Security. The Government of Canada has also announced the creation of Shared Services Canada, which will better protect federal government systems and the information they carry. Government will switch to one email system, reduce the overall number of data centres, and streamline our electronic network. Not only will this make our networks more secure, it will save money and improve services to Canadians.

Public Safety Canada continues to lead federal efforts to partner with other levels of government within Canada and critical infrastructure sectors to ensure that the integrity, availability, and confidentiality of information and services, is maintained. Federal efforts to help Canadians be secure online include a range of activities such as increasing public awareness and increasing the ability and capacity of the national law enforcement community to tackle cybercrime in Canada.

Q2. What is the Government of Canada doing to protect systems that are the responsibility of provincial and territorial governments or the private sector?

A2. The Government of Canada is partnering with other levels of government and critical infrastructure sectors to identify cyber threats, provide advice on mitigation measures and establish information sharing mechanisms and arrangements. By facilitating the sharing of threat information and identifying the needs of the critical infrastructure community, the Government of Canada will be able to best leverage its resources and ensure that other levels of government and critical infrastructure sectors are getting the information they need, when they need it.

Q3. How does the Strategy help me if my computer becomes infected, hacked or compromised?

A3. Through its *Get Cyber Safe* public awareness campaign, the Government has helped Canadians better understand cyber threats and the tools available to recognize and avoid them. The Government's ultimate goal is to create a culture of cyber security whereby Canadians are aware of both the threats and the actions they can take to ensure the safe use of cyberspace.

Q4. What else is the government doing in addition to the Strategy to ensure that Canadian interests are protected online?

A4. Recognizing the borderless nature of cyberspace, the Government of Canada continues to work actively with allies to advance cyber security issues. For example, as noted in the *Shared Vision for Perimeter Security and Economic Competitiveness*, Canada is working with the United States to both expand joint leadership on international cyber security efforts and strengthen cyber security to protect vital government and critical digital infrastructure of bi-national importance. Canada is also active at international organizations considering Internet issues. At these venues the Government of Canada continues to promote Canada's interests on such issues as Internet governance, and criminal and state sponsored malicious activity online.

Q4. Is *Canada's Cyber Security Strategy* related to Bill C-30, Protecting Children from Internet Predators Act?

A4. While Bill C-30 is not one of the direct commitments within *Canada's Cyber Security Strategy*, several provisions within the proposed legislation will enable Canada to move forward with essential cyber security measures, such as ratifying the international Budapest Convention on Cyber Crime.

CONTACTS:			
Prepared by Robert Dick, Director General, National Cyber Security Directorate	Tel. no. 613-990-2661	Approved by (ADM level only) Lynda Clairmont, Senior Assistant Deputy Minister, National Security Branch	Tel. no. 613-990-4976

Pages 372 to / à 377

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

UNCLASSIFIED

DATE:

File No.:
RDIMS No.: 750580

MEMORANDUM FOR THE DEPUTY MINISTER

MEETING WITH GENERAL THOMAS J. LAWSON
CHIEF OF DEFENCE STAFF, CANADIAN FORCES

(For information)

ISSUE

You are scheduled to meet with General Thomas J. Lawson, Chief of Defence Staff of the Canadian Forces, on January 8, 2013.

BACKGROUND

Public Safety Canada (PS) is the lead department for *Canada's Cyber Security Strategy* (the Strategy). The Strategy received an initial $90 million over five years, with a further $155 million announced in 2012, to secure federal networks.

Under the Strategy, the Canadian Forces (CF) and the Department of National Defence (DND) are tasked with strengthening their capacity to defend their own networks, and with working with other Government departments to identify threats and possible responses, principally through the office of the Chief of Defence Intelligence. DND and the CF are also directed to work with allies to develop the policy and legal framework for military aspects of cyber security, in partnership with the Department of Foreign Affairs and International Trade Canada (DFAIT).

No direct funding was allocated to either the DND or CF in the Strategy, although Defence Research Development Canada was allocated $200,000 per year for science and technology development.

The CF has established a Cyber Task Force that is exploring operational aspects of cyber security in a military setting. The Canadian Forces Network Operations Centre, based at Canadian Forces Station Leitrim, just south of Ottawa, operates as the network defence and incident response unit for Defence networks. General Lawson participates as a member of the Deputy Ministers' Committee on Cyber, and the CF have recently

.../2

established a new one-star general position to serve as Director General Cyber. This position is currently held by Brigadier-General Greg Loos.

CONSIDERATIONS

PS and DND/CF have good working relationships on cyber security, centred principally in the civilian led Policy Group of DND. There was seamless cooperation in crafting national input for the development of the 2011 North Atlantic Treaty Organization (NATO) Policy on Cyber Defence, and NATO's subsequent Cyber Defence Action Plan. DND/CF have been proactive in engaging PS on initial drafts of a CF policy on cyber operations, and staff from the Judge Advocate General Office provided outstanding legal advice to the PS and DFAIT led delegation to the United Nations Group of Governmental experts meeting on cyber security in August 2012.

The role of the military in delivering cyber security has, to date, not been the subject of much debate in Canada. However, the American military is increasingly expanding its mandate to include direct defence and monitoring of some civilian networks within the United States (U.S.), direct sharing of military intelligence with some critical infrastructure partners, and even, potentially, the use of military assets to respond to cyber attacks on civilian systems.

Given the close operational history of the American military and the CF, some in the U.S. may erroneously assume the CF will adopt a similar posture in Canada. PS will continue to work with DND and with the full range of respective American counterparts to ensure that all are aware of respective roles and mandates.

Should you require additional information, please do not hesitate to contact me, Acting Director General, National Cyber Security, 613-990-2661.

Mr. Sébastien Labelle
Acting Director General
National Cyber Security

s.21(1)(b)

Enclosures: (1)

Prepared by: Corey Dvorkin

KEY MESSAGES

MEETING WITH GENERAL THOMAS J. LAWSON
CHIEF OF DEFENCE STAFF, CANADIAN FORCES

- Cyber security is one of the most complex challenges we face, and I am pleased with the strength of cooperation between our Departments in addressing it.

- We each have very specific roles to play in cyber security, but can certainly benefit from outside support.

- Managing our relationships is key to success on this file. We have been following how the United States military is taking a larger more active role in cybersecurity domestically.

- To avoid creating stress in our continental relationship, we will need to be transparent in managing expectations from our American counterparts, and ensure they clearly understand our domestic roles and missions.

Public Safety Canada / Sécurité publique Canada

Senior Assistant Deputy Minister / Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

For your meeting with:
Deputy Ministers Committee on Cyber Security
On: January 12, 2012

2012 JAN -9

SECRET – with attachments

DATE: JAN 0 9 2012

File No.: 384918
RDIMS No.: 537473

Seen by the DM
Vu par le SM

JAN 1 2 2012

MEMORANDUM FOR THE DEPUTY MINISTER

DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

(Information only)

ISSUE

You will be chairing the inaugural meeting of the Deputy Ministers Committee on Cyber Security (DM Cyber), which is scheduled to take place on January 12, 2012.

A briefing binder with necessary background information and proposed speaking points is enclosed for your convenience.

BACKGROUND

As you will recall, DMs and their representatives expressed a need for greater governance on cyber security at a November 8, 2011 meeting with the National Security Advisor (NSA) to the Prime Minister and officials from the Canadian Security Intelligence Service, the Communications Security Establishment Canada (CSEC), the Department of National Defence and Public Safety Canada.

It was agreed that the inaugural meeting of DM Cyber would take place in mid-December 2011; however, this meeting was postponed to January 12, 2012. The Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber) met on December 5, 2011, to review the draft DM Cyber agenda and prepare for the meeting.

CURRENT STATUS

At the inaugural DM Cyber meeting, it is proposed that DMs consider five main agenda items.

As this will be the first meeting of DM Cyber, and given that several participants were not at previous meetings with the NSA, the primary objective will be to seek agreement on the membership and terms of reference of the Committee. This item, the first on the agenda, is for decision.

Canada

Responding to requests made at the previous meeting of DMs, two items are on the agenda for information. The Treasury Board of Canada Secretariat will speak to network hygiene in the Government by describing the challenge in protecting Government systems, work undertaken in this area to date, and planned work going forward. I will then present on roles and responsibilities of departments with respect to cyber security.

Finally, there are two additional items for information.

Second, you could brief on the January 23, 2012 meeting of Federal/Provincial/Territorial Clerks, at which cyber will be discussed.

NEXT STEPS

Since DMs agreed to meet quarterly, the next DM Cyber will be scheduled in late March or early April 2012. ADM Cyber and the Directors General Committee on Cyber Security will meet monthly to support the efforts of DM Cyber.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure: (1)

s.15(1) - Int'l

Prepared by: Melanie Mohammed

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

Deputy Ministers Committee on Cyber Security

January 12, 2012 – 14:00 to 15:00
19th floor boardroom, 269 Laurier Avenue West

AGENDA

	Time	Item	Associated Documentation
1.	14:00 *5 min*	**Opening Remarks** William Baker, Deputy Minister, Public Safety	N/A
2.	14:05 *5 min*	**Deputy Ministers Committee on Cyber Security** William Baker, Deputy Minister, Public Safety *For decision: Agree upon the proposed role and scope of the Committee; and discuss Committee forward agenda.*	Draft Terms of Reference
3.	14:10 *20 min*	**Network Hygiene** Michelle D'Auray, Secretary of the Treasury Board, Treasury Board of Canada Secretariat *For information: Provide an aperçu of the challenges in protecting Government IT systems, the actions taken to date, and forward work.*	Deck: Cyber Security – the Challenge in Protecting Government Systems
4.	14:30 *10 min*	**Cyber Security Roles and Responsibilities** Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada *For information: Provide an overview of the roles and responsibilities of cyber security lead departments.*	Roles and responsibilities dashboard
5.	14:40 *5 min*	Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada *For information:* [redacted]	[redacted]
6.	14:45 *5 min*	**FPT Clerks Meeting, January 23, 2012** William Baker, Deputy Minister, Public Safety *For discussion: Seek views on the strategic objectives for the meeting.*	Deck: FPT Clerks Meeting
7.	14:50 *10 min*	**Roundtable**	N/A

s.15(1) - Int'l

Comité des sous-ministres sur la cybersécurité

Le 12 janvier 2012 – 14h00 à 15h00
Salle de conférence au 19e étage du 269, avenue Laurier ouest

ORDRE DU JOUR

	Heure	Item	Documentation connexe
1.	14h00 *5 min*	**Mot de bienvenue** William Baker, sous-ministre, sécurité publique	S/O
2.	14h05 *5 min*	**Comité des sous-ministres sur la cybersécurité** William Baker, sous-ministre, sécurité publique *Pour approbation : S'accorder sur le rôle et la portée du comité; et discuter du programme d'activités à long terme.*	Stipulations proposées
3.	14h10 *20 min*	**L'hygiène des réseaux** Michelle D'Auray, secrétaire du Conseil du Trésor, Secrétariat du Conseil du Trésor du Canada *Pour information : Donner un aperçu du défi quant à la protection des systèmes gouvernementaux, des efforts actuels et des initiatives à venir.*	Présentation : Le défi quant à la protection des systèmes gouvernementaux
4.	14h30 *10 min*	**Rôles et responsabilités en cybersécurité** Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, sécurité publique *Pour information : Donner une vue d'ensemble des rôles et responsabilités des ministères principaux en matière de la cybersécurité.*	Tableau de bord sur les rôles et responsabilités
5.	14h40 *5 min*	[redacted] Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, sécurité publique *Pour information :* [redacted]	[redacted]
6.	14h45 *5 min*	**Réunion des greffiers FPT, le 23 janvier 2012** William Baker, sous-ministre, sécurité publique *Pour discussion : Recherche des commentaires sur les objectives stratégiques pour la réunion.*	Présentation : Réunion des greffiers FPT
7.	14h50 *10 min*	**Tour de table**	S/O

s.15(1) - Int'l

1. OPENING REMARKS

- Bonjour tout le monde, et bienvenue à notre première réunion.
  - *Good afternoon everyone, and welcome to our first meeting.*

- Since this is our first meeting, and since several around the table were not at previous related meetings with the National Security Advisor, today's primary objective will be to set the stage for future work. Our first item of discussion will be to agree on the Committee's terms of reference and membership.

- Next, there are two information items intended to provide us with the necessary knowledge to help us contextualize future discussion. The first item today will be on network hygiene, which Michelle (D'Auray) will brief on given her responsibility for the Chief Information Officer Branch.

- For the second item, a higher-level overview of roles and responsibilities across the federal government, I've asked Lynda Clairmont to present, given her responsibility as lead Senior Assistant Deputy Minister for *Canada's Cyber Security Strategy*.

- I would invite each of you to identify future topics on which you would like to brief this Committee, or be briefed.

- Finally, there are two transactional items on which it is timely that we be briefed. [redacted] Last, I will speak to the January 23, 2012 meeting of the Federal-Provincial-Territorial Clerks, at which cyber will be discussed.

- A final note: a template has been circulated to your departments seeking input on the forward agenda for this Committee, so you'll have an opportunity to shape that by talking to your ADMs.

s.15(1) - Int'l

2. DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

PROPOSED TALKING POINTS

- I'd like to take a couple of minutes to outline the draft terms of reference and membership for this Committee, formally known as the Deputy Ministers Committee on Cyber Security (DM Cyber), and seek any comments that you may have with respect to what is proposed.

- DM Cyber will guide the overall policy direction and set priorities for forward work. We will also be monitoring progress on the implementation of *Canada's Cyber Security Strategy*, and our meetings will serve as a venue for considering emerging issues. We would not be an operational committee – crisis management mechanisms already exist.

- The Directors General Committee on Cyber Security (DG Cyber) met in late November 2011 to discuss the membership of DM Cyber. That group recommended that the Department of Foreign Affairs and International Trade be added to the membership list for DM Cyber and we have done so.

- At the December 2011 meeting of the Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber), Public Works and Government Services Canada (PWGSC) also indicated potential interest given its roles to protect Government's sensitive information provided through contract to industries within Canada and abroad; however, it was agreed that they would postpone joining our meetings until a future date.

- In the interim, I believe it would be beneficial that Shared Services Canada keep PWGSC apprised of issues that may require their attention.

- I want to underscore that should issues touch on the roles, responsibilities and mandates of other departments, implicated Deputy Heads would be invited to attend our meetings.

- We are proposing that DM Cyber meet on a quarterly basis, with additional meetings, if necessary, to consider urgent issues.

- My Department is also developing a draft forward agenda. Input is being sought from DG and ADM Cyber member departments, and I hope to have a version ready for your review by our next meeting.

ISSUE

You will lead a discussion on the draft terms of reference and membership for the Deputy Ministers Committee on Cyber Security (DM Cyber). **You** will also speak to the development of a draft forward agenda that will be presented at a future meeting.

Draft terms of reference and membership for DM Cyber were distributed to participants in advance of the meeting, and are enclosed for your ease of reference.

CURRENT STATUS

Terms of reference
Public Safety Canada has developed draft terms of reference and a proposed membership for DM Cyber. The terms of reference indicate that the purpose of the Committee is to:

- establish policy direction;
- set priorities;
- monitor the implementation of *Canada's Cyber Security Strategy*; and
- consider emerging issues.

Membership
During the November 30, 2011 meeting of the Directors General Committee on Cyber Security (DG Cyber), the Department of Foreign Affairs and International Trade (DFAIT) indicated that their DM was interested in participating on DM Cyber.

DG Cyber supported this request given international focus, DFAIT's role, and broader policy linkages that would benefit from a greater awareness on the part of the DM of Foreign Affairs to cyber security concerns.

Public Works and Government Services Canada (PWGSC) also indicated that they were interested in having their Deputy participate on DM Cyber given the Department's mandate to protect Government's sensitive information provided through contracts to industries within Canada and abroad. At the December 5, 2011 meeting of ADM Cyber, however, it was agreed that PWGSC would consider joining DM Cyber at a future date. In the interim, it was deemed to be preferable that Shared Services Canada keep PWGSC apprised of issues that may require their attention.

It will be important to underscore that should issues touch on the roles, responsibilities and mandates of other departments, other Deputy Heads would of course be invited to attend.

Forward agenda
Information presented in the forward agenda will show alignment of activities with domestic priorities, and will provide information regarding efforts underway to advance objectives.

A template was circulated during the week of December 16, 2011, to DG and ADM Cyber member departments. Input is expected in early 2012, and will be refined at the DG and ADM levels before being presented at the next DM Cyber meeting.

Prepared by: Melanie Mohammed
Approved by: Corey Dvorkin

Deputy Ministers Committee on Cyber Security

Terms of Reference

[redacted]

The purpose of the Deputy Ministers Committee on Cyber Security (DM Cyber) is to:

- establish policy direction;
- set priorities;
- monitor progress on the implementation of *Canada's Cyber Security Strategy*; and
- consider emerging issues.

[redacted]

- Chair and Secretariat:
  - Deputy Minister, Public Safety Canada

- Core members:
  - Director, Canadian Security Intelligence Service
  - Commissioner, Royal Canadian Mounted Police
  - Deputy Minister, National Defence
  - Chief of Defence Staff, Canadian Forces
  - Chief, Communications Security Establishment Canada
  - Deputy Minister, Foreign Affairs
  - Deputy Minister, Industry Canada
  - Deputy Minister and Deputy Attorney General of Canada, Department of Justice Canada
  - National Security Advisor to the Prime Minister, Privy Council Office
  - President, Shared Services Canada
  - Secretary of the Treasury Board, Treasury Board of Canada Secretariat

[redacted]

DM Cyber is supported by the Assistant Deputy Ministers' Committee on Cyber Security, which is supported by the Directors General Committee on Cyber Security.

[redacted]

DM Cyber will meet quarterly, with *ad hoc* meetings called by the Chair as required.

Comité des sous-ministres sur la cybersécurité

Mandat

Le Comité des sous-ministres sur la cybersécurité vise à :

- orienter les politiques;
- établir les priorités;
- surveiller les progrès relatifs à la mise en œuvre de la *Stratégie de cybersécurité du Canada*;
- examiner les problèmes qui surviennent.

- Présidence et secrétariat :
  - Sous-ministre, Sécurité publique Canada

- Membres principaux :
  - Directeur, Service canadien du renseignement de sécurité
  - Commissaire, Gendarmerie royale du Canada
  - Sous-ministre, Défense nationale
  - Chef d'état-major de la Défense, Forces canadiennes
  - Chef, Centre de la sécurité des télécommunications du Canada
  - Sous-ministre, ministère des Affaires étrangères
  - Sous-ministre, Industrie Canada
  - Sous-ministre et sous-procureur général du Canada, Justice Canada
  - Conseiller national pour la sécurité auprès du premier ministre, Bureau du Conseil privé;
  - Président, Services partagés Canada
  - Secrétaire du Conseil du Trésor, Secrétariat du Conseil du Trésor

Le Comité des SM est appuyé par le Comité des sous-ministres adjoints sur la cybersécurité, lui-même appuyé par le Comité des directeurs généraux sur la cybersécurité.

Le Comité des SM se réunira sur une base trimestrielle; le président pourra organiser des réunions au besoin.

3. NETWORK HYGIENE

PROPOSED TALKING POINTS

- At the November 8, 2011 meeting, some of our colleagues expressed interest in learning more about network hygiene and how best to advance it in Government. This is a fundamental cyber security issue.

- The Treasury Board of Canada Secretariat has drafted a deck, and I invite them to walk us through it.

During discussion

- Given that this is a long-term goal, does our current approach respond directly enough to the evolving threat environment? If we had to move faster, could we?

- Is there more we need to do to manage our network hygiene while we undertake the consolidation of our systems? Can we provide a clearer framework to departments, or specific guidelines to Deputies?

- Can we work more collaboratively to expedite this process?

ISSUE

You will introduce this agenda item. Treasury Board of Canada Secretariat (TBS) will present for discussion a deck they have prepared with input from the Communications Security Establishment Canada (CSEC).

The deck was distributed to participants in advance of the meeting, and is enclosed for your ease of reference.

BACKGROUND

Network hygiene refers to regularly performing the "bread and butter" activities of network and information technology (IT) security, such as upgrades and patch maintenance. It is well recognized that disciplined network hygiene makes a significant

difference in security, but that it can also be onerous and time-consuming for IT staff given other operational priorities.

Shared Services Canada (SSC) will centralize the governance of Government IT, which should simplify the maintenance of uniform network hygiene. This transition will evolve over years, during which time discipline will still be required across the decentralized IT infrastructure.

CURRENT STATUS

TBS, CSEC and SSC are recommending the increased consolidation of Government networks to ensure that all departments are operating in the same environment. (

This number has been reduced by one third since 2009.

The creation of SSC will continue to advance this endeavour; however, consolidation alone will not resolve all of Government's IT or cyber security issues, and other steps are also underway.

TBS is also assessing departmental IT security compliance via the Management Accountability Framework to hold each Deputy Head accountable for their department's level of compliance.

NEXT STEPS

Government departments implicated in *Canada's Cyber Security Strategy*, principally TBS, CSEC, SSC and Public Safety Canada (PS), will continue to promote awareness of IT security practices among Deputy Heads and in other fora within and outside Government.

TBS and SSC will continue to redesign the enterprise IT security model to ensure that IT security is built in to the architecture, rather than added as an afterthought.

Finally, TBS and SSC are working to establish a Government of Canada Incident Recovery Team (IRT). The IRT would provide IT incident recovery services to Government departments and agencies with a view to reducing recovery time and ensuring comprehensive and lasting solutions.

s.15(1) - Def

CONCLUSION

To ensure that network hygiene is effective, a simplified and more cohesive network infrastructure needs to be implemented across Government. TBS, CSEC and SSC are working to reduce complexity, increase IT homogeneity, and reduce the footprint of Government IT infrastructure.

Prepared by: Melanie Mohammed
Approved by: Adam Hatfield

Cyber Security

The Challenge in Protecting Government Systems

Canada

SECRET

Agenda

- Threat Landscape
- What we have done to date
- The Way Ahead
- Conclusions

SECRET

Cyber Threat Landscape

Opportunistic

SIMPLE

SOPHISTICATED

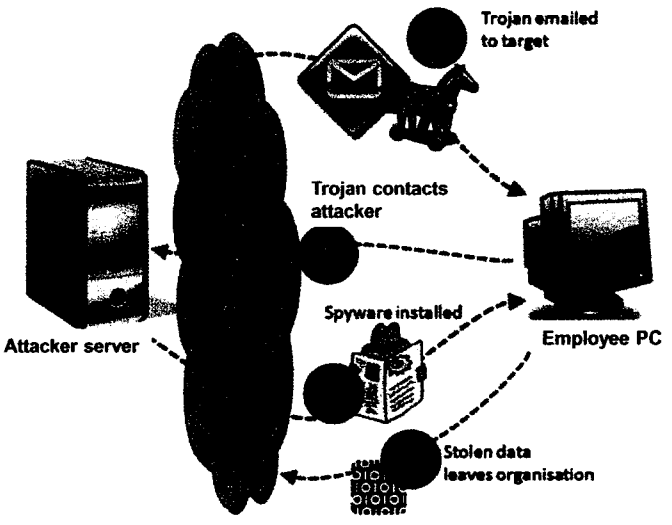
Planned

- Hackers and Hacktivists
  - Motivation: Social/political
  - Target: Organizations promoting political and/or societal positions
  - Methods: Website defacement, denial of service
  - Techniques: Exploitation of common software vulnerabilities
- Criminals
  - Motivation: Profit
  - Target: Canadian citizens, retailers, financial sector
  - Methods: Social engineering to send malicious emails to groups of people, exploitation of common software vulnerabilities, establishment of fake websites
- State Sponsored
  - Motivation: Political, military, economic advantage
  - Target: Government, academia, industry, critical infrastructure
  - Methods: Exploitation of non-public software vulnerabilities, targeted social engineering of individuals, tampering with products during manufacture to build in vulnerabilities or malicious code

3

SECRET

Typical Attack Scenario



4

SECRET

Cyber Defence is a Challenge

- IT security is not implemented in a systemic, coordinated fashion at the enterprise level – uncoordinated evolution, various level of services, disperse operation, multiple authorities and accountabilities
- People are also targets - it can be hard for a user to detect malicious emails
  - Adversaries use social engineering techniques to trick people into believing the malicious email or attachment is valid and important to them
- Sophisticated attackers constantly probe and persist until they succeed, exploiting any weaknesses in our defences, scaling from most common and well known vulnerability to the most complex methods and non-public vulnerability.
  - Constantly harvesting data (network and human behaviour) for future exploitation.
  - Successfully implementing top "x" mitigations is not enough

5

SECRET

Government IT Systems Complexity and Diversity

- The GC IT infrastructure has been cobbled together over time without an overarching plan:
  - Networks of networks: over 3000 overlapping networks
    - Unique security requirements, in some cases accountable to other international partners
  - Data centers: over 300 data centers
  - Mid-range servers: over 25,000
    - Wide range of vendors, platforms (MS, Unix, Linux)
    - 30% simple, 40% web or mail, 30% complex apps & databases
  - Applications: over 16,000 business applications
    - Aging/legacy apps; some 45 years old
  - Desktops: wide range of OS currently in service; from Windows 95 on, Unix family, Linux, etc
  - [redacted]

[redacted]

6

s.15(1) - Subv

SECRET

What We Have Done To Date

- TBS Assessing IT Security compliance via MAF (2006)
  - Improvements in compliance
  - Awareness including basic network hygiene practices
- TBS leading the Consolidation of Internet Access Points
  - Reduced by one third since 2009
  - TBS has clearly defined acceptable / not acceptable configurations (2011 shows 80% acceptable)
  - Allows for cost-effective deployment of defence solutions
- [redacted]
  - [redacted]
  - [redacted]

s.15(1) - Subv

7

SECRET

Moving Forward

TBS continues to champion initiatives that support IT infrastructure consolidation and rationalization

- Creation of SSC
  - Game changer: significant impact on our consolidation effort
  - Consolidating and standardizing Enterprise IT Architecture
  - Increasing operational excellence at the enterprise level
  - Standing up a Gov-CIRT at SSC
- Enterprise-wide secret network
- Application Consolidation Strategy
- End User Device Strategy
  - Desktop rationalization Ex. HRSDC Cluster
    - HRSDC, DFO, AGAF/CFIA, IC *(SSC & HC as observers)*
    - 61,700 seats and over 100,000 devices
    - Moving to Windows 7, Internet Explorer 8, Office 2010
- Security awareness: changing behaviour

8

SECRET

Consolidation is a Prerequisite for Sustainable Network Hygiene

- Government must defend against the full spectrum of cyber threats, including the most sophisticated
- GC IT infrastructure is complex, massive, heterogeneous, and still teeming with legacy systems
- Implementing the simplest security measure is an operational and technical challenge. A comprehensive security effort in such an environment is complex, risky and costly
- For network hygiene to be effective we need a simplified and more cohesive network infrastructure
- We are tackling the issue with initiatives that will reduce complexity, increase IT homogeneity, and reduce our infrastructure footprint
- Even with a simple, cohesive network, there must be ongoing efforts to ensure security-conscious behaviour by individuals and management

We will leverage current consolidation initiatives to build a cohesive, resilient and secure enterprise IT infrastructure

9

SECRET

ANNEX

10

SECRET

Network Hygiene – Top 10 Mitigating Actions*

1. Patch Operating systems in a timely manner
2. Patch applications (PDF viewer, browser, office applications)
3. Minimize use of administrator privileges
4. Application "whitelisting" to prevent malicious programs
5. Host-based intrusion detection/prevention system
6. Workstation inspection of Microsoft Office files
7. Whitelisted email content filtering to block malicious attachments
8. User education on Internet risks, social engineering
9. Ensure routing of internal traffic does not exit the network
10. Tools to help prevent malicious code from running

** Extracted from CSEC Top 35 Mitigation Actions*

Cybersécurité

Le défi associé à la protection des systèmes gouvernementaux

Canada

SECRET

Ordre du jour

- Disposition des menaces
- Ce que nous faisons
- La voie de l'avenir
- Conclusions

SECRET

Disposition des cybermenaces

Opportuniste

SIMPLE

SOPHISTIQUÉ

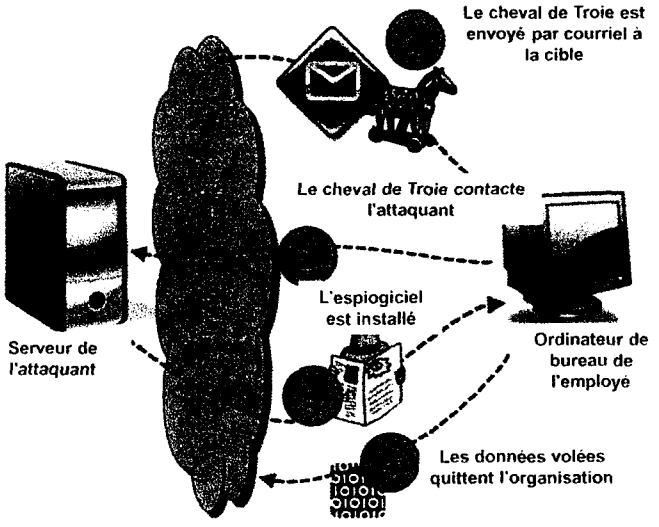
- Pirates informatiques et hacktivistes
  - Motivation : De nature sociale ou politique
  - Cibles : Organisations faisant la promotion des positions politiques ou sociales
  - Méthodes : Altération des sites Web, refus de service
  - Techniques : Exploitation des vulnérabilités communes des logiciels
- Criminels
  - Motivation : Profit
  - Cibles : Citoyens canadiens, détaillants, secteur financier
  - Méthodes : Ingénierie sociale envoyant des courriels malveillants aux groupes de personnes, exploitation des vulnérabilités communes des logiciels, création de faux sites Web
- Appuyé par l'État
  - Motivation : Avantage politique, militaire ou économique
  - Cibles : Gouvernement, milieu universitaire, industrie, infrastructure essentielle
  - Méthodes : Exploitation des vulnérabilités des logiciels non publics, ingénierie sociale ciblée des personnes, modification des produits au cours de la fabrication afin d'y intégrer des vulnérabilités ou un code malveillant

Prévu

3

SECRET

Scénario type d'attaques



4

SECRET

La cyberdéfense représente un défi

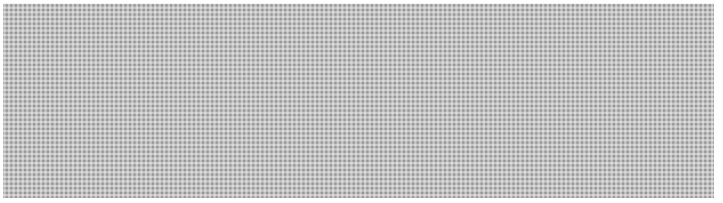
- La sécurité des TI n'est pas établie de manière systémique et coordonnée à l'échelle de l'entreprise – évolution non coordonnée, différents niveaux de services, activités disséminées, autorités et responsabilités multiples
- Les personnes sont également des cibles; il peut être difficile pour un utilisateur de détecter des courriels malveillants
  - Les adversaires emploient des techniques d'ingénierie sociale pour amener des personnes par la ruse à croire que le courriel ou la pièce jointe malveillant est valide et qu'il est important
- Les attaquants subtils examinent et persistent constamment jusqu'à ce qu'ils réussissent, en exploitant toute faiblesse dans nos défenses, allant des vulnérabilités les plus communes et les plus connues jusqu'aux méthodes les plus complexes et profitant des vulnérabilités non publiques.
  - Récolte constante des données (réseau et comportement humain) aux fins d'exploitation future
  - La mise en œuvre réussie des principales mesures d'atténuation « x » est insuffisante

5

SECRET

Complexité et diversité des systèmes de TI du gouvernement

- L'infrastructure de TI du gouvernement a été concoctée au fil du temps sans plan général :
  - *Réseaux de réseaux : il y plus de 3 000 réseaux qui se chevauchent.*
    - Des exigences uniques relatives à la sécurité qui, dans certains cas, rendent compte aux partenaires internationaux
  - Centres de données : plus de 300 centres de données
  - Serveurs moyens : plus de 25 000 serveurs
    - *Vaste éventail de fournisseurs, plateformes* (MS, Unix, Linux)
    - 30 % simple, 40 % par site Web ou par courriel, 30 % applications complexes et bases de données
  - Applications : plus de 16 000 applications d'entreprise
    - Applications vieillissantes/anciennes; certaines applications sont en place depuis 45 ans
  - Ordinateurs de bureau : un vaste éventail de systèmes d'exploitation est actuellement en service; à partir de Windows 95, famille Unix, Linux, etc.



6

s.15(1) - Subv

SECRET

Ce que nous avons fait à ce jour

- Évaluation de la conformité à la sécurité de la TI par l'entremise du CRG (2006)
  - Amélioration de la conformité
  - *Sensibilisation incluant les pratiques de base d'hygiène de réseau*
- Le SCT menant la consolidation des points d'accès Internet
  - Réduction d'un tiers depuis 2009
  - Le SCT a défini clairement les configurations acceptables et inacceptables (2011 montre que 80 % des configurations sont acceptables)
  - *.Permet le déploiement rentable des solutions de défense*
  - [redacted]
  - [redacted]

s.15(1) - Subv

7

SECRET

Aller de l'avant

Le SCT continue de défendre les initiatives qui soutiennent la consolidation et la rationalisation de l'infrastructure de la TI

- Création du SPC
  - Point tournant : une grande incidence sur nos efforts de regroupement
  - Regroupement et normalisation de l'architecture de TI d'entreprise
  - Hausse de l'excellence opérationnelle à l'échelle de l'entreprise
  - Création d'une équipe de réaction aux cyberincidents du gouvernement au SSC
- Réseau secret à l'échelle de l'entreprise
- Stratégie de regroupement des applications
- Stratégie pour le recours aux appareils des utilisateurs finaux
  - Rationalisation des postes de travail, p. ex. regroupement RHDCC
    - *RHDCC, MPO, AGAF/ACIA, IC (SSC et SC comme observateurs)*
    - 61 700 sièges et plus de 100 000 appareils
    - Passage à Windows 7, Internet Explorer 8, Microsoft Office 2010
- Sensibilisation à la sécurité : Modifier le comportement

8

SECRET

Le regroupement est un prérequis au bien-être durable de réseau

- Le gouvernement du Canada doit lutter contre tous les aspects de la cybermenace, y compris la menace la plus ingénieuse
- L'infrastructure de TI du gouvernement est complexe, massive et hétérogène et les anciens systèmes y abondent toujours
- La mise en œuvre de la mesure la plus simple représente un défi opérationnel et technique. Un effort global en matière de sécurité dans un tel environnement est complexe, risqué et coûteux
- Afin que le bien-être de réseau soit efficace, nous avons besoin d'une infrastructure de réseau simplifiée et plus cohérente
- Nous nous attaquons au problème par le truchement d'initiatives qui réduiront la complexité, augmenteront l'homogénéité de TI et réduiront l'empreinte de notre infrastructure
- Même avec un réseau simple et cohérent, il est nécessaire de déployer un effort soutenu afin de veiller à ce que les gens assument un comportement sécuritaire conscient, tant à l'échelle des employés que de la gestion

Nous tirerons profit des initiatives de regroupement actuelles afin de créer une infrastructure de TI d'entreprise cohérente, résiliente et sécuritaire

9

SECRET

ANNEXE

10

SECRET

Hygiène de réseau – 10 principales mesures d'atténuation*

1. Rapiécer rapidement les systèmes d'exploitation
2. Rapiécer les applications (visualiseur PDF, navigateur, applications bureautiques)
3. Minimiser l'utilisation des privilèges de l'administrateur
4. Application « liste blanche » pour prévenir les programmes malveillants
5. Système de détection et de prévention d'intrusion géré par le système central
6. Inspection du poste de travail des fichiers Microsoft Office
7. Filtrage du contenu des courriels de la liste blanche pour bloquer les pièces jointes malveillantes
8. Éducation des utilisateurs sur les risques de l'Internet, ingénierie social
9. Vérifier que l'acheminement de l'achalandage interne ne sort pas du réseau
10. Outils pour prévenir l'exécution du code malveillant

* *Extrait des 35 principales mesures d'atténuation du CSTC*

Rob (PCO)

4. CYBER SECURITY ROLES AND RESPONSIBILITIES

PROPOSED TALKING POINTS

- It's obviously critical that we have a shared understanding of who does what on cyber security.

- Lynda Clairmont, Senior Assistant Deputy Minister of National Security at Public Safety Canada, will give us a high-level overview of the key roles of federal departments and agencies.

ISSUE

You will introduce this item. Lynda Clairmont, Senior Assistant Deputy Minister of National Security at Public Safety Canada, will speak to the distribution of cyber security efforts across Government, with a view to informing Deputies on the roles and responsibilities of cyber security lead departments.

A roles and responsibilities dashboard was distributed to participants at the beginning of the meeting, and is enclosed for your ease of reference.

BACKGROUND

In November 2010, members of the Directors General Committee on Cyber Security (DG Cyber) provided Public Safety Canada with a slide that described their department's mandate as it relates to cyber security. In November 2011, departments were asked to update or validate their response. This information was categorized so as to be able to be presented visually.

Comments received at the late November and early December 2011 meetings of DG Cyber and the Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber) indicated a need to better describe the roles of departments in terms of cyber security, primarily with regard to the role of defence departments, and with regard to critical infrastructure protection. It was suggested that a dashboard may be more representative and accurate means of doing this.

CONSIDERATIONS

The roles and responsibilities of Government departments and agencies as presented in the *Government of Canada Information Technology Incident Management Plan* (GC IT IMP) are somewhat defined in terms of responding to a cyber incident affecting a Government network; however, owing to the launch of Shared Services Canada, this

mechanism needs to be revised. In the case of a cyber incident affecting a province or territory, critical infrastructure sector or private sector entity, however, roles, responsibilities and capabilities are more ambiguous.

A series of tabletop exercises beginning January 13, 2012, will help to provide the necessary clarity, and identify policy and operational barriers to information sharing. Additionally, these exercises will contribute to Public Safety Canada's initiative to establish a national cyber incident response framework. This framework would clarify the roles and responsibilities of Government, provincial and territorial partners, and private sector entities.

CONCLUSION

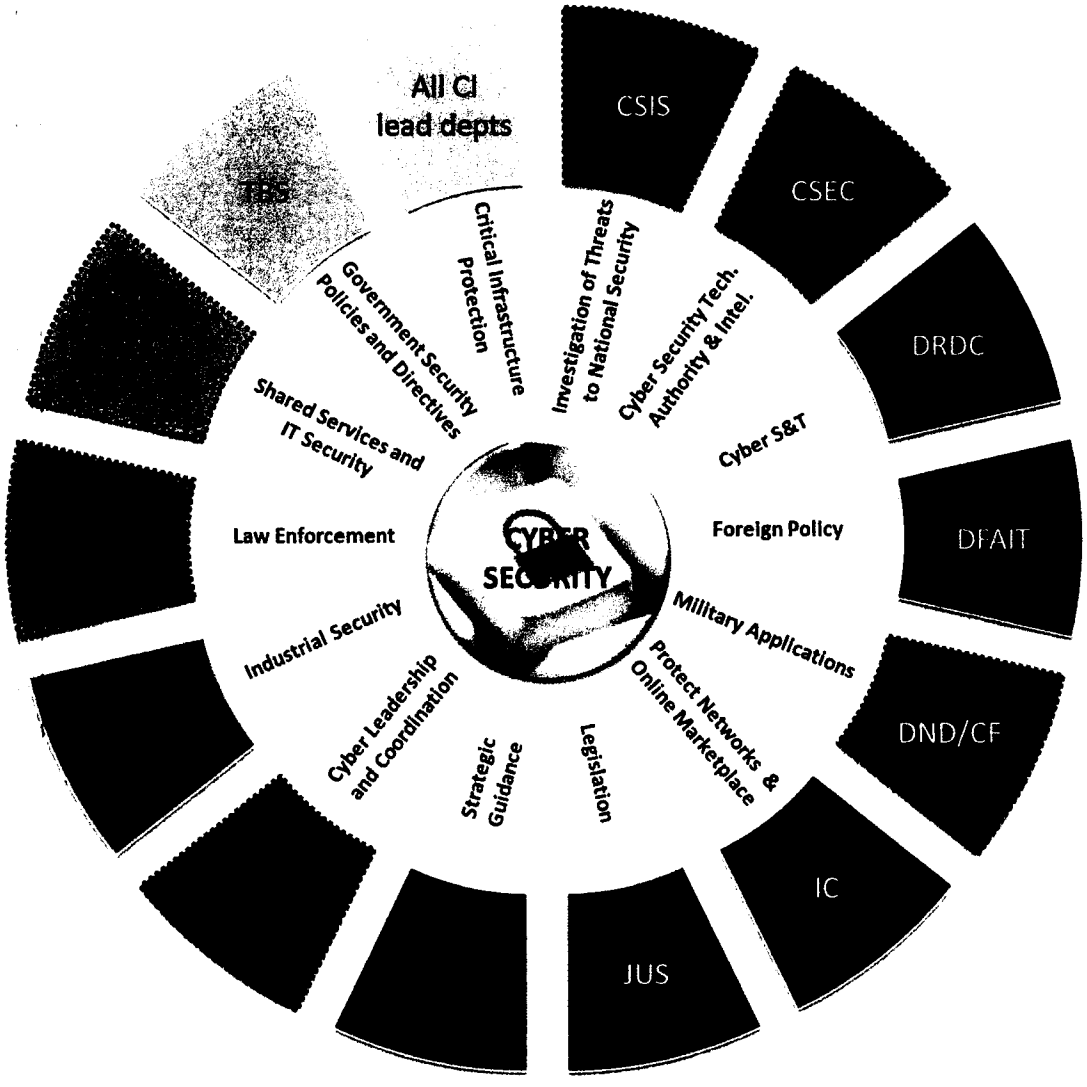
It is expected that the current dashboard, along with the exercises, will provide a better understanding of cyber security roles and responsibilities.

There is potential for synergy between Public Safety Canada efforts, and ongoing efforts by the Treasury Board of Canada Secretariat (TBS) to revise the GC IT IMP. We are open to coordinating with TBS so that one set of exercises could help inform our respective efforts.

Prepared by: Melanie Mohammed
Approved by: Corey Dvorkin and Adam Hatfield

s.15(1) - Int'l

Roles and responsibilities with respect to cyber security



Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

All critical infrastructure lead departments
Includes Finance Canada, Environment Canada, Health Canada, Transport Canada, Natural Resources Canada, Agriculture and Agri-Food Canada, and Public Safety Canada.

Treasury Board of Canada Secretariat
Establishes and oversees a whole-of-government approach to cyber security, including: setting government-wide direction and establishing priorities for securing government IT systems and networks; providing direction and advice to lead security agencies on the approach and implementation of measures for managing IT security incidents; and providing oversight of IT incident management, including post-mortem reviews and lessons learned.

Shared Services Canada
Streamlines and consolidates ICTs in the areas of email, data centres and networks, and for ensuring the confidentiality, integrity and availability of common IT services provided to departments.
Provides common information technology (IT) security services and other solutions to enable departments to exchange information with citizens, businesses and employees.
Gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to common IT services and Government IT critical infrastructure managed by Shared Services Canada, and communicates the information to the Canadian Cyber Incident Response Centre and, as authorized, to departments and cyber security partners.

Royal Canadian Mounted Police
Leads the criminal investigative response to suspected criminal cyber incidents involving critical information infrastructure (i.e., unauthorized use of computer and mischief in relation to data). Leads the investigative response to suspected criminal national security cyber incidents.
Assists domestic and international partners with advice and guidance on cyber crime threats.

Public Works and Government Services Canada
Provider of shared and common services. As part of its Industrial Security Program activity, ensures security in contracts awarded by the Department or when requested by other Government departments.
Ensures the protection of foreign and NATO classified information within the private sector in Canada.
The Industrial Security Sector maintains relationships with allies and negotiates Memoranda of Understanding on industrial security matters, including cyber security, in contracting.

Public Safety Canada
Leads and coordinates the implementation of *Canada's Cyber Security Strategy*, including the design of a whole-of-Government approach to performance measurement and reporting; engagement with provinces and territories, critical infrastructure, and international allies on strategic cyber security policy issues and national cyber incident management; and public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace.
The Canadian Cyber Incident Response Centre acts as Canada's national CERT (Computer Emergency Response Team) in providing assistance and mitigation advice to domestic partners and coordinating the national response to any cyber security incident.

Privy Council Office
Houses and provides support to the National Security Advisor to the Prime Minister.
Coordinates activities among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to national security issues.

Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

Communications Security Establishment Canada
Monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government through its sensor network, and provides mitigation and/or recovery advice and/or guidance to Government departments to help them recover from cyber incidents.
Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the Five Eyes cryptologic community. Undertakes classified research and development for cyber security.

Canadian Security Intelligence Service
Conducts national security investigations, reports to and advising the Government of Canada of activities constituting a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act*.
Provides analysis that will assist the Government of Canada in understanding cyber threats, the actors behind those threats, and overall situational awareness enabling the Government of Canada to better identify cyber vulnerabilities and take action to secure critical infrastructure, prevent cyber espionage or other related cyber threat activity.

Defence Research and Development Canada
Leads the development of military cyber security S&T in support of the Canadian Forces.
Leads domestic Public Safety Canada cyber security S&T efforts not specifically assigned to another department or agency through the Centre for Security Science and with domestic security partners in the Public Security Technical Program. This is delivered in partnership between Government, industry, academia and allies.

Department of Foreign Affairs and International Trade
Supports international bodies in mitigating cyber threats and assisting foreign governments in improving their cyber security profile and capabilities.
Contributes to diplomatic engagement in order to help shape the multilateral regulatory space that is emerging with respect to cyber security. Enables the Government to better position Canada on the international stage to defend and promote its foreign policy and cyber security-related interests.

Department of National Defence / Canadian Forces
Responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process.
Contributes to Government situational awareness during the monitoring and analysis, mitigation, and response phases of the *GC IT IMP* by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

Industry Canada
Responsible for spectrum management in Canada and for fostering a robust and reliable telecommunications system. Develops policies to ensure a safe and secure online marketplace. Helps to ensure the continuity of telecommunications during an emergency.

Department of Justice Canada
Supports initiatives of client departments and agencies through the provision of legal advice on matters relating to cyber policy and law.
In respect of certain matters, especially those relating to criminal law policy and information sharing, Justice plays a leading role. Departmental Legal Services within the Communications Security Establishment Canada had been designated as the centre of excellence on cyber-related legislation.

#634168

Pages 415 to / à 416

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 418 to / à 419

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 421 to / à 425

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 427

is withheld pursuant to sections

est retenue en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

6. FEDERAL-PROVINCIAL-TERRITORIAL CLERKS MEETING

PROPOSED TALKING POINTS

- Federal-Provincial-Territorial (FPT) Clerks are meeting on January 23, 2012, and they will be discussing cyber security, among other things.

- We have a one-hour time slot that will allow us to deliver a comprehensive threat briefing, including a focus on cyber. In many ways, it will mirror the brief given to FPT Justice Ministers last year. The Canadian Security Intelligence Service and the Communications Security Establishment Canada have offered to give these presentations.

- I think it is important that the briefing focus on areas of concern for PTs, and should pay particular attention to areas where we want to invite them to get in partnership with us, such as energy, resources and risks to officials travelling abroad. There are also threats to the PTs' own systems and the sensitive economic information they hold, such as corporate financial, land use and exploration data.

- There is a keen appetite in the PT community for information on which to base decisions and priority-setting for practical outcomes on cyber security. [redacted]

Page 429

is withheld pursuant to section

est retenue en vertu de l'article

14(a)

of the Access to Information

de la Loi sur l'accès à l'information

UNCLASSIFIED

Discussion of Cyber Security at the FPT Clerks Meeting

Presentation to DM Cyber
January 12, 2011

Background

- The Clerk of the Privy Council meets with his provincial and territorial counterparts twice per year
- Co-chaired by a PT clerk: British Columbia is co-chairing this year
- Meetings are informal in nature and typically focus on common challenges of public service management rather than serving as a forum to discuss substantive policy files
- FPT Clerks will be meeting for a full day on January 23, 2012, to address:
  - innovation in times of fiscal restraint
  - open government
  - the governance of horizontal government
  - streamlining intergovernmental business
  - security and cyber security

Page 432

is withheld pursuant to section

est retenue en vertu de l'article

14(a)

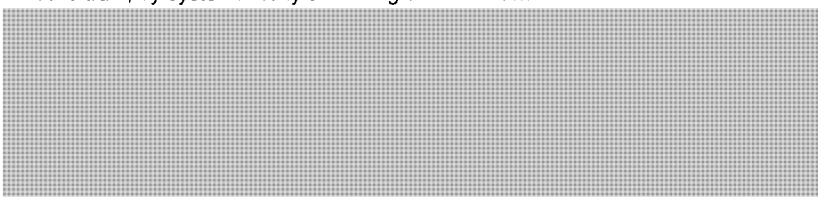
of the Access to Information

de la Loi sur l'accès à l'information

Strategic framework for PT engagement

UNCLASSIFIED

- Strategic objectives for engagement are to have PTs:
  - take steps to ensure resiliency and security of their cyber systems
  - engage as active partners in areas of shared interest (e.g., critical infrastructure sectors) in line with jurisdictional roles
- The proposed FPT approach is to:
  - build trust, by systematically delivering on commitments



  - establish a rhythm of working together, through regular outreach, meetings, collaboration on projects at various levels
  - seek their commitment of resources at the operational and policy levels

Current status

UNCLASSIFIED

- Progress is being made:
  - initial consultations have been positive, and have informed the development of a federal engagement strategy
  - senior level FPT committee established, chaired by ADM – PS; working towards defining the elements of a shared action plan
    - a gap analysis, informed by table top exercises, is among next steps
  - PS is working with FPT Chief Information Security Officers on early deliverables
    - portal for information exchange, protocols for incident reporting, baseline assessment of PT cyber security, sharing sensitive information
  - FPT communications working group established, focusing on public awareness and incident communications coordination
  - B.C., Alberta, Manitoba, Ontario and New Brunswick have indicated a high willingness to engage, and are leaders in capability

Next steps

UNCLASSIFIED

- A teleconference on December 15 with the ADM level FPT cyber security committee was held to discuss the proposed elements of a joint action plan
- Develop a regular approach for information exchange and threat briefings
- Increase the pace of collaboration with willing PTs, and show responsiveness to their priorities
- Work federally to improve the gap analysis, and to operationalize the strategic framework for PT engagement
- Invite working level PT officials to participate in shaping CCIRC products, services, tools (e.g., on the design and functionality of the Cyber Community Portale)
- Use Public Safety Canada regional offices to bring together PT emergency management and cyber security

Objectives for the Clerks meeting

UNCLASSIFIED

- The Clerks' meeting is an excellent opportunity to:
  - secure support for intergovernmental collaboration on cyber security
  - reinforce our commitment to sharing more information through action
  - secure support for a multi layered approach (strategic, operational and communications)
  - recommend the review of existing emergency response protocols to asses their applicability for cyber incidents

7. ROUNDTABLE

During the roundtable, it is not expected that you will have any items to add.

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:

File No.: 392100
RDIMS No.: 732885

MEMORANDUM FOR THE DEPUTY MINISTER

TRAVEL REQUEST TO ATTEND THE 14th ANNUAL PRIVACY AND SECURITY CONFERENCE IN VICTORIA, BRITISH COLUMBIA, FEBRUARY 6-8, 2013

(Signature required)

ISSUE

Your approval is sought for six Public Safety Canada (PS) employees to travel to Victoria, British Columbia, to participate in the 14th Annual Privacy and Security Conference, February 6-8, 2013, at an estimated cost of $18,499.40.

BACKGROUND

The Privacy and Security conference is an important event in the field of technology security. It allows participants to explore the most recent developments in policies, programs, laws and research in the field of privacy and security. The program for the 14th annual edition of the conference is attached (**TAB A**).

The conference brings together government officials and representatives from the private sector through the use of workshops and information sessions that allow participants to cover a variety of themes and exchange ideas.

CONSIDERATIONS

It is proposed that Public Safety's (PS) participation consist of representatives from National Cyber Security Directorate (NCSD), National Security Operations Directorate (NSOD) and Communications Branch.

As a part of PS's public awareness campaign Get Cyber Safe, two representatives from NCSD and one from Communications will set up and host an information booth at the conference. The purpose is to promote NCSD's programs and activities, including the products and services offered by the Canadian Cyber Incident Response Center and to increase its client base. The cost of the booth is $2,000.32 which includes three conference passes. The requisition is attached (**TAB B**).

In addition, three representatives from NSOD will attend the conference given the focus on privacy and security. Discussions and panel presentations will strengthen the Department's capacity to develop effective policy proposals and program management in order to continue to advance work in the area of Canada's lawful interception framework.

The conference will also provide insight with respect to the adherence to confidentiality provisions linked to the *Investment Canada Act*'s national security provisions. In addition, sessions on privacy impact assessments and lessons learned regarding privacy breaches will provide context for the ongoing enhancement of the foreign investment review process. Sessions related to counterterrorism, intelligence and privacy will facilitate a better assessment of the capabilities and strengths of Canada's national security initiatives relative to those of other countries. Finally, presented case studies will help develop a more nuanced understanding of gaps that could exist in the Canadian security framework.

Attendance at the conference will inform future policy development, program improvement and legislative work in the realm of national security. The estimated cost of this event is $18,499.40 and all costs related to this request fall within my sector's allocated Travel/Hospitality/Conference cap for this fiscal year. All efforts have been made to consider value for money and cost effectiveness.

RECOMMENDATION

It is recommended that you approve this travel request, including the costs associated with conference participation. Should you agree, your signature is sought on the attached Travel Authority and Advance Forms (**TAB C**) and the Request to attend a Conference Form (**TAB D**).

Should you require additional information, please do not hesitate to contact me, Robert Dick, Director General, National Cyber Security, at 613-990-2661 or Michael MacDonald, Director General, National Security Operations at 613-993-4595.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Gary Robertson
Assistant Deputy Minister
Corporate Management Branch

Enclosures: (4)

I approve:

Q4 THC 2012 NS
François Guimont

I do not approve:

François Guimont

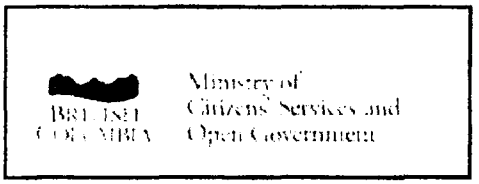
Prepared by: Guillaume Lefebvre

- **About**More information
  - Overview
  - Corporate Bios
  - Sponsors & Partners
  - Galleries
  - Testimonials
- **Core**Reboot's services
  - Conferences & Events
  - Venture Capital
  - Executive Institute
- **Events**Reboot productions
  - Upcoming
  - Past
- **Contact**Get in touch!
- **Register Now**

Information Location Speakers Agenda Sponsors
Accommodations Register Now

The 14th Annual Privacy and Security Conference

Trust in a Connected World
Feb 6, 2013 - Feb 8, 2013
The Victoria Conference Centre



14th Annual Conference Returns to Victoria February 6-8, 2013!

About the Conference
Held in Victoria, British Columbia, Canada this conference is a must attend for those working in the privacy and security fields. Presented by the Office of the CIO, Government of British Columbia, this two-day conference, is recognized as one of the top tier events in North America. Anyone working in the information privacy and security fields will benefit from the speakers, discussions and networking at the conference. Attendees are from every level both within government and private industry. The conference draws an international audience of some 1,000 delegates with an interest in cutting edge policy, programs, law, research and technologies aimed at the protection of privacy and security.

On-line registration is now open. Click HERE to access your early bird delegate rate!

The Province of BC is delighted to announced the first round of headliners for this year's conference:

-  **General Michael Hayden**, former CIA Director and former Director of the US National Security Agency

-  **Robert Herjavec**, founder of Canada's largest IT security provider *The Herjavec Group*, TV personality (Dragon's Den and Shark Tank) and bestselling author

- **Cole Stryker**, Author of *Hacking the Future: Privacy, Identity, and Anonymity on the Web* 

- **Simon Davies**, Founder and former Director General, Privacy International (United Kingdom) 

Reasons to Attend

- Get face-to-face dialogue with international industry experts who have successfully implemented best practices solutions
- Learn about current trends, issues and actions
- Obtain your annual Continuing Professional Development credits
- Discover new methods and products that can lower expenses and increase revenues
- Take the pulse of what is happening for tools, technologies, and processes
- Get Immediate answers and solutions to issues current in your organization

Conference Rates:

	Early bird registration before midnight December 15, 2012	**Regular registration** after December 15, 2012
Public Sector	$475.00 CAD (plus HST)	$675.00 CAD (plus HST)
Private Sector	$700.00 CAD (plus HST)	$900.00 CAD (plus HST)

Registration Fees Include:

- 2 plated lunches
- All coffee breaks
- All keynotes, plenaries, panel sessions and business breakouts
- Pre-conference workshops
- Access to exhibit hall
- Conference bag/portfolio
- Conference materials
- On-line access to presentations post-event

Accommodation:

If you need to make accommodation arrangements, the Fairmont Empress is offering a special conference rate of $122/night for Corporate reservations and $100/night for Government reservations. Please contact the hotel directly at (250) 384-8111 to book a room or you can book online using the following links:

Corporate Reservations – https://resweb.passkey.com/go/privseccorp

Government Reservations – https://resweb.passkey.com/go/privsecgov

Fairmont Empress
721 Government Street
Victoria, BC
V8W 1W5

https://www.fairmont.com/empress-victoria/

Accommodations Register Now

The 14th Annual Privacy and Security Conference

The following speakers will be talking at The 14th Annual Privacy and Security Conference.
Click on a speaker's picture for more information.

Information for the PSV2013 Conference is coming soon...

Information Location Speakers Agenda Sponsors
Accommodations Register Now

The 14th Annual Privacy and Security Conference

February 6-8, 2013

Victoria Conference Centre, Victoria, B.C.

Notional Agenda (subject to change)

Updated December 7, 2012
***Invited**

WEDNESDAY, February 6, 2013

Pre-Conference Privacy and Security Workshops

Morning Workshops:

9:00-12:00 *Sidney*	BC Ministry of Citizens' Services – Legislation, Privacy and Policy presents; ***Standard FOIPP Workshop*** **Speaker tbc**
9:00-12:00 *Theatre*	BC Ministry of Citizens' Services – Strategic Initiative Support & Advisory presents; ***STRA Workshop*** **Speaker tbc**
9:00-12:00 *Oak Bay I*	CA Technologies Workshop; **Presenter: Denny Prvu**, Sr. Principal Consultant Security Practice, CA
9:00-12:00 *Oak Bay II*	Government of Alberta presents; **Speaker tbc**
9:00-12:00 *Saanich*	Office of the Information and Privacy Commissioner of Ontario presents; ***Operationalizing Privacy by Design*** **Presenter: Ken Anderson**, Deputy Information and Privacy Commissioner, Province of Ontario
9:00-12:00 *Esquimalt*	IPS Workshop; **Speaker tbc**
9:00-12:00 *View Royal*	Workshop TBC; **Speaker tbc**
9:00-12:00 *Colwood*	CGI Workshop; **Speaker tbc**
9:00-3:00pm *Empress*	IAPP CIPP/C Training; *The Certified Information Privacy Professional/Canada (CIPP/C) is a professional*

certification offered by the International Association of Privacy Professionals (IAPP). The CIPP/C demonstrates understanding and application of Canadian information privacy laws, principles and practices at the federal, provincial and territorial levels. Training for the CIPP/C is an integral part of preparing for the CIPP/C exam and maximizes your potential for success.
Speaker TBC

Afternoon Workshops:

9:00-3:00pm *Empress*	IAPP CIPP/C Training (continued) *The Certified Information Privacy Professional/Canada (CIPP/C) is a professional certification offered by the International Association of Privacy Professionals (IAPP). The CIPP/C demonstrates understanding and application of Canadian information privacy laws, principles and practices at the federal, provincial and territorial levels. Training for the CIPP/C is an integral part of preparing for the CIPP/C exam and maximizes your potential for success.*
1:00-4:00 *Colwood*	Workshop TBC; **Speaker tbc**
1:00-4:00 *Sidney*	BC Ministry of Citizens' Services – Legislation, Privacy and Policy presents; ***Privacy Impact Assessment (PIA) Workshop*** **Speaker tbc**
1:00-4:00 *Theatre*	Office of the Information and Privacy Commissioner of Alberta presents; ***"Oh *@#%! We Have a Privacy Breach!" - Lessons Learned*** **Presenters:** **Diane McLeod-McKay**, Director, Personal Information Protection Act, Office of the Information and Privacy Commissioner of Alberta **Cara-Lynn Stelmack**, Portfolio Officer, Office of the Information and Privacy Commissioner of Alberta
1:00-4:00 *Esquimalt*	***Ethics Workshop*** **Melanie Vipond***, Associate, Heenan Blaikie
1:00-4:00 *Oak Bay I*	SafeNet Inc. Workshop; **Speaker tbc**
1:00-4:00 *Oak Bay II*	BC Information Access Operations Branch Workshop; **Elizabeth Vander Beesen,** Director, Staff Administration, Information Access Operations, Ministry of Citizens' Services and Open Government
1:00-4:00 *Saanich*	Privacy Analytics, Inc. Workshop; **Speaker tbc**
1:00-4:00 *View Royal*	Workshop TBC; **Speaker tbc**

****

THURSDAY, February 7, 2013

7:00-8:00	Registration
8:00-8:10 *Salon AB*	Call to Conference **MC: Richard Purcell**, CEO/Corporate Privacy Group, Executive Director/The Privacy Projects, and Chairman/DHS Data Privacy and Integrity Advisory Committee
8:10-8:20 *Salon AB*	Welcome Remarks: **Honourable Ben Stewart**, Minister of Citizens' Services and Open Government
8:20-9:00 *Salon AB*	Session1 - **Keynote Speaker: General Michael Hayden**, former Director of the CIA and former Director of the US National Security Agency **Security, Secrecy, Privacy and the Law** *In an era of globalization in which threats emanate from unexpected and unprecedented sources, in which borders are often rendered meaningless, in which real threats can come*

from non-state and even individual actors---how do free people defend themselves....and remain free?

9:00-9:40 Session 2 - **Keynote Speaker: Simon Davies**, Founder and former Director General, Privacy International (United Kingdom)
Salon AB

9:40-10:00 Morning Break
Upper & Lower Foyers

10:00-10:40 Session 3 - Concurrent Keynote Speakers

Salon AB A. IBM - Speaker tbc

Theatre B. Microsoft - Speaker tbc

10:45-12:00 Session 4 - Concurrent Sessions

Salon AB Panel A: **Health Data Research – Big Data, Big Opportunities, Big Challenges**
Moderator: **Erwin Malzer,** Certified Director & Management Consultant, Executive Advisory Services
Speakers:

1. **Ken Anderson,** Deputy Information and Privacy Commissioner, Province of Ontario
2. **Colin Hansen,** MLA, Vancouver-Quilchena, Legislative Assembly of B.C.
3. **Tim Grance*,** Senior Computer Scientist, National Institute of Standards and Technology (NIST)
4. **Dr. Khaled El Emam***, Founder & CEO, Privacy Analytics, Inc.
5. **Lindsay Kislock***, Assistant Deputy Minister of Health, Province of British Columbia
6. Sponsor - SAS (tbc)

Theatre Panel B: **Mobile Payments - Consumer Benefits and New Privacy Concerns**
Payment systems that allow people to pay using their mobile phones promise to reduce transaction fees, increase convenience, and enhance payment security. New mobile payment systems are also likely to make it easier for business to identify consumers, collect more information and share information about their purchases. Studies have reported security concerns as a barrier to adopt mobile payment technologies, privacy implications have been largely neglected. Trust in the mobile payment world who will deliver on their promises?
Moderator: TBC
Speakers:

1. **Jennifer M Urban,** Assistant Clinical Professor of Law, Berkley Center for Law & Technology
2. **Bruce Burke,** Founder, Gulf Bay Consulting
3. **Jack Dorsey*,** Founder, Square
4. **Google**
5. **PayPass**

Salon C Panel C: **Biometrics: Facial Recognition – Impacts and Opportunities**
Moderator: **Michael McEvoy**, Assistant Commissioner - Policy & Technology, Office of the Information and Privacy Commissioner of B.C.
Speakers:

1. **Nalini K. Ratha*,** Research Staff Member, Biometrics Lead, IBM
2. **Dr. Svetlana Yanushkevich,** Co-Founder, Biometric Technologies Lab, University of Calgary
3. **Ben Shotton**, Manager, Driver Licensing Integrity & Risk Management, ICBC
4. TBC

12:05-1:10 Luncheon Keynote Address

Salon AB Telus - Speaker tbc

Crystal **Trevor Hughes**, President & CEO, International Association of Privacy Professionals (IAPP)

Session 5 - Keynote Speaker: Symantec - Speaker tbc

1:15-1:55 *Salon AB*	
2:00-2:30	Session 6 - Vendor Sessions
Salon AB	**Symantec** - speaker tbc
Sidney	**IBM - Chris Poulin**, Industry Security Systems Strategist
Theatre	**Radware - Carl Herberger**, Vice President, Security Solutions
Salon C	**Oracle** - speaker tbc
Oak Bay I	**RSA** - speaker tbc
Saanich	**Fortinet** - speaker tbc
Esquimalt	**TELUS** - speaker tbc
Oak Bay II	**CGI** - speaker tbc
Colwood	**Adobe** - speaker tbc
View Royal	**IPS** - speaker tbc
2:30-2:50 *Upper & Lower Foyers*	Afternoon Break
2:50-4:05	Session 7 - Concurrent Sessions
Salon AB	Panel A: **The Challenges of Identity Management** Moderator: **Dave Nikolejsin,** Associate Deputy Minister, Environment Assessment Office, Government of British Columbia Speakers: 1. **Kim Cameron*,** Distinguished Engineer and Chief Architect of Identity, Microsoft 2. **Dick Hardt,** Founder and CEO, Sxip Identity 3. **Dmitry Barinov**, Chief Security Officer, SecureKey 4. **Louis Beauséjour***, Assistant Deputy Minister, Integrity Services Branch, Service Canada 5. SafeNet
Theatre	Panel B: **Open Government, Open Data** Moderator: **Jill Clayton***, Commissioner, Office of the Information and Privacy Commissioner of Alberta Speakers: 1. **Jean-François Gauthier,** Executive Director, Loran Technologies 2. **David Hume***, Executive Director, Citizen Engagement, Government of B.C. 3. TBC
Salon C	Panel C: **BYOD** *The BYOD bandwagon keeps rolling along and with it the growing concerns about supporting employee-owned devices in the workplace. Protecting corporate and government data is at the top of the list of concerns for IT professionals. How do you integrate smart phones, tablets, and laptops using cloud based storage solutions into the infrastructure that protects corporate and government assets?* Moderator: **Winn Schwartau**, "The Civilian Architect of Information Warfare," Author, Speaker, Security Theorist, Serial Entrepreneur, Distinguished Fellow Ponemon Institute, and Founder, SecurityExperts.Com Speakers: 1. **Derick Cassidy**, Founder and CTO, Device Identity 2. Symantec 3. Citrix 4. Forsythe
4:10-4:50	Session 8 - Concurrent Keynote Speakers:

Salon AB	A. **John Proctor**, Director, Cyber Resilience, CGI
Theatre	B. **John Landwehr**, Vice President, Public Sector Solutions, Adobe Systems

****

FRIDAY, February 8, 2013

8:00-8:05	Administrative Announcements
Salon AB	**MC: Richard Purcell**, CEO/Corporate Privacy Group, Executive Director/The Privacy Projects, and Chairman/DHS Data Privacy and Integrity Advisory Committee
8:05-*8:30*	Opening Address: **Elizabeth Denham**, Privacy and Information Commissioner of British
Salon AB	Columbia
8:30-*9:10*	Session 9 - Keynote Speaker: **Cole Stryker**, Writer and Media Strategist, Author of *Hacking*
Salon AB	*the Future*
9:10-9:50	Session 10 - Keynote Speaker: **Chris Hadnagy**, Author of *Social Engineering: The Art of*
Salon AB	*Human Hacking*, Lead Developer of Social-Engineer.org
9:50-10:10	Morning Break & Book Signing
Upper Foyer	
10:10-10:50	Session 11 - Concurrent Keynote Speakers
Salon AB	A. **Nuala O'Connor***, Vice President and Associate General Counsel, Compliance and Privacy, Amazon
Theatre	B. **RSA** - Speaker tbc
10:55-12:10	Session 12 - Concurrent Panel Sessions
Salon AB	Panel A: **Social Media** Moderator: **Cole Stryker,** Writer and Media Strategist, Author of *Hacking the Future* Speakers: 1. **Rosemary Fitzgerald***, Partner, Digital Media and Mobile Strategies, Spiderweb Studio 2. **Larry Magid,** On-Air Technology Analyst, CBS 3. **Nicole Wong***, Chief Privacy Officer, Twitter 4. **Barbara Bucknell**, Strategic Policy Analyst, Office of the Privacy Commissioner of Canada 5. Sponsor
Theatre	Panel B: **Cloud Computing: Trust but Verify** *With the advent of cloud computing and the growth of connectivity between institutions, companies and individuals electronic security has never been a more visible and urgent issue.* Moderator: **David Loukidelis**, former Information and Privacy Commissioner of British Columbia Speakers: 1. **Mike Howard***, Chief Security Officer, Microsoft Corporation 2. **Benoit Long***, Sr. Assistant Deputy Minister, Shared Services Canada 3. **Martin Kratz**, Board Chair, Canadian Cloud Council 4. Sponsor
Salon C	Panel C: **Cyber Security and Critical Infrastructure** Lead Speaker: **Tim McCreight***, Executive Director - Corporate Information Security Office, Government of Alberta Speakers:

1. **Toni Moffa***, Deputy Chief/ADM, Information Technology Security Program, Communications Security Establishment Canada
2. **Colleen D'Iorio***, Executive Director, Security, Treasury Board of Canada Secretariat
3. **Gregory Nojeim***, Senior Counsel, Center for Democracy & Technology
4. **Carl Herberger**, Vice President, Security Solutions, Radware
5. **CGI**

12:10-1:15	Luncheon Keynote Address
Salon AB	Fortinet - Speaker tbc
Crystal	**Larry Magid**, On-Air Technology Analyst, CBS
1:20-1:50 *Salon AB*	Session 13 - Keynote Speaker: **TBC**
1:55-2:25	Session 14 - Vendor Sessions
Oak Bay I	**Canada Revenue Agency** - Secure Portals - **Caroline Babcock**
Salon C	**Websense, Inc.** - speaker tbc
Sidney	**Grant Thornton** - speaker tbc
Salon AB	**Research In Motion** - speaker tbc
Theatre	**Forsythe/Check Point Software** - speaker tbc
Esquimalt	**SafeNet Inc.** - speaker tbc
Saanich	**Bell** - speaker tbc
Oak Bay II	**Palo Alto Networks** - speaker tbc
Colwood	**SAS** - speaker tbc
View Royal	**Sierra** - speaker tbc
2:25-2:45 *Upper & Lower Foyers*	Afternoon Break
2:45-4:00	Session 15 - Concurrent Sessions
Salon AB	Panel A: **Lawful Access** Moderator: TBC Speakers: 1. BC Civil Liberties Association 2. TBC 3. Sponsor
Theatre	Panel B: **What is the Future of Surveillance?** Moderator: TBC Speakers: 1. **Jamie Graham***, Chief Constable, Victoria Police Department 2. **David Loukidelis**, former Information and Privacy Commissioner of British Columbia 3. **Simon Davies**, Founder and former Director General, Privacy International, United Kingdom 4. **Alex Dow**, Senior Security & Privacy Consultant, IPS
Salon C	Panel C: **CyberSafety, Security & Privacy for Kids and Families** Lead Speaker: **Winn Schwartau**, "The Civilian Architect of Information Warfare," Author, Speaker, Security Theorist, Serial Entrepreneur, Distinguished Fellow Ponemon Institute, and Founder, SecurityExperts.Com Speakers: 1. **Daphne Guerrero**, Manager, Public Education & Outreach, Office of the Privacy Commissioner of Canada 2. **Eric Green***, President, ELG Consulting

3. **Spencer Wilcox***
4. **Susan Wright***

4:05-4:45 *Salon AB*	Session 16 - Closing Keynote Speaker: **Robert Herjavec**, Founder, The Herjavec Group, Investor, and Television Personality (Dragon's Den and Shark Tank)
4:45-4:55 *Salon AB*	Closing Remarks: **Kim Henderson**, Deputy Minister, Ministry of Citizens' Services and Open Government
4:55-5:00 *Salon AB*	Closing Announcements **MC: Richard Purcell**, CEO/Corporate Privacy Group, Executive Director/The Privacy Projects, and Chairman/DHS Data Privacy and Integrity Advisory Committee

Information Location Speakers Agenda Sponsors
Accommodations Register Now

The 14th Annual Privacy and Security Conference

The 14th Annual Privacy and Security Conference is proudly sponsored by the following companies.
If you would like to sponsor this event, please download the sponsorship brochure for more information.

Title Sponsor

Symantec

Platinum Sponsors

Adobe

FORTINET

HERJAVEC GROUP

RSA

TELUS

Gold Sponsors

BlackBerry

Deloitte

FORSYTHE
Realize the business value of IT

Grant Thornton

IPS

ORACLE
PUBLIC SECTOR

sense
ESSENTIAL INFORMATION PROTECTION

Conference Sponsors & Exhibitors

Event Partners

Share:

Follow us on...

Facebook

Twitter
Follow @Reboot_Comm
LinkedIn

YouTube

Upcoming Conferences

- The 14th Annual Privacy and Security Conference
- 4th Annual Canadian Videogame Awards
- The 13th Annual Healthcare Conference
- Micro Cap Financial Conference 2013

Past Events

- The 13th Annual Privacy and Security Conference
- The Canadian Videogame Awards
- The 12th Annual Healthcare Conference
- The 3rd Annual Privacy, Access and Security Congress 2012

Contactget in touch with us

Search Site

Refund & Privacy Policy

Government of Canada / Gouvernement du Canada

Requisition for Goods and Services - Demande de biens et de services

For Amendment Only / Aux fins de modification seulement

Amend No. / Modif. N°	Increase/Decrease / Augmentation/ Réduction	Previous Cost / Coût précédent

Current Funding / Financement actuel: 1,786.00

Requisition No. - N° demande: Ordering Office / Bureau demand. | Year / Année: 3 | Serial No. / N° de série: 3427

Accounting Office Code / Code du bureau compt.:

Page 1 of 1

SSC Use Only / ASC seulement

To:/À:

Originator - Auteur: PSEPC/SPPCC

Tel. No. - N° de tél.: 613-990-2614

Address Inquiries To: / Adresser toute demande de renseignements à: Guillaume Lefebvre 949-7376

Telephone Number / Numéro de téléphone

Destination: As per consignee addresses within / Voir adresse des destinataires particuliers

Inspection Agency - Chargé de l'inspection: ☐ Consignee at Destination / Destinataire ☐ Specified herein / Précisé dans les présentes

Quality Assurance - Assurance de la qualité: ☐ DND / MDN ☐ Specified herein / Précisé dans les présentes

Instructions:

Refer to Supply and Services Canada Customer Manual, Chapter 210, Acquisition of Goods and Services, for detailed explanation of fields.

Pour plus de précisions, se reporter au Chapitre 210 (Acquisition de Biens et de Services) du Manuel du Client, Approvisionnements et Services Canada.

Confirmation with PWGSC - Confirmation de TPSGC

Buyer's Name / Nom de l'acheteur

Telephone Number / Numéro de téléphone

Invoices - Original and two copies are to be made out and sent to

Factures - Remplir et envoyer l'original et deux copies à

Invoice_Processing@ps-sp.gc.ca

SSC Use Only - ASC seulement

Financial Code(s) - Code(s) financier(s): SEE BELOW / VOIR CI-APRÈS

Amount - Montant

Item / Article	Reference/Stock No. and Description / N° de référence de nomenclature et description	Date Required / Demandé pour le D/J M Y/A	Consignee Code / Code du destinataire	U. of I. / U. de D.	Quantity / Quantité	Estimated Cost / Prix estimatif	Previous Quantity and Unit Price / Quantité et prix unitaire précédents	Previous Contract No. and Date / Date et n° du contrat précédent
00001	**Kiosk Rental for Reboot Conference** Reboot Communications Ltd. Exhibition Sponsorship - 14th Annual Privacy and Security Conference February 6-8, 2013 Kiosk rental 1 @ $1786.00	29 03 13		EA	1.00	1,786.00		

Financial Codes - Codes financiers

Fund / Fonds	GL Account / Compte du GLG	Cost Centre / Centre de Coût	Internal Order / N° de projet	Amount / Montant
0001	05050	000493		1,786.00

Dept.No - N° du min. | IS org - RI org.: FIS - SIF | IS Ref. - RI réf.

Special Instructions - Instructions spéciales

Reboot Conference February 6-8, 2013
Kiosk rental @ $1786.00 (includes passes to conference)
Invoice #8025PSV
Technical Lead:
Guillaume Lefebvre 613-949-7376

Security - Sécurité

Does this requisition include security provisions? / Cette demande comprend-t-elle des exigences en matière de sécurité? No / Non ☐ Yes / Oui ☐

If yes, is a Security Requirement Check List (SRCL) required? / Si oui, une liste de vérification des exigences relatives à la sécurité (LVERS) est-elle requise?

No / Non ☐ Yes / Oui ☐ If an SRCL is required, attach the properly signed SRCL to this requisition. / Si une LVERS est requise, la joindre dûment complétée et signée à cette demande.

If an SRCL is not required, but the requisition does require security provisions, explain why in the requisition.
Si une LVERS n'est pas requise, mais le demande comprend des exigence en matière de sécurité, expliquer la raison dans la demande.

The Undersigned certifies that this requisition, including any attached SRCL, accurately details the security provisions of this requirement.
Je, soussigné, certifie que cette demande, y compris toute LVERS, décrit exactement les exigences en matière de sécurité de ce besoin.

Signature _____ Date _____

Recommended by - Recommandé par

G4 THC PLAN 2012 NS 42 Jan 23, 13

Signature Date

PURSUANT TO SUB SECTION 32(1) OF THE FINANCIAL ADMINISTRATION ACT, FUNDS ARE AVAILABLE.
EN VERTU DU PARAGRAPHE 32(1) DE LA LOI SUR LA GESTION DES FINANCES PUBLIQUES, DES FONDS SONT DISPONIBLES.

Sebastien Labelle, Director, Engagement and Partnerships

The Undersigned approves this requisition and certifies that the necessary approvals have been obtained and requests SSC to acquire the goods and/or services described herein.
Je, soussigné, approuve la présente demande, certifie, que les approbations requises ont été obtenues et demande à ASC d'obtenir les biens et services décrits dans les présentes.

Signature _____ Date _____

000450

Public Safety Canada / Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: 23 novembre 2012

To – A

François Guimont
Deputy Minister
Public Safety

Requested by – Demandé par

Guillaume Lefebvre
Analyst
National Cyber Security Directorate
National Security

Name of Conference – Titre de la conférence

The 14th Annual Privacy and Security Conference

Type of Conference – Genre de conférence

☐ International / Internationale ☒ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

BC Ministry of Citizen's Services and Open Government

Official Host – Hôte officiel

Reboot Communication

Duration of Conference – Durée de la conférence

From / Du: February 6, 2013 To / À: February 8, 2013

Location - Adresse

The Victoria Conference Centre, Victoria BC

Agenda – Ordre du jour

See attachment

Purpose of Participation - Object de la participation

As part of its conference attendance initiative National Cyber Security Directorate (NCSD) engagement and partnership division has identified the Annual Privacy and Security Conference an event of great value. The main objective of this initiative is to develop relationships with stakeholders including Critical Infrastructure owner and operators, security experts and academics to further the achievements of NCSD's outcomes. Part of this effort is intended to increase NCSD's brand awareness and recognition as well as to shape its image though outreach activities. Conferences are unmatched venues to reach an industrial target audience and meet with stakeholders in an economical fashion enabling both the promotion of NCSD and relationship building. Our plan is to set up an information booth at major security and privacy conferences in Canada to promote the products and services offers by the Canadian Cyber Incident Response Center and increase its client base as well as to promote NCSD's other programs and activities (e.g., assessment program, best practices program and the control system security workshop). The conference draws an audience of some 1,000 delegates from the privacy and security fields. The Annual Privacy and Security Conference is the main conference to be held on the West coast and, as such, it represent a unique opportunity to ensure regional coverage for that region.

Ø conf Fee – free w booth

Financial Coding – Code financier

Estimated Total Cost / Coût total prévu

$ 2,698.28

Recommended by – Recommandé par

Signature: [signature] Date: Jan 11, 2013

Branch Approval – Approbation de la direction

Signature: _____ Date: _____

Assistant Deputy Minister – Sous-ministre adjoint

Signature: [signature] Date: _____

Deputy Minister – Sous-ministre

Signature: _____ Date: _____

MS-18 (4/04)

Public Safety Canada / Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: 23 novembre 2012

To – A

François Guimont
Deputy Minister
Public Safety

Requested by – Demandé par

Laura langs
Analyst
National Cyber Security Directorate
National Security

Name of Conference – Titre de la conférence

The 14th Annual Privacy and Security Conference

Type of Conference – Genre de conférence

☐ International / Internationale ☒ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

BC Ministry of Citizen's Services and Open Government

Official Host – Hôte officiel

Reboot Communication

Duration of Conference – Durée de la conférence

From / Du: February 6, 2013 To / À: February 8, 2013

Location - Adresse

The Victoria Conference Centre, Victoria BC

Agenda – Ordre du jour

See attachment

Purpose of Participation - Object de la participation

As part of its conference attendance initiative National Cyber Security Directorate (NCSD) engagement and partnership division has identified the Annual Privacy and Security Conference an event of great value. The main objective of this initiative is to develop relationships with stakeholders including Critical Infrastructure owner and operators, security experts and academics to further the achievements of NCSD's outcomes. Part of this effort is intended to increase NCSD's brand awareness and recognition as well as to shape its image though outreach activities. Conferences are unmatched venues to reach an industrial target audience and meet with stakeholders in an economical fashion enabling both the promotion of NCSD and relationship building. Our plan is to set up an information booth at major security and privacy conferences in Canada to promote the products and services offers by the Canadian Cyber Incident Response Center and increase its client base as well as to promote NCSD's other programs and activities (e.g., assessment program, best practices program and the control system security workshop). The conference draws an audience of some 1,000 delegates from the privacy and security fields. The Annual Privacy and Security Conference is the main conference to be held on the West coast and, as such, it represent a unique opportunity to ensure regional coverage for that region.

$ conf fee incl. w. booth

Financial Coding – Code financier

Estimated Total Cost / Coût total prévu

$ 1,452.80

Recommended by – Recommandé par

Signature: [signature] Date: Jan 11, 2013

Branch Approval – Approbation de la direction

Signature: _____ Date: _____

Assistant Deputy Minister – Sous-ministre adjoint

Signature: [signature] Date: _____

Deputy Minister – Sous-ministre

Signature: _____ Date: _____

000452

MS-18 (4/04)

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval as orginal dated)
Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Autnority No. (TAN) N°. d'aut de voyager (NAV)	Document No. - N° du document
		RDIMS 731360

Part A - Partie A

Type 2	Name of traveller - Nom du voyageur	Classification
	Laura Langs	EC-04

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	National Security/National Cyber Security Directorate
Address - Adresse	**Telephone No. - No. de téléphone** / If different address, send cheque to: / Si adresse différente, envoyer chèque à
260-858 Beatty Street, Vancouver BC	604-666-9728
Branch Contact - Personne ressource à la direction	**Telephone No. - No. de téléphone**
Jane Hayward	613-991-1982

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)?	If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une?
To attend meetings in Victoria BC, REBOOT	3	☑ Yes / Oui ☑ No / Non	☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival Départ - Arrivée	Transportation Transport Mode	No. of meals prepaid Nbre de repas prépayés	Accommodation - Hébergement	File locator number N°. de repérage du dossier
February 6, 2012	Vanouver	Victoria	07:00-07:25	Air	0	Fairmont Empress	
February 8, 2012	Victoria	Vancouver	17:30-17:55	Air	0	78047000	

Part C - Expenses and Allowances / Partie C - Dépenses et Indemnités

Standard - Générales Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$240.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☑ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	
Transportation Transport	$230.00	Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dussus)	$0.00
Meals and incidentals Repas et frais accessoires	$267.30	☐ First class (Deputy Head or equivalent approval) Prém. Classe (approuvée par le sou-chef ou l'équiv.) ☐ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sou-chef ou l'équiv. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Other (Specify) - Autre (préciser)	$75.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel.

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$640.50
Other - Autre	$812.30
Trip Total - Coût total du voyage	$1,452.80
Funding - Financement	
A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Laura Langs — Signature — January 11, 2013 — Date

Ticket pick-up date and location
Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0				0	

Accounting Information / Renseignement comptables

Type 4				
Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		NCSD THC T25	493-PSABASE - 2000	
	Description			Financial encumberance No. / No. de consignation de fonds: 500102714

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		Date
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé			Amount/Montant
Airfare / Frais d'avion			**$640.50**
Train / Train			**$0.00**
Other / Autres			**$0.00**
			$640.50

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	**$120.00**	**2**	$240.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	**$0.00**	**0**	$0.00
			$240.00
Mid-size car rental / Location d'une voiture intermédiaire	**$0.00**	**0**	$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	**$0.00**	**0**	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière Mileage (km) Employer Rate / Taux parcours (km) pour employé	**0.545**	**0**	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			**$0.00**	$0.00
Taxi/Limo	Home to Airport / Train Station		**$45.00**	$230.00
	Airport / Train Station / Hotel / Meeting		**$50.00**	
	Hotel / Airport / Train Station		**$40.00**	
	Airport / Train Station / to Home		**$45.00**	
	Meeting / Meetings		**$50.00**	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous				$0.00
				$230.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits dejeuners	**$15.50**	**3**	$46.50
Lunch / Déjeuners	**$15.00**	**3**	$45.00
Dinner / Dîners	**$41.30**	**3**	$123.90
Incidentals /Frais divers	**$17.30**	**3**	$51.90
			$267.30

Business Phone / Téléphone d'affaires	**$0.00**
Airport Improvement Fee / Frais de l'Aeroport	**$0.00**
Cash Advance Fee / Frais d'avances	**$0.00**
Misc. Business Services / Diverses charges d'affaires	**$0.00**
Miscellaneous / Diverses	**$75.00**
	$75.00

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé			Amount/Montant
Airfare / Frais d'avion			**$640.50**
Train / Train			**$0.00**
Other / Autres			**$0.00**
			$640.50
Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	**$120.00**	**2**	$240.00
Accomodation (**GREEN** page hotel) / Hebergement (un des hôtels figurant dans la partie **VERT** du répertoire)	**$0.00**	**0**	$0.00
			$240.00
Mid-size car rental / Location d'une voiture intermédiaire	**$0.00**	**0**	$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	**$0.00**	**0**	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00
	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière Mileage (km) Employer Rate / Taux parcours (km) pour employé	**0.545**	**0**	$0.00
	Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage		**$0.00**	$0.00
Taxi/Limo — Home to Airport / Domicile à l'aéroport		**$45.00**	$230.00
Taxi/Limo — Airport / Train Station to Home / Aéroport / Gare ferroviaire au domicile		**$50.00**	
Taxi/Limo — Home to Airport / Train Station / Domicile à l'aéroport / Gare ferroviaire		**$40.00**	
Taxi/Limo — Airport / Train Station to Home / Aéroport / Gare ferroviaire au domicile		**$45.00**	
Taxi/Limo — Airport / Train Station to Airport / Aéroport / Gare ferroviaire à l'aéroport		**$50.00**	
Transportation / Transportation (No receipt)			$0.00
Ferry & Miscellaneous			$0.00
			$230.00
	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.50**	**3**	$46.50
Lunch / Déjeuners	**$15.00**	**3**	$45.00
Dinner / Dîners	**$41.30**	**3**	$123.90
Incidentals /Frais divers	**$17.30**	**3**	$51.90
			$267.30
Business Phone / Téléphone d'affaires			**$0.00**
Airport Improvement Fee / Frais de l'Aeroport			**$0.00**
Cash Advance Fee / Frais d'avances			**$0.00**
Misc. Business Services / Diverses charges d'affaires			**$0.00**
Miscellaneous / Diverses			**$75.00**
			$75.00

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande

☐ Amended (Same levels of approval oas orginal dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document
		RDIMS 731360

Type 2	Name of traveller - Nom du voyageur	Classification
	Laura Langs	EC-04

Part A - Partie A

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	National Security/National Cyber Security Directorate
Address - Adresse	**Telephone No. - No. de téléphone** / **If different address, send cheque to: / Si adresse differente, envoyer chèque à**
260-858 Beatty Street, Vancouver BC	604-666-9728
Branch Contact - Personne ressource à la direction	**Telephone No. - No. de téléphone**
Jane Hayward	613-991-1982

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)?	If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une?
To attend meetings in Victoria BC, REBOOT	3	☑ Yes / Oui ☑ No / Non	☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival / Départ - Arrivée	Transportation Transport Mode	No. of meals prepaid Nbre de repas prépayés	Accommodation Hébergement	File locator number N°. de repérage du dossier
February 6, 2012	Vanouver	Victoria	07:00-07:25	Air	0	Fairmont Empress	
February 8, 2012	Victoria	Vancouver	17:30-17:55	Air	0	78047000	

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$240.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☑ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dussus)	$0.00
Transportation Transport	$230.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.)	
Meals and incidentals Repas et frais accessoires	$267.30	☐ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Other (Specify) - Autre (préciser)	$75.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel.

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$640.50
Other - Autre	$812.30
Trip Total - Coût total du voyage	$1,452.80
Funding - Financement	
A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / E U	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.

J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Signature _____ Date _____

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date
[signature]		Q4 THC PLAN 2012NS42	Jan 23, 13

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0				| 0	

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		NCSD THC T25	493-PSABASE - 2000	

	Description	Financial encumberance No / No. de consignation de fonds
		500102714

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requistion for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No - N° du chèque
Verified correct (PWGSC) (signature) / Verifié conform (TPSGC) (signature)		
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	Date

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande

☐ Amended (Same levels of approval oas orginal dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document
		RDIMS 731234

Type 2	Name of traveller - Nom du voyageur	Classification
	Guillaume Lefebvre	EC-05

Part A - Partie A

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	National Security/National Cyber Security Directorate
Address - Adresse: 340 Laurier Ave W, 11th Floor	Telephone No. - No. de téléphone: 613-949-7376
Branch Contact - Personne ressource à la direction: Jane Hayward	Telephone No. - No. de téléphone: 613-991-1982
Purpose of travel - Objet du voyage: The 14th Annual Privacy and Security Conference	No. of days / Nbre de jours: 5

If different address, send cheque to / Si adresse differente, envoyer chèque à

Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)? ☐ Yes / Oui ☑ No / Non

If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une? ☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival / Départ - Arrivée	Transportation Transport Mode	No. of meals prepaid Nbre de repas prépayés	Accommodation Hébergement	File locator number N°. de repérage du dossier
February 5, 2013	Ottawa	Victoria	7:40 - 11:25	Air	0	Fairmont Empress	
February 9, 2013	Victoria	Ottawa	7:40 - 17:04	Air	0	79445035	

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du repertoire)	$480.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☑ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable. Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$29.98	Other (Specify) - Autre (préciser)	
Transportation / Transport	$275.00	Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (préciser la <classe> si-dussus)	$0.00
Meals and incidentals / Repas et frais accessoires	$413.30		
Other (Specify) - Autre (préciser)	$0.00		

☐ First class (Deputy Head or equivalent approval) / Prem. Classe (approuvée par le sou-chef ou l'équiv.)

☐ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) / Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)

Approval - Approbation

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$1,500.00
Other - Autre	$1,198.28
Trip Total - Coût total du voyage	$2,698.28

Funding - Financement

A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.

J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Signature — Date: 15 janvier 2013

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date
		Q4 THC 2012N.S42	Jan 23/13

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0				| 0	

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		NCSD THC T25	493PSABASE - 2000	

	Description	Financial encumberance No. / No. de consignation de fonds
		500102714

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	Date

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé			Amount/Montant
Airfare / Frais d'avion			$1,500.00
Train / Train			$0.00
Other / Autres			$0.00
			$1,500.00

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$120.00	4	$480.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	$0.00	0	$0.00
			$480.00
Mid-size car rental / Location d'une voiture intermediaire	$0.00	0	$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermediaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louee			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.545	55	$29.98

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Hotel to Airport - Train Station		$75.00	$275.00
	Airport - Train Station - Hotel - Meetings		$100.00	
	Hotel - Airport - Train Station		$100.00	
	Airport - Train Station - Hotel		$0.00	
	Meeting - Meetings		$0.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$275.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$15.60	5	$78.00
Lunch / Dejeuners	$14.85	3	$44.55
Dinner / Diners	$40.85	5	$204.25
Incidentals /Frais divers	$17.30	5	$86.50
			$413.30

Business Phone / Télephone d'affaires	$0.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses	$0.00
	$0.00

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint(e) principal(e)

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: DEC 2 8 2012

File No.: 391664
RDIMS No.: 725710

MEMORANDUM FOR THE DEPUTY MINISTER

TRAVEL AUTHORITY FOR
JEFFREY BONVIE AND PATRICK CLOW
TO BARCELONA, SPAIN FEBRUARY 18 - 22, 2013

(Decision sought)

ISSUE

Your approval is sought for Jeffrey Bonvie, Advisor, Technical Advice Division, and Patrick Clow, Manager, Technical Services at the Canadian Cyber Incident Response Centre (CCIRC), to travel to Barcelona, Spain, from February 18-22, 2013, to attend the Microsoft Digital Crimes Consortium (DCC). The conference's agenda is enclosed (**TAB A**).

BACKGROUND

In working to advance Canada's Cyber Security Strategy, Public Safety Canada (PS) is developing relationships with key industry partners. PS recently signed the Microsoft Security Cooperation Agreement which enables privileged information sharing between the CCIRC and Microsoft technical staff.

One opportunity enabled by the agreement is attendance at the DCC, which is hosted by Microsoft. The DCC is a large event with anywhere from three to six talks and technical workshops. The scale of this event allows for multiple attendees from the same organization to attend and participate without having overlapping coverage at any one presentation.

This event brings together participants from around the globe to discuss and present on issues relating to cybercrime and cyber security. There is no cost to attend the DCC outside of travel and accommodations, however, potential attendees must be accepted by Microsoft. Mr. Bonvie and Mr. Clow have been approved by Microsoft for admittance to the 2013 DCC.

.../2

Canada

CONSIDERATIONS

PS' representation at this event will allow staff to learn the latest developments, trends, and issues in the area of cybercrime from leaders in the field; it is also a unique opportunity to become engaged in the latest technical, operational and policy level discussions on cybercrime.

Microsoft is a key partner for PS on a range of cyber priorities, but especially as an operational partner in incident reporting, as a collaborator in addressing threats and vulnerabilities to the cyber system, and as a vender uniquely positioned to offer insight on trends and technology. Attendance will support the government's cyber priority, and PS' international strategic framework priorities.

Mr. Bonvie and Mr. Clow are the only known representatives from the PS portfolio attending this event. The cost for both travellers is estimated at $18,213.37. All costs related to this request fall within my sector's allocated Travel/Hospitality/Conference cap for this fiscal year.

RECOMMENDATION

It is recommended that you approve this travel authorization request by signing the two Travel Authority and Advance forms (**TAB B**) and the two Training Application and Authorization forms (**TAB C**). The International Travel Request is included for your information (**TAB D**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976, or Robert Dick, Director General, National Cyber Security at 613-990-2661.

for

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Gary Robertson
Assistant Deputy Minister
Corporate Management Branch

Enclosures: (4)

I approve:

François Guimont

Jan 2, 2013

I do not approve:

François Guimont

Prepared by: Jeff Bonvie

Digital Crimes Consortium | 2013 Conference

February 18 - 22

Barcelona, Spain
Catalonia Palace of Congresses

AGENDA

All sessions designated as a "Lab" are limited in capacity and require advance sign-up.
Sessions will take place in the Catalonia Palace of Congresses which is adjacent to Hotel Rey Juan Carlos I.

Monday, February 18, 2013

time		topic	presenter
1000 - 1100		Birds of a Feather Meetings	Rooms are available for Industry Working Groups - contact DCCEVENT@microsoft.com for room reservations
1000 - 1300		Registration in Conference Center	
1300 - 1330	Plenary	Welcome	T.J. Campana, Director, Digital Crimes Unit, Microsoft
1330 - 1400	Plenary	Keynote Presentation	To Be Announced
1400 - 1430	Plenary	Keynote Presentation	To Be Announced
1430 - 1500	Plenary	Law Enforcement Case Study	To Be Announced
1500 - 1530		Break	
1530 - 1600	Plenary	Presentation	Troels Oerting, Assistant Director, European Cybercrime Center (EC3)
1600 - 1630	Plenary	Presentation	Elly van den Heuvel, Head of Dutch National Cybersecurity Center
1630 - 1700	Plenary	Reserved	To Be Announced
1730 - 2000		Welcome Reception	

Tuesday, February 19, 2013

time		topic	presenter
0900 - 1000		Coffee and Networking	
1000 - 1100	Session 1	APT from Unlikely Sources	Ryan McGeehan and Chad Greene, Facebook
1000 - 1100	Session 2	Shylock: An End-To-End Cybercrime Organization	Peter Kruse and Iurii Khvyl, CSIS Security Group A/S
1000 - 1100	Session 3	Reserved	To Be Announced
1000 - 1300	**Lab 1**	Lab: Malware Reverse Engineering: Understanding Obfuscation and Anti-Analysis Techniques	Dr. Brett Stone-Gross, Dell SecureWorks; Jason Milletary, Dell SecureWorks
1000 - 1300	**Lab 2**	Lab: Hands-On Targeting Attacks FOR LE-ONLY	To Be Announced
1100 - 1200	Session 4	Law Enforcement Case Study	César Lorenzana González, Ministerio del Interior
1100 - 1200	Session 5	Reserved	To Be Announced
1100 - 1200	Session 6	Reserved	To Be Announced

1200 - 1300	Session 7	Merchant Accounts in Monetizing Abusive Advertising	Stefan Savage, University of California San Diego and Chris Grier, University of California Berkeley
1200 - 1300	Session 8	Cybercrime, Bridging the Gap Between Organized Criminal Enterprises	Kirk Arthur, Special Agent USSS, Group Leader, Seattle ECTF, and David Dunn, Seattle Police, Seattle ECTF
1200 - 1300	Session 9	Reserved	To Be Announced
1300 -1430		Lunch	
1430 - 1530	Session 10	Scalable, Automated Baremetal Malware Analysis	Paul Royal, Georgia Tech Information Security Center (GTISC)
1430 - 1530	Session 11	VGT Threat Assessment and Scenarios for Cybercrime in 2020	Victoria Baines, European Cybercrime Center (EC3)
1430 - 1530	Session 12	Malware Monetization Through Advertising	Tommy Blizard and Nikola Livic, Microsoft
1430 - 1800	**Lab 3**	Lab: Intro to Netflow Analysis – and Stock Netflows	Natasha Hellberg, Bell Canada
1430 - 1800	**Lab 4**	Lab: Reserved	To Be Announced
1530 - 1630	Session 13	Mirror, Mirror on the Wall, Who is the Smartest Affiliate Fraudster of Them All?	Wesley Brandi, iPensatori
1530 - 1630	Session 14	Mobile Handset Forensics Internals	David Wolpoff, Kyrus Technologies
1530 - 1630	Session 15	European Cybercrime Centre (EC3) Being Hosted at EUROPOL	Jan Ellermann, EUROPOL Data Protection Office
1630 - 1700		Break	
1700 - 1800	Session 16	Using Graph Databases to Track, Identify, and Disrupt Malware	[redacted] ShadowServer and [redacted]
1700 - 1800	Session 17	Android Malware. Distribution, Disguise, and Damage	[redacted] G Data Software AG
1700 - 1800	Session 18	Reserved	To Be Announced
1800 - 1900	Session 19	TINBA - The Tiny Banker	Robert McArdle, Trend Micro
1800 - 1900	Session 20	Reserved	To Be Announced
1800 - 1900	Session 21	Reserved	To Be Announced

Wednesday, February 20, 2013

time		topic	presenter
0900 - 1000		Coffee and Networking	
1000 - 1100	Session 22	Cyber Espionage	Steven Adair, Terremark
1000 - 1100	Session 23	New Zealand Internet Task Force (NZITF)	Mike Seddon, Telecomm NZ
1000 - 1100	Session 24	Reserved	To Be Announced
1000 - 1300	**Lab 5**	Lab: DDoS Hands-On--Disintegrate Appliances While Fingerprinting Attacks Vectors	Terrence Gareau and David Fernandez, Prolexic Technologies
1000 - 1300	**Lab 6**	Lab: Windows Forensics	To Be Announced

s.19(1)

1100 - 1200	Session 25	Automated malware analysis using the Binary Analysis Characterization and Storage System (BACSS)	Supervisory Special Agent [redacted] and Information Technology Specialist Joseph Opacki, Federal Bureau of Investigation
1100 - 1200	Session 26	The impact of emerging technology on law enforcement & criminal justice agencies	Robert Hayes, Microsoft
1100 - 1200	Session 27	Hackers Profiling Project	Francesca Bosco, UNICRI
1200 - 1300	Session 28	CyberThreat Intel Program	Wesley Brandi, iPensatori and Rich Groves, Microsoft
1200 - 1300	Session 29	Ransomware 2.0 - International Dimensions and How a German Affiliate Got Unmasked	Mirko Manske, Bundeskriminalamt / Federal Criminal Police Office
1200 - 1300	Session 30	Cross Site Scripting Abuses	Randall Haimovici and James Devaney, Shook, Hardy and Bacon; Craig Clark, Facebook; and Bill Harmon, Microsoft
1300 -1430		Lunch	
1430 - 1530	Session 31	Law Enforcement Case Study	To Be Announced
1430 - 1530	Session 32	DDoS: Current and Evolving Frameworks	Terrence Gareau and David Fernandez, Prolexic Technologies
1430 - 1530	Session 33	Reserved	To Be Announced
1430 - 1800	**Lab 7**	Lab: Going from SMS to HTTP - Mobile Malware in the Past and Today	Andre Dornbusch and [redacted] Bundeskriminalamt / Federal Criminal Police Office, and [redacted] BFK
1430 - 1800	**Lab 8**	Lab: Windows Forensics (Session is a repeat from Wednesday morning)	To Be Announced
1530 - 1630	Session 34	ZyklonB Disclosed	Mirko Manske, Bundeskriminalamt / Federal Criminal Police Office
1530 - 1630	Session 35	A Glimpse Into The Future: The Evolution Of Cybercrime In The Next Decade	Ziv Mador, Trustwave SpiderLabs
1530 - 1630	Session 36	Xbox Fraud Scenarios/Xbox Forensics	Chris Compton and Doug Park, Microsoft
1630 - 1700		Break	
1700 - 1800	Session 37	So You Want to Take Over a Botnet...	Dave Dittrich, University of Washington
1700 - 1800	Session 38	Flame: Analysis of the Command and Control Servers and the Malware, Background Research and Findings	Thomas Hungenberg, CERT-Bund, and Costin Raiu, Kaspersky
1700 - 1800	Session 39	Case Study	To Be Announced
1800 - 1900	Session 40	Malicious and Criminal Activities on the Internet	[redacted] Technical Official, the NPA Japan
1800 - 1900	Session 41	Banking Trojans	Thomas Siebert, G Data Software AG
1800 - 1900	Session 42	Reserved	To Be Announced

Thursday, February 21, 2013

time		topic	presenter
0900 - 1000		Coffee and Networking	
1000 - 1100	Session 43	Bad Behavior: the Seamy Side of Search Ads Publisher Networks	Dennis Minium, Microsoft

s.19(1)

1000 - 1100	Session 44	Owning Bad Guys {and Mafia} with Javascript Botnets	Chema Alonso, Information64
1000 - 1100	Session 45	Reserved	To Be Announced
1000 - 1300	**Lab 9**	Lab: To Be Announced	Thorsten Holz, Ruhr-University Bochum
1000 - 1300	**Lab 10**	Lab: Web Injects	Matt Ziemniak, Qintel
1100 - 1200	Session 46	Financial Case Study	To Be Announced
1100 - 1200	Session 47	Real Time Collection and Analysis Methods and Tools	Paul Vixie, ISC
1100 - 1200	Session 48	DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System	Daisuke Inoue, Director, Cybersecurity Laboratory, National Institute of Information and Communications Technology, Japan
1200 - 1300	Session 49	Botnet Case Study	David Anselmi, Sr Manager of Investigations and Richard Boscovich, Assistant General Counsel, Digital Crimes Unit, Microsoft
1200 - 1300	Session 50	Cracolandia: the Brazilian eCrime world	Ronaldo Vasconcellos, Apura Cyber Intelligence Services (APURA-CIS)
1200 - 1300	Session 51	DNS Changer	Tom Grasso, NCFTA
1300 - 1430		Lunch	
1430 - 1530	Session 52	Malware Distribution Economy & Risks	Trevor Tonn, Lead Web Malware Analyst, Verisign iDefense
1430 - 1530	Session 53	Case Study	Keith Tagliaferri, Tiversa
1430 - 1530	Session 54	Traffic-Shaping-Based Real Time Threat Intelligence	Rich Groves, Microsoft
1430 - 1800	**Lab 11**	Lab: Hands-On Analysis of Win32/Georbot	Pierre-Marc Bureau, ESET
1430 - 1800	**Lab 12**	*Lab: Currently open, please submit suggestions to DCCEvent@microsoft.com*	
1530 - 1630	Session 55	ZyklonB Disclosed (Note: repeated session from Wednesday)	Mirko Manske, Bundeskriminalamt / Federal Criminal Police Office
1530 - 1630	Session 56	Reserved	To Be Announced
1530 - 1630	Session 57	Banks Fighting Back: Operation Honey Mule and Honey Bank	John Omernik, Zions Bancorp, and [redacted] Associated Bank
1630 - 1700		Break	
1700 - 1800	Session 58	CSI: Web	William Salusky, AOL
1700 - 1800	Session 59	Ransomware Trojans	Antti Tikkanen and Paolo Palumbo, F-Secure
1700 - 1800	Session 60	Reserved	To Be Announced
1800 - 1900	Session 61	Reserved	To Be Announced
1800 - 1900	Session 62	APT from Unlikely Sources (Note: repeated session from Tuesday)	Ryan McGeehan and Chad Greene, Facebook
1800 - 1900	Session 63	*Currently open, please submit suggestions to DCCEvent@microsoft.com*	

s.19(1)

Friday, February 22, 2013			
time		**topic**	**presenter**
0900 - 1000		Coffee and Networking	
1000 - 1100	Session 64	Law Enforcement Case Study	To Be Announced
1000 - 1100	Session 65	Mapping Out Organized Crime Networks	Peter Anaman, Microsoft
1000 - 1100	Session 66	Flame: Analysis of the Command and Control Servers and the Malware, Background Research and Findings (NOTE: Repeat of session on Wednesday)	Thomas Hungenberg, CERT-Bund, and Costin Raiu, Kaspersky
1000 - 1200	**Lab 13**	Lab: DDoS Hands-On--Disintegrate Appliances While Fingerprinting Attacks Vectors	Terrence Gareau and David Fernandez, Prolexic Technologies
1100 - 1200	Session 67	Mirror, Mirror on the Wall, Who is the Smartest Affiliate Fraudster of Them All? (NOTE: Repeat of session on Tuesday)	Wesley Brandi, iPensatori
1100 - 1200	Session 68	*Currently open, please submit suggestions to DCCEvent@microsoft.com*	
1100 - 1200	Session 69	*Currently open, please submit suggestions to DCCEvent@microsoft.com*	
1200 - 1230	**Plenary**	Closing Session	T.J. Campana, Director, Digital Crimes Unit, Microsoft

GOVERNMENT OF CANADA / GOUVERNEME DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval oas orginal dated)
Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) N°. d'aut de voyager (NAV)	Document No. RDIMS - N° du document SGGDI
	LNW9	688116

Type 2	Name of traveller - Nom du voyageur	Classification
	Jeffrey Bonvie	EC-05

Part A - Partie A

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	NS-NCSD-

Address - Adresse	Telephone No. - No. de téléphone	If different address, send cheque to: Si adresse differente, envoyer chèque à
340 Laurier Ave W.		[redacted] s.19(1)

Branch Contact - Personne ressource à la direction	Telephone No. - No. de téléphone
Jane Hayward	613-991-182

Purpose of travel - Objet du voyage	No. of days Nbre de jours	Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage (C	If no, would you like to request one? Les cas échéant, aimerier-vous en avoir une?
Attend conference on cybercrime		☐ Yes / Oui ☐ No / Non	☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival Départ - Arrivée	Transportation Transport Mode	Class	No. of meals prepaid Nbre de repas prépayés	Accommodation Hébergement	File locator number N°. de repérage du dossier
16-Feb-12	Ottawa	Frankfurt	17:15 - 06:45	Air	Business			
17-Feb-12	Frankfurt	Barcelona	9:50 - 11:45	Air	Business			
23-Feb-12	Barcelona, ESP	Frankfurt	10:00 - 12:25	Air	Business			
23-Feb-12	Frankfurt	Ottawa	13:55 - 16:16	Air	Business			

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales Item Type de dépenses	Estimated cost Coût estimatif	Non-standard - Spéciales Item Type de dépenses	Estimated cost Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$1,161.90	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory Location d'une voiture non intermédiaire (assurance-collision du	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dessus)	$0.00
Transportation Transport	$250.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) ☑ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Meals and incidentals Repas et frais accessoires	$851.73		
Other (Specify) - Autre (préciser)	$0.00		
		Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Part D - Partie D

Estimated Cost - Coût estimatif
Prepaid - Prépayé
$6,718.22
Other - Autre
$2,263.63
Trip Total - Coût total du voyage
$8,981.85

Funding - Financement

A) Travellers cheques / Chèques de voyage

Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00

B) Other advance / Autre avance

Cheque / Chèque	$0.00
Cash / Comptant	$0.00

Total funding requested (A + B)
Financement total demandé (A + B)
$0.00

Ticket pick-up date and location
Date et lieu de la collecte des billets

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Signature — Nov 26, 2012 — Date

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signat	Date
[signature]	Dec 27/12	[signature]	Jan 2, 2013

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount Montant du chèque	Date cheque required Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type Sous-type 8 | 0	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator Indicateur du fournisseur	Due Date Date d'échéance

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type Sous-type	Vendor Code Code du fourn.	Departmental Ref. No. No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		THC TH9	494-2001-PSABASE	

	Description	Financial encumberance No. No. de consignation de fonds
		500102303

Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature)	Requistion for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) Vérifié conform (TPSGC) (signature)		Date
Services officer (PWGSC) (signature) Agent responsible (TPSGC) (signature)	Signature	

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé			Amount/Montant
Airfare / Frais d'avion			$6,718.22
Train / Train			$0.00
Other / Autres			$0.00
			$6,718.22

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du ré	$193.65	6	$1,161.90
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du réperto			$0.00
			$1,161.90
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / *Location d'une voiture* **NON** *intermédiaire*			$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.550		$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$75.00	$250.00
	Airport - Hotel / Meetings		$50.00	
	Hotel - Airport		$50.00	
	Airport to Home		$75.00	
	Meeting - Meetings		$0.00	
Transportation / Transportation (No receipt)		$10.00		$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$250.00

Canadian	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$15.60		$0.00
Lunch / Déjeuners	$14.85		$0.00
Dinner / Dîners	$41.30	1	$41.30
Incidentals /Frais divers	$17.30	1	$17.30
		Total Canadian	$58.60

Barcelona, Spain	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$32.28	2	$64.56
Lunch / Déjeuners	$35.15	4	$140.60
Dinner / Dîners	$53.02	6	$318.12
Incidentals /Frais divers	$38.55	7	$269.85
		Total Barcelona, Spa	$793.13

Country #2	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$0.00		$0.00
Lunch / Déjeuners	$0.00		$0.00
Dinner / Dîners	$0.00		$0.00
Incidentals /Frais divers	$0.00		$0.00
		Total Country #2	$0.00
		GRAND TOTAL	**$851.73**

Business Phone / Téléphone d'affaires	$0.00
Airport Improvement Fee / Frais de l'Aeroport	$0.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses - Conference Fees	$0.00
	$0.00

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval as orginal dated)
Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A | Travel Authority No. (TAN) / N°. d'aut de voyager (NAV): LNW973029 | Document No. RDIMS - N° du document SGGDI: 726443

Type 2 | Name of traveller - Nom du voyageur: Patrick Clow | Classification: CS-04

Part A - Partie A

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	NS-NCSD-CCIRC

Address - Adresse	Telephone No. - No. de téléphone	If different address, send cheque to: / Si adresse différente, envoyer chèque à
257 Slater St	613-944-4074	
Branch Contact - Personne ressource à la direction	Telephone No. - No. de téléphone	
Danielle St-Louis	613-991-7738	

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Gov't Inc. Travel Card (ITC)? / Avez-vous une carte de voyage (C\	If no, would you like to request one? / Le cas échéant, aimerier-vous en avoir une?
Attend conference on cybercrime		☑ Yes / Oui ☑ No / Non	☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation / Transport: Mode	Class	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
16-Feb-12	Ottawa	Frankfurt	17:15 - 06:45	Air	Business			
17-Feb-12	Frankfurt	Barcelona	9:50 - 11:45	Air	Business			
23-Feb-12	Barcelona, ESP	Frankfurt	10:00 - 12:25	Air	Business			
23-Feb-12	Frankfurt	Ottawa	13:55 - 16:16	Air	Business			

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) / Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$1,391.58	Accomodation (green page hotel) / Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory / Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory / Location d'une voiture non intermédiaire (assurance-collision du	$0.00
Private vehicle requested by: / Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable / Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (préciser la «classe» si-dessus) ☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) ☑ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sou-chef ou l'équiv., S'il s'agit d'une classe non prévue à l'article 3.1.9)	$0.00
Transportation / Transport	$260.00		
Meals and incidentals / Repas et frais accessoires	$851.72		
Other (Specify) - Autre (préciser)	$10.00		
		Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Part D - Partie D

Estimated Cost - Coût estimatif: $6,718.22
Prepaid - Prépayé
Other - Autre: $2,513.30
Trip Total - Coût total du voyage: $9,231.52
Funding - Financement
A) Travellers cheques / Chèques de voyage
Cdn / Can: $0.00
US / É.U.: $0.00
Other / Autre: $0.00
B) Other advance / Autre avance
Cheque / Chèque: $0.00
Cash / Comptant: $0.00
Total funding requested (A + B)
Financement total demandé (A + B): $0.00
Ticket pick-up date and location
Date et lieu de la collecte des billets

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Signature | Date: Nov 27, 2012

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signa	Date
	Dec 27/12		

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier Indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 0					

Accounting Information / Renseignement comptables

Tyoe 4

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Clidification	Amount - Montant
		THC-T49	223-2001-PSABASE	

	Description	Financial encumberance No. / No. de consignation de fonds
		500102302

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		Date
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	

s.19(1)

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé			Amount/Montant
Airfare / Frais d'avion			$6,718.22
Train / Train			$0.00
Other / Autres			$0.00
			$6,718.22

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du ré	$231.93	6	$1,391.58
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répert			$0.00
			$1,391.58
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire			$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.550		$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$80.00	$260.00
	Airport - Hotel / Meetings		$50.00	
	Hotel - Airport		$50.00	
	Airport to Home		$80.00	
	Meeting - Meetings		$0.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$260.00

Canadian	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$15.50		$0.00
Lunch / Déjeuners	$15.00		$0.00
Dinner / Dîners	$41.30	1	$41.30
Incidentals /Frais divers	$17.30	1	$17.30
		Total Canadian	$58.60

Barcelona, Spain	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$32.28	2	$64.57
Lunch / Déjeuners	$35.15	4	$140.62
Dinner / Dîners	$53.02	6	$318.11
Incidentals /Frais divers	$38.55	7	$269.84
		Total Barcelona, Spa	$793.12

Country #2	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$0.00		$0.00
Lunch / Déjeuners	$0.00		$0.00
Dinner / Dîners	$0.00		$0.00
Incidentals /Frais divers	$0.00		$0.00
		Total Country #2	$0.00
		GRAND TOTAL	$851.72

Business Phone / Téléphone d'affaires	$10.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses - Conference Fees	$0.00
	$10.00

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
Microsoft Digital Crimes Consortium	From - *Du* : 18 Feb 2013	To - *Au* : 22 Feb 2013
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Barcelona, Spain	$18,318.83	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
The Microsoft Digital Crimes Consortium (DCC) is an event which draws together, researchers, educattors, policy makers and law enforcement to present and discuss all issues relating to cyber crime. Agenda is attached.	☒Yes/Oui ☐No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Jeffrey Bonvie	NCSD/NS	340 Laurier	613 990 9380
Patrick Clow	NCSD/NS	257 Slater	613 944 4074

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Study / Learning

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

Cyber security is a priority for Public Safety as the department continues to implement and advance Canada's Cyber Security Strategy for which cyber crime is a major concern. Governments, researchers / educators, law enforcement and even private entities all have a role to play in combatting cyber crime. Public Safety's representation at this event will allow for the staff to learn the latest developments, trends, and issues in the field of cyber crime from botnet take down issues to child exploitation on the internet. This conference is a unique and expansive opportunity to become engaged in the latest technical, operational and policy level discussions on cyber crime.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

There are no other government attendees, particularly Public Safety attendees to this event.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

Consultation has been with Microsoft only.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travellers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of participant's Director General
Nom du Directeur Générale du voyageur

Date: Dec 3/12

Reviewed by/

Date: Dec 6/12

Examiné par :	Director General, International Affairs Directorate *Directeur Générale, Direction générale des affaires internationales*	Date
Approved by/ ***Approuvé par*** :	[signature]	Dec 27/12
	Name of participant's Assistant Deputy Minister *Nom du sous-ministre adjoint du voyageur*	Date

PS023

Public Safety Canada / Sécurité publique Canada

PROTECTED WHEN COMPLETED (for privacy Act Statement see page 2)
PROTÉGÉ UNE FOIS REMPLIE (pour l'énoncé de la Loi, sur la protection des renseignements personnels, voir la page 2)

TRAINING APPLICATION AND AUTHORIZATION
DEMANDE ET AUTORISATION DE FORMATION

For PSC USE ONLY RÉSERVÉ À la CFP		

* REFER TO INSTRUCTIONS ON PAGE 2
VOIR LES INSTRUCTIONS SUR LA PAGE 2

DEPARTMENT USE ONLY RÉSERVÉ AU MINISTÈRE	2. Special needs * (enter indicator) Besoins spéciaux * (inscrire l'indicateur)
1. File number – Numéro de dossier	

☒ Original / Première ☐ Amendment / Modification ☐ Cancellation / Annulation

APPLICANT INFORMATION – RENSEIGNEMENTS SUR LE CANDIDAT

3. Family name – Nom de famille	Given name and initials – Prénom et initiales
Clow	Patrick

4. PRI – CIDP	5. Sex – Sexe	6. Classification Gr.	S.-gr.	Lev.Niv.	7. First official language – Première langue officielle
	☒ Male / Homme ☐ Female / Femme	CS		04	☒ (1) English / Anglais ☐ (2) French / Français

8. Position title – Titre du poste
Advisor

9. Employee's office telephone number / N° de téléphone de l'employé au bureau	Facsimile – Télécopieur	E-Mail – Courrier électronique
613 -944-4074		patrick.clow@ps-sp.gc.ca

10. Department name – Nom du ministère	11. Dept. Code – Code min.	12. Branch/Division – Direction/Division
Public Safety	0880	NCSD-CCIRC

13. Office, Workstation, mailing address – Adresse postale, bureau, poste de travail	City/Postal code – Ville/Code postal
257 Slater St	Ottawa, ON K1A 0P8

14. Supervisor's name and title – Nom du surveillant et titre	Telephone No. – N° de téléphone
Windy Anderson	613-991-7055

15. Supervisor's Office, Workstation, mailing address – Adresse postale, bureau, poste de travail du superviseur	City/Postal code – Ville/Code postal
257 Slater St	Ottawa, ON K1A 0P8

16. Objective of training *- Objective de la formation *

Expenditure Initiation Approval - L'engagement des dépenses	Date	Print Name- Imprimer Nom	Signature – (Authorized Signing Officer) / (Un dirigeant autorisé)
	JAN 0 2 2013	François Guimont	

Employee Name and Signature -Nom de l'employé et signature	Date	Print Name- Imprimer Nom	Employee's – Signature – Employé(e)
		Patrick Clow	

TRAINING INFORMATION – RENSEIGNEMENTS SUR LA FORMATION

17. Course code * Code du cours *	18. Course title – Titre du cours
N/A	Microsoft Digital Crimes Consortium

19. Location of training * - Lieu de formation *	20. Date of course - Date du cours						21. Departmental training program code * Code min. du programme de formation *
	From – Du			To - Au			
	Y-A	M	D-J	Y-A	M	D-J	
Barcelona Spain	13	02	17	13	02	22	

22. Time of training - Période retenue pour la formation	23. Duration of training * (nearest half-day) Durée de la formation * (plus proche demi-journée)	24. Language of course - Langue de cours
☐ (1) Outside working hours / En dehors des heures de travail ☒ (2) During working hours / Pendant les heures de travail	5	☒ English / Anglais ☐ French / Français ☐ Bilingual / Bilingue ☐ Other / Autre

25. Source of training - Source de la formation	26. Transit time (person-days) * Durée des déplacements (journées-personnes)	27. Province	28. Location* Lieu *
☐ (1) TPB/PSC DGPF/CFP ☐ (2) Dept'l Min. ☐ (3) Interdept'l Intermin. ☐ (4) University/College Université/Collège ☒ (5) Other Autre	1.5	OT	

29. FINANCIAL AUTHORIZATION – AUTORISATION FINANCIÈRE

Cost / Coût	Financial code (include R.C. codes only if several R.C.'s are sharing the costs, otherwise complete box 30) Code financier (indiquer des codes de C.R. uniquement si plusieurs C.R. se partagent les coûts, sinon remplir la case 30)	Estimated cost (planning purposes) Coût estimatif (à des fins de planification)	Actual cost (reporting purposes) Coût réel (à des fins de compte rendu)
Tuition fee / Reimbursement * Frais de scolarité / Remboursement * ☐ 0% ☐ 50% ☒ 100%		0	a) * 0
Travel / Living Déplacement / Subsistance		9231.52	b)
Other * Autres *			c) *
30. Responsibility centre (collator) code Code du centre de responsabilité (destinataire) 223	TOTAL	$9231.52	d)

Recipient organization code Code d'organization du/de la récipiendaire	Récipient référence code Code de référence du/de la récipiendaire

31. Financial signing authority (Certified that funds are available pursuant to **Section 32(1)FAA)** * Signataire autorisé en matière financière (Attestation de la disponibilité des fonds aux termes **du par. 32(1) LGFP)** *	Date	32. This candidate meets course selection criteria (Manager's approval) Le candidat satisfait aux critères de sélection du cours (approbation du gestionnaire)	
Print Name – Imprimer / Signature		Funds Commitment No. / Engagement des Fonds	

33. DEPARTMENTAL TRAINING COORDINATOR* - COORDONNATEUR DE LA FORMATION DU MINISTÈRE *

Remarks - Observations

Signature / Date

34. DEPARTMENTAL USE CODES * - CODES À L'USAGE DU MINISTÈRE *

A	B	C	
D	E	F	R S T U V W X Y Z

RDIMS / SGDDI # 473357

Public Safety Canada / Sécurité publique Canada

PROTECTED WHEN COMPLETED (for privacy Act Statement see page 2)
PROTÉGÉ LORSQU'IL EST REMPLI (pour l'énoncé de la Loi, sur la protection des renseignements personnels, voir la page 2)

TRAINING APPLICATION AND AUTHORIZATION
DEMANDE ET AUTORISATION DE FORMATION

For PSC USE ONLY RÉSERVÉ À la CFP		

s.19(1)

* REFER TO INSTRUCTIONS ON PAGE 2
VOIR LES INSTRUCTIONS SUR LA PAGE 2

DEPARTMENT USE ONLY RÉSERVÉ AU MINISTÈRE	2. Special needs * (enter indicator) Besoins spéciaux * (inscrire l'indicateur)
1. File number – Numéro de dossier	

☒ Original / Première ☐ Amendment / Modification ☐ Cancellation / Annulation

APPLICANT INFORMATION – RENSEIGNEMENTS SUR LE CANDIDAT

3. Family name – Nom de famille	Given name and initials – Prénom et initiales
Bonvie	Jeffrey

4. PRI – CIDP	5. Sex – Sexe	6. Classification			7. First official language – Première langue officielle
		Gr.	S.-gr.	Lev./Niv.	
	☒ Male / Homme ☐ Female / Femme	EC		05	☒ (1) English / Anglais ☐ (2) French / Français

8. Position title – Titre du poste
Advisor

9. Employee's office telephone number / N° de téléphone de l'employé au bureau	Facsimile – Télécopieur	E-Mail – Courrier électronique
613 -990-9380		jeff.bonvie@ps-sp.gc.ca

10. Department name – Nom du ministère	11. Dept. Code – Code min.	12. Branch/Division – Direction/Division
Public Safety		National Security / National Cyber Security

13. Office, Workstation, mailing address – Adresse postale, bureau, poste de travail	City/Postal code – Ville/Code postal
340 Laurier Ave West	Ottawa / K1A 0P8
14. Supervisor's name and title – Nom du surveillant et titre	Telephone No. – N° de téléphone
Adam Hatfield	613-993-9521
15. Supervisor's Office, Workstation, mailing address – Adresse postale, bureau, poste de travail du superviseur	City/Postal code – Ville/Code postal
340 Laurier Ave West	Ottawa / K1A 0P8

16. Objective of training *- Objective de la formation *

To attend a conference on cyber crime for the purpose of becoming more informed of global trends, research and tactics relating to combating cyber crime.

	Date / Print Name- Imprimer Nom	Signature / (Authorized Signing Officer) / (Un dirigeant autorisé)
Expenditure Initiation Approval - L'engagement des dépenses	JAN 0 2 2013	
Employee Name and Signature -Nom de l'employé et signature	Date / Print Name- Imprimer Nom 11- 21- 2012 Jeffrey Bonvie	Employee's – Signature – Employé(e)

TRAINING INFORMATION – RENSEIGNEMENTS SUR LA FORMATION

17. Course code * / Code du cours *	18. Course title – Titre du cours
N/A	Microsoft Digital Crimes Consortium

19. Location of training * - Lieu de formation *
Hotel Rey Juan Carlos
Avinguda Diagonal, 661 08028
Barcelona Spain

20. Date of course - Date du cours						21. Departmental training program code * / Code min. du programme de formation *
From – Du			To - Au			
Y-A	M	D-J	Y-A	M	D-J	
13	02	17	13	02	22	

22. Time of training - Période retenue pour la formation	23. Duration of training * (nearest half-day) Durée de la formation * (plus proche demi-journée)	24. Language of course - Langue de cours
☐ (1) Outside working hours / En dehors des heures de travail ☒ (2) During working hours / Pendant les heures de travail	5	☒ English / Anglais ☐ French / Français ☐ Bilingual / Bilingue ☐ Other / Autre

25. Source of training - Source de la formation	26. Transit time (person-days) * Durée des déplacements (journées-personnes)	27. Province	28. Location* Lieu *
☐ (1) TPB/PSC DGPF/CFP ☐ (2) Dept'l Min. ☐ (3) Interdept'l Intermin. ☐ (4) University/College Université/Collège ☒ (5) Other Autre	2.0	N/A	SPAIN

29. FINANCIAL AUTHORIZATION – AUTORISATION FINANCIÈRE

Cost / Coût	Financial code (include R.C. codes only if several R.C.'s are sharing the costs, otherwise complete box 30) Code financier (indiquer des codes de C.R. uniquement si plusieurs C.R. se partagent les coûts, sinon remplir la case 30)	Estimated cost (planning purposes) Coût estimatif (à des fins de planification)	Actual cost (reporting purposes) Coût réel (à des fins de compte rendu)
Tuition fee / Reimbursement * Frais de scolarité / Remboursement * ☒ 0% ☐ 50% ☐ 100%		0	a) * 0
Travel / Living Déplacement / Subsistance		8891.85	b)
Other * Autres *			c) *
30. Responsibility centre (collator) code / Code du centre de responsabilité (destinataire) 494	TOTAL	8891.85	d)

Recipient organization code / Code d'organization du/de la récipiendaire	Récipient référence code / Code de référence du/de la récipiendaire

31. Financial signing authority (Certified that funds are available pursuant to **Section 32(1)FAA**) * Signataire autorisé en matière financière (Attestation de la disponibilité des fonds aux termes **du par. 32(1) LGFP**) *	Date	32. This candidate meets course selection criteria (Manager's approval) Le candidat satisfait aux critères de sélection du cours (approbation du gestionnaire)	
Print Name – Imprimer / Signature		Funds Commitment No. / Engagement des Fonds	

33. DEPARTMENTAL TRAINING COORDINATOR* - COORDONNATEUR DE LA FORMATION DU MINISTÈRE *

Remarks - Observations

Signature / Date

34. DEPARTMENTAL USE CODES * - CODES À L'USAGE DU MINISTÈRE *

A	B	C	
D	E	F	R S T U V W X Y Z

RDIMS / SGDDI # 473357

Public Safety Canada
Senior Assistant Deputy Minister

Ottawa, Canada
K1A 0P8

Sécurité publique Canada
Sous-ministre adjoint principal

SECRET (with attachments)

DATE:

File No.: 391713
RDIMS No.: IS1860-725247

MEMORANDUM FOR THE DEPUTY MINISTER

INTERNATIONAL TRAVEL AUTHORITY FOR ALEXANDRE GRIGSBY TO ATTEND THE UNITED NATIONS GROUP OF GOVERNMENTAL EXPERTS ON INFORMATION SECURITY AND OTTAWA 5 MEETING GENEVA, SWITZERLAND, JANUARY 13-19, 2013

(Decision sought)

ISSUE

Alexandre Grigsby, Analyst, Policy and Issues Management, National Cyber Security Directorate, is requesting international travel authority to attend the second meeting of the United Nations Group of Governmental Experts on Information Security (GGE) in Geneva, Switzerland, January 13-18, 2013, and attend a meeting of the Ottawa 5 on January 19, 2013.

BACKGROUND

The United Nations (UN) established the GGE in 2004-05 to study "existing and potential threats in the sphere of information security" and possible cooperation mechanisms to address them. Permanent members of the UN Security Council were asked to contribute to the work of this group, along with a rotating membership from other states. The results of GGE studies are forwarded as recommendations to the UN General Assembly.

The GGE process has become an important venue for talks on the future of cyber space, as GGE reports can form the basis for future UN resolutions. Countries participating in the GGE fall into two distinct groups that each advocates opposing visions for cyber security and Internet governance. Western countries, including the Five Eyes and other European states, have argued forcefully that current Internet governance arrangements work well under a multi-stakeholder model that includes the private sector and civil society; that existing international law should apply online; and that cyber security is a matter for internal state policy and should largely be focused on the integrity of networks themselves. In contrast, Russia and China have argued that Internet governance should be brought under UN control with only states having a decision in the evolution of communications technologies; that existing law is no longer relevant and that new cyberspace treaties are required; and that

Canada

.../2

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		T64	496-2001-PSABASE-500102223	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the *Payment Requisition Regulations* / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les *réquisitions de paiements.*	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		Date
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	

existing law is no longer relevant and that new cyberspace treaties are required; and that cyber security should be understood as "information security", which includes the policing of content online and curtailing the democratic right of freedom of speech.

While the GGE has previously held two rounds of studies, only the second meeting in 2009-2010 produced a consensus report to the General Assembly. The current session of GGE talks began in August 2012 in New York. Canada participated in these talks for the first time, joining the Permanent Five members of the Security Council, as well as Australia, Germany, Japan, Indonesia, India, Belarus, Estonia, Argentina, and Egypt. The tone of this meeting was positive and constructive, with many of the Canadian delegation's suggestions being supported by the larger group. A report of the proceedings is attached (**TAB A**).

Australia is chairing the GGE and has drafted a summary of the discussions that will likely form the basis of a final report. Negotiations around the Australian document will be the focus of this second session of the GGE.

CONSIDERATIONS

Mr. Grigsby will support Mr. Michael Walma, Director, Policy and Planning, Department of Foreign Affairs and International Trade, who will lead the Canadian Delegation (CANDEL). Legal officers from the Department of Foreign Affairs and the Department of National Defence, as well as a diplomat from the Canadian Permanent Mission to the United Nations in Geneva will complete the delegation.

Participating in these meetings represents a key commitment to our allies, and is a Tier I priority within the Department's International Strategic Framework. Moreover, departmental involvement is vital to preventing the international community from moving in a policy direction that fundamentally undermines Canada's values and national security objectives.

Mr. Grigsby's expertise on cyber security matters will be essential for the CANDEL, and DFAIT has requested that Mr. Grigsby specifically be assigned by Public Safety Canada to participate in the delegation. Mr. Grigsby supported CANDEL in the first round of GGE discussions in New York, and he is also a member of Canada's delegation to the World Conference on International Telecommunications, acting as a cyber security specialist for negotiations around the International Telecommunications Regulations. His knowledge of cyber security issues will be required as the upcoming session will focus primarily on negotiating changes to the Chair's summary from the first meeting.

Following the GGE meeting, a working level meeting on international cyber events in 2013, and share information on domestic cyber security initiatives. Mr. Grigsby will attend on behalf of Public Safety

s.15(1) - Int'l

.../3

Canada. This will be more cost effective than sending Public Safety Canada's regular [redacted], Mr. Bob Gordon, to attend a one day meeting.

This trip will cost approximately $ $10,245.90. All costs related to this request fall within my sector's allocated Travel/Hospitality/Conference cap for this fiscal year.

RECOMMENDATION

It is recommended that you approve Mr. Grigsby's travel request. Should you agree, your signature is sought on the Travel Authority and Advance form (**TAB B**). The International Travel Request form is also attached for your information (**TAB C**).

Should you require additional information, please do not hesitate to contact me or Robert Dick, Director General, National Cyber Security at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Gary Robertson
Assistant Deputy Minister,
Corporate Management Branch

Enclosures: (3)

I approve:

_____
François Guimont

I do not approve:

_____
François Guimont

Prepared by : Alexandre Grigsby

s.15(1) - Int'l

Pages 477 to / à 480

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

GOVERNMENT OF CANADA / GOUVERNE DU CANAD

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande

☐ Amended (Same levels of approval oas orginal dated)

Modifications (approbation par des agents du même niveau que

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. RDIMS - N° du document SGGDI
	LNW9	729205

Type 2

Name of traveller - Nom du voyageur: Alex Grigsby

Classification: EC-03

Part A - Partie A

Department - Ministère: Public Safety Canada

Branch / Division / Group - Direction / Division / Groupe: NS-NCSD-Policy

Address - Adresse: 11C-340 Laurier Avenue West

Telephone No. - No. de téléphone: 949-4243

If different address, send cheque to: / Si adresse differente, envoyer chèque à

Branch Contact - Personne ressource à la direction: Jane Hayward

Telephone No. - No. de téléphone: 613-991-182

Purpose of travel - Objet du voyage: UN GGE Meeting and Ottawa 5 Meeting

No. of days / Nbre de jours: 10

Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage: ☑ Yes / Oui ☐ No / Non

If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une? ☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival Départ - Arrivée	Transportation Transport Mode	Transportation Transport Class	No. of meals prepaid Nbre de repas prépayés	Accommodation Hébergement	File locator number N°. de repérage du dossier
11-Jan-13	Ottawa	Montreal	18:05-18:53	Air	Business			
12-Jan-13	Montreal	Geneva	20:50-10:15 +1	Air	Business	2	hôtel Jade	
20-Jan-13	Geneva	Montreal	12:05-14:20	Air	Business	2		
20-Jan-13	Montreal	Ottawa	16:00-16:44	Air	Business			

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$2,394.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory Location d'une voiture non intermédiaire (assurance-collision du	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dessus)	$0.00
Transportation Transport	$260.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) 3.1.9 ☑ Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une	
Meals and incidentals Repas et frais accessoires	$1,536.90		
Other (Specify) - Autre (préciser) Baggage fees	$55.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

The length of travel exceeds 9 hours as per Travel Policy.

Part D - Partie D

Estimated Cost - Coût estimatif

Prepaid - Prépayé

$6,000.00

Other - Autre

$4,245.90

Trip Total - Coût total du voyage

$10,245.90

Funding - Financement

A) Travellers cheques / Chèques de voyage

Cdn / Can

US / É.U. $0.00

Other / Autre $0.00

B) Other advance / Autre avance

eque / Chèque $0.00

ash / Comptant $0.00

Total funding requested (A + B)

Financement total demandé (A + B)

$0.00

Ticket pick-up date and location
Date et lieu de la collecte des billets

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Alexandre Grigsby — asperomail — December 6 2012

Signature — Date

Recommended by (signature) - Recommandé par (signatu	Date	Approved by (signature) - Approuvé par (	Date

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicat / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0					

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		T64	496-2001-PSABASE-500102223	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)

Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Cheque No. - N° du chèque

Verified correct (PWGSC) (signature) / *Vérifié conform (TPSGC) (signature)*

Date

Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)

Signature

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$6,000.00
Train / Train	$0.00
Other / Autres	$0.00
	$6,000.00

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE**	$299.25	8	$2,394.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du r			$0.00
			$2,394.00
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire			$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour emp	0.550	0.0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$25.00	$260.00
	Airport - Hotel / Meetings		$30.00	
	Hotel - Airport		$30.00	
	Airport to Home		$25.00	
	Meeting - Meetings		$150.00	
Transportation / Transportation (No receipt)		**$10.00**		$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$260.00

Canada	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.50**	0	$0.00
Lunch / Déjeuners	**$15.00**	0	$0.00
Dinner / Dîners	**$41.30**	0	$0.00
Incidentals /Frais divers	**$17.30**	1	$17.30
		Total Canada	$17.30

Geneva, Switzerland	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$41.98**	0	$0.00
Lunch / Déjeuners	**$55.10**	8	$440.80
Dinner / Dîners	**$73.47**	8	$587.76
Incidentals /Frais divers	**$54.56**	9	$491.04
		Total Geneva, Sw	$1,519.60

	Rate / Tarif	No. / Nbre	Amount/Montant
		GRAND TOTAL	**$1,536.90**
Business Phone / Téléphone d'affaires			$0.00
Airport Improvement Fee / Frais de l'Aeropart			$0.00
Cash Advance Fee / Frais d'avances			$0.00
Misc. Business Services / Diverses charges d'affaires			$0.00
Miscellaneous / Diverses -			$55.00
			$55.00

Public Safety Canada / Sécurité publique Canada

s.15(1) - Int'l

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
	From - *Du* :	To - *Au* :
United Nations Group of Governmental Experts (UN GGE) (Second Meeting) and Five Eyes cyber meeting	January 13, 2013	January 19, 2013
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
UN office in Geneva (Place des Nations) Geneva, Switzerland	$$10,688.25	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
Experts from 15 countries will study existing and potential threats in the sphere of information security (also known as cyber security) and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States (A/RES/66/24 - attached). This second session will take place from Jan 14-18, 2013. The Five Eyes cyber meeting will take place on Jan 19 and cover outcomes from the GGE	☒Yes/Oui ☐No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Alexandre Grigsby	National Cyber Security Directorate - NS Branch	340 Laurier Ave, 11th Floor	613-949-4243

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.) *Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)*

Role: Member of the Canadian Delegation and principal subject matter expert on cyber security.

Purpose:

1. Promote the notion that existing international law, including human rights law and the law of armed conflict, apply in cyberspace; and

2. Develop practical confidence building measures to minimize the collective risk of a cyber incident which could threaten international peace and security.

Background: Pursuant to UN General Assembly Resolution sponsored by Russia, a GGE has met since 2004-05 to study "existing and potential threats in the sphere of information security" and develop collective measures to address them. In 2009-10, the Group issued its first and only consensus report which recommended, among other things, that states "discuss norms pertaining to the use of information and telecommunications technologies (ICTs) and develop "confidence building, stability and risk reduction measures to address the implication of state use of ICTs."

The GGE is comprised of the five permanent members of the UN Security Council (China, France, Russia, the United Kingdom (U.K.), and the U.S.) and ten other countries that wish to join based on geographic distribution. Canada will be participating in the discussion for the first time. Canada will be represented by Michael Walma, Director, Policy and Planning at the Department of Foreign Affairs and International Trade (DFAIT). Public Safety initially recommended to DFAIT that Canada join the GGE and has led the development of Canada's position on the items expected to be discussed.

s.15(1) Int'l

The first GGE session was held in August, 2012 in New York and the final session of the GGE is scheduled for 3-7 June, 2013 in New York.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

As the Department works to implement the Canada's Cyber Security Strategy (RPP priority #4), participating at the UN GGE will strengthen Canada's cyber security by promoting norms, rules, and measures to guide state activity in cyberspace to avoid a potentially devastating cyber incident which could not only impact Canada's security, but that of the international community.

Further, the GGE process is expected to be the driving international venue for cyber policy development. Canada's traditional allies are heavily vested in this process and Australia chairs the GGE (a Tier 1 priority). Participation is a key commitment to our allies, and is vital to ensure that the international community does not pursue actions and approaches in cyberspace that would fundamentally undermine Canada's values and security objectives.

The Five Eyes cyber meeting is a forum where the allies discuss approaches to cyber security issues domestically and internationally. It is an International Strategic Framework Tier 1 priority.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

Mr. Grigsby will support Michael Walma, Director, Policy and Planning at DFAIT who will lead the Canadian Delegation (CANDEL). A member of DND's Judge Advocate General will be on the CANDEL in addition to a Candian diplomat from the Canadian Permanent Mission to the United Nations in Geneva.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

Consulted within Public Safety and with the DFAIT. Further, Canada's key allies, notably the U.S., U.K., and Australia have all been made aware of Public Safety's attendance at the GGE.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of paticipant's Director General
Nom du Directeur Générale du voyageur

Dec 6/12
Date

Reviewed by/
Examiné par :

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

Date

Approved by/
Approuvé par :

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date

PS023

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

CONFIDENTIAL

DATE: OCT 30 2012

File No.: 391010
RDIMS No.: 1860-708973

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, CMB

INTERNATIONAL TRAVEL AUTHORITY FOR ROBERT GORDON AND MARK MATZ TO ATTEND THE MERIDIAN CONFERENCE, BERLIN, GERMANY NOVEMBER 26-29, 2012

(Decision sought)

ISSUE

Mr. Robert Gordon and Mr. Mark Matz are requesting approval to travel to Berlin, Germany, November 26-29, 2012, to attend the Meridian Conference.

BACKGROUND

The Meridian Conference, an annual event bringing together representatives from 29 countries, serves as a forum for policy level discussions on critical information infrastructure protection (CIIP). A formal invitation from the German Federal Government, the Ministry of the Interior, has been extended for this event **(TAB A)**.

In the past, Public Safety Canada (PS) has used the annual event to promote its CIIP initiatives. Mr. Gordon delivered a keynote address on *Canada's Cyber Security Strategy* at the 2010 event and led a session highlighting Canada's efforts to implement the *Strategy* the following year.

.../2

Mr. Gordon accepted an invitation from Dr. Michael Pilgermann from the German Federal Ministry of the Interior to be a member of the program committee for the 2012 Meridian Conference. He attended an initial meeting of the committee in Berlin, Germany, March 21-22, 2012, and has been participating in monthly teleconference calls to develop the program. The following countries were also represented on the committee: Argentina, France, Japan, The Netherlands, Qatar, Singapore, Switzerland, Sweden, Taiwan, the United Kingdom, and the United States (U.S.).

CONSIDERATIONS

The Meridian Conference offers Canada an excellent opportunity to engage international partners on a broad range of cyber security issues

At Mr. Gordon's suggestion, PS and the Department of Homeland Security, U.S., will provide a joint presentation highlighting the effectiveness of collaboration and leveraging the capabilities of others in developing national cyber awareness campaigns. Mr. Gordon will present the Canadian portion of the presentation. This will be the first time a binational presentation has been given at a Meridian Conference. It will be an opportunity to highlight Canada's achievements with its cyber awareness campaign and the benefits of collaboration both internationally and with the private sector.

Following the conference, on the afternoon of November 28 and the next day, arrangements will be made for bilateral discussions with representatives of the Federal Ministry of the Interior (FMI) and a meeting at the Canadian Embassy. Discussions with the FMI will focus on the innovative work being done by the German National Cyber Security Council and the National Cyber Response Center with a particular focus on their engagement with the private sector and related policy initiatives.

I recommend that Mr. Mark Matz, Director, Policy and Issues Management, accompany Mr. Gordon. Mr. Matz will become PS' representative at future Meridian conferences following Mr. Gordon's departure from PS in April 2013.

The approximate cost of the travel for both Mr. Matz and Mr. Gordon is $21,363.70 which falls within the Deputy Minister's approval authority of $25,000. All costs related to this request fall within my sector's allocated Travel, Hospitality, Conference cap for this fiscal year.

.../3

RECOMMENDATION

It is recommended that you approve this travel. Should you agree, your signature is sought on the attached Conference Authorization **(TAB B)** and Travel Authority and Advance Forms **(TAB C)**. My approval is noted on the International travel request **(TAB D)**.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Robert Dick, Director General, National Cyber Security at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (4)

I approve:

NOV - 7 2012

Graham Flack
Acting Deputy Minister

Prepared by: Robert Gordon

Federal Ministry
of the Interior

MERIDIAN
Connecting and Protecting

Dear colleague,

on behalf of the German Federal Government, the Ministry of the Interior is pleased to invite delegates from your country to the Meridian 2012 International Conference, taking place on the premises of the Foreign Affairs Office, Berlin from November 26 – 28. This year's conference will focus on "CIIP policy challenges and common denominators".

The Meridian Conference as part of the Meridian Process provides a unique opportunity for the international community to take collective action on Critical Information Infrastructure Protection (CIIP). The process is designed to promote trust and partnership through the sharing of experience and best practices from around the world.

The Federal Minister of the Interior, Dr. Hans-Peter Friedrich, is going to open the conference on the 26th of November 2012 and welcome the participants. Further on in the agenda, interactive workshops and robust discussions promise to empower senior policy makers to work together to address Critical Information Infrastructure Protection challenges.
Meridian 2012 will focus on the policy challenges arising from Cybersecurity more and more impacting CIIP. Discussions under the three relevant perspectives: economical, legislative as well as preparedness are aiming to identify common denominators for a major step forward in protecting CII on a global scale – please consult our website for more information and the preliminary agenda.
We look forward to a dynamic conference that will continue in the Meridian tradition of connecting countries and encouraging governments to collaboratively take action to improve the protection of Critical Information Infrastructure.

For registration, please provide your details on the website. We will check available capacities and – after successful verification – you will receive a registration confirmation by email. In addition, you will receive your personal login details for the login area on the website. Please note that you are not registered without the official confirmation.

Sincerely,
Martin Schallbruch
Director General for Information Technology, Federal Ministry
of the Interior
www.meridian2012.org

BERLIN 2012

Pages 489 to / à 490

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Meridian 2012 International Conference

It is the pleasure of the German Federal Ministry of the Interior to extend a warm welcome to all delegates invited to participate in Meridian 2012 International Conference.

read more

Federal Foreign Office

The headquarters of the Federal Foreign Office at the Werderscher Markt has a particularly unusual history.

read more

Imprint

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
Meridian Process Annual Conference and Meetings with Federal Ministry of the Interior (FMI) and Canadian Embassy.	From - *Du* : November 26, 2012	To - *Au* : November 29 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Berlin, Germany	$ 21,363.71	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
The proposed agenda is attached. Discussions with at the FMI will focus on the innovative work being done by the German National Cyber-Security Council and the National Cyber Response Center with a particular focus on their engagement with the private sector and related policy initiatives.	☒Yes/Oui ☐No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Robert Gordon Mark Matz	NS- National Cyber Security Directorate	340 Laurier Ave, 11D	613-949-7380 613-993-9635

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

At Mr. Gordon's suggestion, Public Safety Canada and the Department of Homeland Security, United States, will provide a joint presentation highlighting the effectiveness of collaboration and leveraging the capabilities of others in developing national cyber awareness campaigns. Mr. Gordon will present the Canadian portion of the presentation. This will be the first time a binational presentation has been given at a Meridian Conference. It will be an opportunity to highlight Canada's achievements with its cyber awareness campaign and the benefits of collaboration both internationally and with the private sector. Mr. Matz will become PS's representative at future Meridian conferences following Mr. Gordon's departure from PS in April 2013.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

The Meridian Conference offers Canada an excellent opportunity to engage international partners on a broad range of cyber security issues

s.15(1) - Int'l

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

None

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

None

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of paticipant's Director General
Nom du Directeur Générale du voyageur

Date

Reviewed by/
Examiné par :

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

Date

Approved by/
Approuvé par :

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date

PS023

Public Safety Canada | Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: October 23, 2012

To – A

Graham Flack
A/Deputy Minister
Public Safety Canada

Requested by – Demandé par

Robert Gordon
Special Advisor Cyber Security
National Cyber Security Directorate
National Security

Name of Conference – Titre de la conférence

Meridian Process Annual Conference

Type of Conference – Genre de conférence

☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

Official Host – Hôte officiel

Federal Ministry of the Interior - Germany

Duration of Conference – Durée de la conférence

From / Du: November 26 2012 To / À: November 28 2012

Location - Adresse

Doha, Qatar

Agenda – Ordre du jour

Attached.

Purpose of Participation - Object de la participation

At Mr. Gordon's suggestion, Public Safety Canada and the Department of Homeland Security, United States, will provide a joint presentation highlighting the effectiveness of collaboration and leveraging the capabilities of others in developing national cyber awareness campaigns. Mr. Gordon will present the Canadian portion of the presentation. This will be the first time a binational presentation has been given at a Meridian Conference. It will be an opportunity to highlight Canada's achievements with its cyber awareness campaign and the benefits of collaboration both internationally and with the private sector.

Financial Coding – Code financier

475 - 500 - PSCYBINTENG - 5000101302 -

Estimated Total Cost / Coût total prévu

$ 10,670.55

Recommended by – Recommandé par		Branch Approval – Approbation de la direction	
Signature	Date	Signature	Date
Assistant Deputy Minister – Sous-ministre adjoint		Deputy Minister – Sous-ministre	
Signature	Date: 30/11/2	Signature	Date: NOV 07 2012

MS-18 (4/04)

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande

☐ Amended (Same levels of approval oas orginal dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N° d'aut de voyager (NAV)	Document No. - N° du document
	LNW9	

Type 2	Name of traveller - Nom du voyageur	Classification
	Robert Gordon	EX-05

Part A - Partie A

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	National Security - DGO

Address - Adresse	Telephone No. - No. de téléphone	If different address, send cheque to: / Si adresse différente, envoyer chèque à
340 Laurier Ave. West	613-949-7380	
Branch Contact - Personne ressource à la direction	Telephone No. - No. de téléphone	
Jane Hayward	613-991-1982	

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Govt Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)?	If no, would you like to request one? / Le cas échéant, aimerier-vous en avoir un
To attend Meridian conference and meting in Berlin	7	☑ Yes / Oui ☐ No / Non	☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation / Transport: Mode	Flight Class	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N° de
November 24 2012	Ottawa	Berlin	17:15 - 08:55 (next day)	Air	Business	1		
November 30 2012	Berlin	Ottawa	07:00 - 15:45	Air	Business	1		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) / Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$759.40	Accomodation (green page hotel) / Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory / Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory / Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: / Voiture particulière demandée par: ☑ Traveller / Voyageur ☐ Employer / Employeur — Public Liability and Property Damage min $1 million. Deductibles NON reimbursable / Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$37.40	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (préciser la <classe> si-dussus)	$0.00
Transportation / Transport	$490.00	☐ First class (Deputy Head or equivalent approval) / Prem. Classe (approuvee par le sou-chef ou l'équiv.) — Business class / Other-Upgraded (other than article 3.1.9 ☑ Assistant Deputy Head or equivalent approval) / Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv.. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Meals and incidentals / Repas et frais accessoires	$639.26		
Other (Specify) - Autre (préciser) — Business phone, baggage, internet, cash advance	$155.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Part D - Partie D

Estimated Cost - Coût estimatif

Prepaid - Prépayé

$8,589.49

Other - Autre

$2,081.06

Trip Total - Coût total du voyage

$10,670.55

Funding - Financement

A) Travellers cheques / Chèques de voyage

Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00

B) Other advance / Autre avance

Cheque / Chèque	$0.00
Cash / Comptant	$0.00

Total funding requested (A + B) / Financement total demandé (A + B)

$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Robert Gordon — Signature — 2012/10/23 — Date

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date
Lynda Clairmont	30/10	Graham Flack	NOV 07 2012

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Detail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'echeance
	8 | 0					

Accounting Information / Renseignement comptables

Type 4

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No / No. de ref. Du ministère	Coding - Cidification	Amount - Montant
		THC NCSD - TIB	475- PSCYBINTLENG -	

	Description	Financial encumberance No. / No. de consignation de fonds
		5001013O2

Department pre-audit and account verification (signature) / Agent min. chargé de la ver. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demande pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifie au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du cheque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		Date
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$8,589.49
Train / Train	$0.00
Other / Autres	$0.00
	$8,589.49

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$151.88	5	$759.40
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	$0.00	0	$0.00
			$759.40
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00
	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.550	68	$37.40
	Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage		$15.00	$15.00
Taxi/Limo — Home to Airport		$0.00	$475.00
Taxi/Limo — Airport - Hotel - Meetings		$100.00	
Taxi/Limo — Hotel - Airport		$100.00	
Taxi/Limo — Airport to Home		$75.00	
Taxi/Limo — Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)			$0.00
Ferry & Miscellaneous		$0.00	$0.00
			$490.00

Canada	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$15.50	0	$0.00
Lunch / Déjeuners	$15.00	0	$0.00
Dinner / Dîners	$41.30	0	$0.00
Incidentals /Frais divers	$17.30	1	$17.30
	Canada	Meals	$17.30
Berlin	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners (receipts required) Estimated rate	$38.62	1	$38.62
Lunch / Déjeuners	$34.66	3	$103.98
Dinner / Dîners	$48.94	5	$244.70
Incidentals /Frais divers	$39.11	6	$234.66
	Berlin	Meals	$621.96
Country 3	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners (receipts required) Estimated rate	$0.00	0	$0.00
Lunch / Déjeuners	$0.00	0	$0.00
Dinner / Dîners	$0.00	0	$0.00
Incidentals /Frais divers	$0.00	0	$0.00
	Country 3	Meals	$0.00
	TOTAL MEALS		**$639.26**

Business Phone / Téléphone d'affaires	$50.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$5.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses -	$100.00
	$155.00

Public Safety Canada | Sécurité publique Canada

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions** Travel - Robert Gordon - Berlin Nov 2012
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☒ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☒ Other Specify: ITR

☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?
	Have I completed all the paperwork requested by the Contracting Material Management group? ☒ Is the Sole Source Checklist complete and attached? ☒ Is the Competitive Contract Checklist complete and attached?
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☒ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☒ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

	Purchase Requisition #	Purchase Order #	Funds Commitment #:	RDIMS #
			500101302	716562

INSTRUCTIONS FOR COMPLETION OF SECTION 32 CHECKLIST

These instructions are meant to assist staff in the preparation of the Section 32 checklist for Grants and Contributions payments. The numbers used relate to the same number on the checklist.

Legend: ☒ **= completed or has been considered**

1) Use the Delegated Financial Signing Authorities matrix located at: http://icarchive/foryou/divisions/comptroller/dfsa/_fl/dfsa-matrix-dept-eng.pdf to ensure that the person exercising Expenditure Initiation authority has the authority delegated to his/her position.

2) Forms can be found in Microsoft Office/Excel templates when starting a new document.

3) Ensure that you have the authority to sign under Section 32: a) by using the Delegated Financial Signing Authorities matrix located at: http://icarchive/foryou/divisions/comptroller/dfsa/_fl/dfsa-matrix-dept-eng.pdf; and b) by the completion of a Financial Authority Specimen Signature Record.

4) Run a free balance report in SAP to ensure that you have sufficient unencumbered funds to legally sign Section 32.

5) These forms are applicable to the Contracting and Procurement Unit and may not be applicable to expenditures such as Hospitality and Travel.

6) Enter the commitment into the SAP system and verify that the correct g/l, cost center, amount, vendor and description are entered. When the commitment is entered and saved please provide the Fund Commitment/ Purchase Order number on the indicated line.

7) When entering into a contract for the purchase of a good, please consider if the following will be a capital asset as per the criteria stated. Please contact External Reporting Group within the Financial Services & Systems Division (FSSD) for further instruction on ensuring the proper coding/description.

Public Safety Canada | Sécurité publique Canada
Senior Assistant Deputy Minister | Sous-ministre adjoint principal
Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:

File No.: 390455
RDIMS No.: IS1860-691349

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
via: Gary Robertson, Assistant Deputy Minister, Corporate Management Branch

INTERNATIONAL TRAVEL AUTHORITY FOR ALEXANDRE GRIGSBY TO ATTEND THE INTERNET GOVERNANCE FORUM BAKU, AZERBAIJAN, NOVEMBER 6-9, 2012

(Decision sought)

ISSUE

Alexandre Grigsby, Analyst, Policy and Issues Management, National Cyber Security Directorate, is requesting international travel authority to attend the Internet Governance Forum (IGF) in Baku, Azerbaijan, November 6-9, 2012.

BACKGROUND

The IGF is a major annual conference where government representatives, academics, businesses, and civil society discuss current and emerging Internet issues. It embodies the multistakeholder model of Internet governance that Canada seeks to sustain and promote internationally. This stands in contrast to the top-down model advocated by a number of countries, such as [redacted] that would rather see the Internet governed solely by states at the United Nations (UN). While the UN sponsors the IGF, the Forum has no decision making power.

CONSIDERATIONS

The IGF will be the last major Internet governance meeting before the World Conference on International Telecommunications (WCIT) that will take place on December 3-14, 2012 in Dubai, United Arab Emirates which Mr. Grigsby will be attending (**TAB A**). Many WCIT participants are expected to attend the IGF, providing an excellent opportunity for Mr. Grigsby to network prior to his attendance to the WCIT, and assist the Canadian delegation to the IGF raise countries' awareness of the negative consequences that Chinese and Russian proposals would entail.

Industry Canada will represent the Government of Canada at the IGF. Mr. Grigsby would support the Canadian Delegation as the subject matter expert on cyber security issues.

[redacted] They have specifically raised the importance of having a cyber security subject matter expert supporting Canadian delegations to the IGF. Additionally, the United States, as part of the Beyond the Border Vision, has requested that Canada take a more active role in engaging internationally to promote common cyber security interests. Having a Canadian cyber security expert at the IGF is a step towards that objective.

This trip falls within the 2012-2013 travel cap for the National Security Branch, and will cost approximately $5,927.18.

RECOMMENDATION

It is recommended that you approve this travel request. Should you agree, your signature is sought on the Travel Authority and Advance form (**TAB B**) as well as the Conference Authorization form (**TAB C**). The International Travel Request form is also attached for your information (**TAB D**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Robert Dick, Director General, National Cyber Security at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security Branch

Enclosures: (2)

s.13(1)(a)

I approve:

s.15(1) - Int'l

_____
Graham Flack

Day 0	5 November 2012			
Time	09:00 - 10:30	11:00 - 12:30	12:30 - 14:30	
Main Session Room				
Conference Room #1				
Conference Room #2	[redacted]			
Conference Room #3				
Conference Room #4				
Conference Room #5	[redacted]			
Conference Room #6				
Conference Room #7				
Conference Room #8				
Conference Room #9				
Conference Room #10				
Conference Room #11				

Day 1 6 November 2012

Time	09:30- 11:00	11:00 - 12:30	12:30 - 15.00	15.00
Main Session Room	*Opening Ceremony	*Opening Session	Lunch Break	New Delegates
Time	09:00 - 10:30	11:00 - 12:30	12:30 - 14:30	14:30
Conference Room #1			Lunch Break	WS 1
Conference Room # 2			Lunch Break	WS 126 EURid Report on IDN D opportunities associated with multilin
Conference Room # 3			Lunch Break	WS 12
Conference Room # 4			Lunch Break	WS 10
Conference Room #5			Lunch Break	WS 16 Op cybersecurityha mat
Conference Room #6			Lunch Break	WS 2
Conference Room #7			Lunch Break	WS 130 Digital I Access to the Policymakers Libraries and O Services
Conference Room #8			Lunch Break	WS 128 Empow whic
Conference Room #9			Lunch Break	
Conference Room #10			Lunch Break	WS 5
Conference Room #11			Lunch Break	

			Taking Stock and the Way Forward and Others (TSWF)	Dynamic
* Translation Available	Access and Diversity (AD)		Security Openness and Privacy (SOP)	Ope

Day 2 7 November 2012

Time	09.30-12.30		12:30 - 15.00	
Main Session Room	[redacted]		Lunch Break	[redacted]
Time	**09:00 - 10:30**	**11:00 - 12:30**	**12:30 - 14:30**	**14:**
Conference Room #1	[redacted]	[redacted]	Lunch Break	[redacted]
Conference Room #2	WS 40 Mobile is changing the world- challenges and opportunities are paralleled for the enterprises	[redacted]	Lunch Break	WS 157 Is acc hum
Conference Room #3	[redacted]	Open Forum EBU: Safety of online media actors (SUBTITLE: as a precondition for media pluralism and freedom of expression)	Lunch Break	WS 82 Measu promoting environment (c
Conference Room #4	WS 50 Internet privacy and freedom of expression (UNESCO launches a global survey on legal frameworks	WS 143: Measuring the economic and social impact of the Internet to inform policy making	[redacted]	WS 60 As
Conference Room #5	[redacted]	WS 85 Quo Vadis IGF – Evolution of IGF	Lunch Break	WS 105 Inte improved ac m
Conference Room #6	[redacted]	WS 57 Broadband access and consumer rights	Lunch Break	WS 86 Solution borde
Conference Room #7	WS 129 The sustainable benefits of inclusion on the Internet	[redacted]	Lunch Break	WS 88 Onlin toolkits preve offenses por
Conference Room #8	WS 97 Concepts of acceptable behavior to protect and enhance trust	WS 72 Jurisdictional issues on civil and law enforcement access to cloud data	Lunch Break	Open Foru operations (ho
Conference Room #9	WS 125 Innovative application of ICTs to facilitate child protection online	[redacted]	Lunch Break	WS 136 Free Inte
Conference Room #10	WS 191 The influence of politics over Internet users' access and diversity	WS 168 Capacity building Initiatives for better economic and social inclusion of vulnerable people into the Information society	Lunch Break	One stop sho dynamic co capacity bu
Conference Room #11	How to submit a workshop proposal	The UN Convention on the Rights of the Child's 20th anniversary: digital agenda	Lunch Break	

[redacted]	[redacted]	Taking Stock and the Way Forward after 7 IGFs (WS)	Dynam
Access and Diversity (AD)	[redacted]	Security, Openness and Privacy (SOP)	O

* Translation Available

Day 3 8 November 2012

Time	09.30 - 12.30		12.30-15.00	
Main Session Room	Main session: Access and Diversity		Lunch Break	Ma
Time	**09:00 - 10:30**	**11:00 - 12:30**	**12:30 - 14:30**	**14:30**
Conference Room #1	WS 181 Who is following me: tracking the trackers	WS 176 Law enforcement via domain names: caveats to DNS neutrality	Lunch Break	WS Dealing across different
Conference Room #2	WS	WS 180 Blocking and filtering Internet DNS content	Lunch Break	WS 96 Accurat the Journe
Conference Room #3	WS 185 Criminal law and the free and open Internet: tensions and ways forward in democratic societies		Lunch Break	WS 98 A plan to cre
Conference Room #4			Lunch Break	WS 176 Nationa looking at some
Conference Room #5	WS 178 Cybersecurity that achieves privacy and civil liberties	WS 96 The Internet of humans: online human behaviour and its policy impacts	Lunch Break	WS Ways freedom of ex Intern
Conference Room #6	WS Threats to multi-stakeholder Internet governance: is it worth protecting?	WS Freedom of expression online: key challenges and best practices	Lunch Break	WS 88 Internet shared values
Conference Room #7	WS Freedom of expression and freedom from hate on line: (Young people combating hate speech on line)	WS 188 Growing up and living in a society with censorship: challenges and lessons	Lunch Break	Dynamic Coa Access in Libr
Conference Room #8	Google: Broadband measurement and metrics for a sustainable Internet		Lunch Break	Open Foru Digital pres multilin
Conference Room #9	Open Forum Council of Europe : Security, openness and privacy	WS 163 Governing identity online: Internet	Lunch Break	Open Governme GPI recipi
Conference Room #10	WS	Dynamic Coalition on Child Online Safety	Lunch Break	Dynamic Coalitio and D
Conference Room #11	ICANN Open Forum	Communication with and among objects – How can we envisage the governance of the Internet of Things (IoT)?	Dynamic Coalition Internet of Things	
			Ekaterina Stocker and the Way Forward and Others (ITSWF)	Dynamic
* Translation Available	Access and Diversity (AD)		Security Openness and Privacy (SOP)	Ope

GOVERNMENT OF CANADA / GOUVERNEME DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval oas orginal dated)
lodifications (approbation par des agents du même niveau ue

14A	Travel Authority No. (TAN) N°. d'aut de voyager (NAV)	Document No. RDIMS - N° du document SGGDI
		695466

Type 2 | Name of traveller - Nom du voyageur: Alex Grigsby | Classification

art A - Partie A

epartment - Ministère: ublic Safety Canada

Branch / Division / Group - Direction / Division / Groupe: NS-NCSD-Policy and Issues Management

ddress - Adresse: 1C-340 Laurier Avenue West

Telephone No. - No. de téléphone: 949-4243

If different address, send cheque to: Si adresse differente, envoyer chèque à

ranch Contact - Personne ressource à la direction: ane Hayward

Telephone No. - No. de téléphone: 613-991-182

urpose of travel - Objet du voyage: nternet Governance Forum

No. of days / Nbre de jours: 7

Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage ☑ Yes / Oui ☐ No / Non

If no, would you like to request one? Les cas échéant, aimerier-vous en avoir une? ☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival Départ - Arrivée	Transportation Transport Mode	Transportation Transport Class	No. of meals prepaid Nbre de repas prépayés	Accommodation Hébergement	File locator number N°. de repérage du dossier
4-Nov-12	Ottawa	Frankfurt, Germany	17:15-06:45	Air	Economy	2	NA	
5-Nov-12	Frankfurt, Germany	Baku, Azerbaijan	13:55-21:25	Air	Economy	1	Sheraton Airport Baku	
10-Nov-12	Baku, Azerbaijan	London, England	07:30-09:40	Air	Economy	1	215413582	
10-Nov-12	London, England	Ottawa	13:00-15:45	Air	Economy	1		

art C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales Item / Type de dépenses	Estimated cost / Coût estimatif
ccomodation (white page hotel) ébergement (un des hôtels figurant ans la partie blanche du répertoire)	$1,071.30	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
id-size car rental (collision damage aiver mandatory ocation d'une voiture intermédiaire ssurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
rivate vehicle requested by: oiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur ublic Liability and Property Damage min million. Deductibles NON reimbursable esponsabilité civile et dommages atériels (min. 1 000 000$). Les franchises O SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dessus)	$0.00
ansportation ansport	$220.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) 3.1.9 ☐ Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une	
eals and incidentals epas et frais accessoires	$800.84		
ther (Specify) - Autre (préciser) siness use of phone, baggage fees	$75.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Part D - Partie D

Estimated Cost - Coût estimatif

Prepaid - Prépayé

$3,760.04

Other - Autre

$2,167.14

Trip Total - Coût total du voyage

$5,927.18

Funding - Financement

A) Travellers cheques / Chèques de voyage

Cdn / Can	$1,700.00
US / É.U.	$0.00
Other / Autre	$0.00

B) Other advance / Autre avance

eque / Chèque	$0.00
ash / Comptant	$0.00

Total funding requested (A + B)

Financement total demandé (A + B)

$1,700.00

Ticket pick-up date and location
Date et lieu de la collecte des billets

art E Traveller / Partie E - Voyageur

ave access to the Treasury Board Travel Policy (internal policy for separate employers) and accept *e terms and conditions of travel that are in accordance with current policy.*
ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques terne pour les employeurs distincts) et en accepte les conditions.

ex Grigsby

Signature | Date

ecommended by (signature) - Recommandé par (signatu: nda Clairmont | Date

Approved by (signature) - Approuvé par (: Graham Flack | Date

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le
	A. Grigsby, Baku, Nov 4-10 2012	$1,700.00	November 1 2012

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicat / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0					

Tyoe 4

Accounting Information / Renseignement comptables

ub-type / us-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		T46	5001 00685 - 2001 - PAABA8E	

Description

Financial encumberance No. / No. de consignation de fonds

epartment pre-audit and account verification (signature) ent min. chargé de la vér. Préalable des comptes (signature)

Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Cheque No. - N° du chèque

rified correct (PWGSC) (signature) rifié conform (TPSGC) (signature)

rvices officer (PWGSC) (signature) ent responsible (TPSGC) (signature)

Date

	Signature	

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
irfare / Frais d'avion	$3,760.04
rain / Train	$0.00
ther / Autres	$0.00
	$3,760.04

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
ccomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du	$214.26	5	$1,071.30
ccomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du rép	$0.00	0	$0.00
			$1,071.30

id-size car rental / *Location d'une voiture intermédiaire*			$0.00
ON Mid-size car rental / Location d'une voiture **NON** intermédiaire			$0.00
asoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
ivate vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employ	0.555	0.0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
arking & Tolls / stationnement et frais de péage			$0.00	$0.00
	Home to Airport		$30.00	
	Airport - Hotel / Meetings		$30.00	
axi/Limo	Hotel - Airport		$30.00	$220.00
	Airport to Home		$30.00	
	Meeting - Meetings		$100.00	
ansportation / Transportation (No receipt)		**$10.00**		$0.00
rry & Miscellaneous			$0.00	$0.00
				$220.00

anada	Rate / Tarif	No. / Nbre	Amount/Montant
eakfast / Petits déjeuners	**$15.60**	0	$0.00
nch / Déjeuners	**$14.85**	0	$0.00
nner / Dîners	**$40.85**	0	$0.00
identals /Frais divers	**$17.30**	1	$17.30
		Total Canada	$17.30

ankfurt	*Rate / Tarif*	No. / Nbre	Amount/Montant
eakfast / Petits déjeuners	**$21.38**	0	$0.00
nch / Déjeuners	**$36.05**	1	$36.05
nner / Dîners	**$49.65**	0	$0.00
identals /Frais divers	**$34.27**	1	$34.27
		Total Frankfurt	$70.32

aku	Rate / Tarif	No. / Nbre	Amount/Montant
eakfast / *Petits déjeuners*	**$26.67**	4	$106.68
nch / Déjeuners	**$41.43**	4	$165.72
nner / Dîners	**$58.90**	4	$235.60
identals /Frais divers	**$40.65**	4	$162.60
		Total Baku	$670.60

ndon	Rate / Tarif	No. / Nbre	Amount/Montant
eakfast / Petits déjeuners	**$25.33**	0	$0.00
nch / *Déjeuners*	**$46.22**	0	$0.00
nner / Dîners	**$61.63**	0	$0.00
identals /Frais divers	**$42.62**	1	$42.62
		Total London	$42.62
		GRAND TOTAL	**$800.84**

siness Phone / Téléphone d'affaires	$25.00
ort Improvement Fee / Frais de l'Aeropart	$0.00
sh Advance Fee / *Frais d'avances*	$0.00
c. Business Services / Diverses charges d'affaires	$0.00
cellaneous / Diverses -	$50.00
	$75.00

Public Safety Canada / Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: 2/10/2012

) – A

raham Flack
/Deputy Minister

Requested by – Demandé par

Alexandre Grigsby
Analyst
National Cyber Security Directorate

ame of Conference – Titre de la conférence

ternet Governance Forum

pe of Conference – Genre de conférence

☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe: ☒ Yes / Oui ☐ No / Non

onsor - Promoteur

ne United Nations

Official Host – Hôte officiel

Govnerment of Azerbaijan

uration of Conference – Durée de la conférence

om: November 6, 2012 To / À: Novermber 9, 2012

Location - Adresse

Baku Expo Centre, Surakhani, Baku, Azerbaijan

genda – Ordre du jour

nclosed in package

s.15(1) - Int'l

rpose of Participation - Object de la participation

urpose:
- Obtain insights into countries' positions in advance of the World Conference on International Telecommunications; and
- Establish relationships with representatives from certain countries to advocate Canada's interests and to faciliate the promotion these interests at the WCIT.

ackground:
ne IGF will be the last major Internet governance meeting before the WCIT that will take place on December 3-14, 2012 in ubai. The WCIT will revise a treaty to which Canada is a party. Certain countries [redacted] are using this ocess to push their longstanding telecommunications interests by proposing language that could expand the UN system's role governing the Internet, and allow the International Telecommunications Union, a UN agency, to provide policy direction on atters of cyber security, criminal policy, and national defence. Many WCIT participants are expected to attend the IGF, oviding an excellent opportunity for Mr. Grigsby to network prior to his attendance to the WCIT, and assist the Canadian legation to the IGF raise countries' awareness of the negative consequences that Chinese and Russian proposals would entail.

ancial Coding – Code financier

101 00685 - 2001 - RABABE

Estimated Total Cost / Coût total prévu: $ 5927.18

commended by – Recommandé par

Signature: [signature] Date: Oct 3, 2012

Branch Approval – Approbation de la direction

Signature: _____ Date: _____

sistant Deputy Minister – Sous-ministre adjoint

Signature: _____ Date: _____

Deputy Minister – Sous-ministre

Signature: _____ Date: _____

000507

-18 (4/04)

Public Safety Canada / Sécurité publique Canada

s.15(1) - Int'l

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
	From - *Du* :	To - *Au* :
Internet Governance Forum	Nov 6, 2012	Nov 9, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Baku, Azerbaijan	$4,849.76	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
Agenda for the meeting is attached.	☒Yes/Oui ☐No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Alexandre Grigsby	National Cyber Security Directorate - NS Branch	340 Laurier Ave, 11th Floor	613-949-4243

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.) *Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)*

Role: Member of the Canadian Delegation (CANDEL) and principal subject matter expert on cyber security.

Purpose:

1 - Obtain insights into countries' positions in advance of the World Conference on International Telecommunications; and

2- Establish relationships with representatives from certain countries to advocate Canada's interests and to faciliate the promotion of these interests at the WCIT.

Background:

The IGF is a major annual conference where government representatives, academics, businesses, and civil society discuss current and emerging Internet issues. It embodies the multistakeholder model of internet governance that Canada seeks to sustain and promote internationally. This stands in contrast to the top-down model advocated by a number of countries, such as [redacted] that would rather see the Internet governed solely by states at the United Nations (UN). While the UN sponsors the IGF, the Forum has no decision-making power.

The IGF will be the last major Internet governance meeting before the World Conference on International Telecommunications (WCIT) that will take place on December 3-14, 2012 in Dubai, United Arab Emirates. As you know, the WCIT will revise a treaty to which Canada is a party. Certain countries, [redacted] by proposing language that could expand the UN system's role in governing the Internet, and allow the International Telecommunications Union, a UN agency, to provide policy direction on matters of [redacted] Many WCIT participants are expected to attend the IGF, providing an excellent opportunity for Mr. Grigsby to network prior to his attendance to the WCIT, and assist the Canadian delegation to the IGF raise countries' awareness of the negative consequences that [redacted] proposals would entail.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

As the Department works to implement the Canada's Cyber Security Strategy (RPP priority #4), participating in the IGF will inform preparations for the WCIT.

The WCIT is a conference organised by the International Telecommunication Union -- a Tier 2 priority under Public Safety's ISF -- and the IGF is explicitly mentionedas a Tier 3 priority. Finally, Canada's traditional allies (U.K., U.S., Australia) are heavily vested in this process and are working to advance

shared objectives (Tier 1 priority).

The United States, as part of the Beyond the Border Vision, has requested that Canada take a more active role in engaging internationally to promote common cyber security interests. Having a Canadian cyber security expert at the IGF is a step towards that objective.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

Alexandre will support the CANDEL to be led by Industry Canada.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

Industry Canada is supportive of Alexandre's attendance to the IGF.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of paticipant's Director General *Nom du Directeur Générale du voyageur*	Date: Oct 3/12

Reviewed by/
Examiné par :

Director General, International Affairs Directorate *Directeur Générale, Direction générale des affaires internationales*	Date

Approved by/
Approuvé par :

Name of participant's Assistant Deputy Minister *Nom du sous-ministre adjoint du voyageur*	Date

PS023

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: Oct 2/12

File No. 389976
RDIMS No.: 681377

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, CMB

INTERNATIONAL TRAVEL AUTHORIZATION FOR ROBERT DICK TO TRAVEL TO NEW ZEALAND AND AUSTRALIA OCTOBER 17-27, 2012

(Signature required)

ISSUE

Your approval is sought for the international travel request for Mr. Robert Dick to travel to Sydney and Canberra, Australia and Wellington, New Zealand, October 17-27, 2012. The purpose of the travel is to attend the 2012 Australian Defence Signals Department's (DSD) Cyber Security Conference and to hold bilateral meetings with counterparts responsible for policy and operational response in Sydney, Canberra and Wellington.

BACKGROUND

Mr. Mike Burgess, First Assistant Secretary Cyber and Information Security, DSD, invited Public Safety Canada (PS) and the Communications Security Establishment Canada (CSEC) to participate in the cyber conference at the Director General level. The theme for the conference is "Cyber Resilience - Are you ready?" The conference will feature speakers from DSD, key government agencies and industry including key industry partners in Canada and the United States as well as academia (**TAB A**). Mr. Dick will be in attendance with [redacted] CSEC.

s.15(1) - Subv

.../2

Canada

Attendance to this conference with CSEC is important to our engagement with industry as it reinforces the extent to which the Canadian Cyber Incident Response Centre (CCIRC) and PS are connected to the international community. Equally, it is an opportunity to convey Canada's commitment to cyber security and international engagement to our allies.

At the same time, the conference will provide an opportunity to gauge how Australia is engaging its private sector, and the extent of real alignment between its policy and operational arms.

This trip is also an opportunity to meet counterparts in both Australia and New Zealand. Meetings are being sought with Cabinet Affairs, the Attorney General and our cyber policy counterparts.

Final travel logistics will depend on the timing of the various meetings, and coordination of Mr. Dick's and travel schedules.

CONSIDERATIONS

Both the conference and bilateral meetings are opportunities to engage with these international partners, learn and discuss the issues that Australia is facing as well as the strategies that are being put forward to combat cyber threats. They will also allow Mr. Dick an opportunity to meet with our colleagues in each of these governments and develop his relationship with them.

All costs related to this request fall within my sector's allocated Travel, Hospitality, Conference cap for this fiscal year.

.../3

s.15(1) - Int'l
s.15(1) - Subv
s.21(1)(b)

RECOMMENDATION

It is recommended that you approve Mr. Robert Dick's travel request to New Zealand and Australia by signing the Travel Authority and Advance forms (**TAB B**) as well his attendance to DSD's Cyber Security Conference by signing the Conference Authorization form (**TAB C**). My approval of this trip is noted in the International Travel Request (**TAB D**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (4)

I approve:

OCT 0 3 2012

Graham Flack

Prepared by: Robert Dick

Public Safety Canada / Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: September 5 2012

To – A

Graham Flack
A/Deputy Minister
Public Safety Canada

Requested by – Demandé par

Robert Dick
Director General
NS-NCSD

Name of Conference – Titre de la conférence

Cyber Security Conference

Type of Conference – Genre de conférence

☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

Various

Official Host – Hôte officiel

Australian Department of Defence Intelligence and Security

Duration of Conference – Durée de la conférence

From / Du: October 23 2012 To / À: October 24 2012

Location - Adresse

Canberra, Australia

Agenda – Ordre du jour

Conference information is attached.

Purpose of Participation - Object de la participation

Mr. Dick will be a conference participant on behalf of Public Safety Canada. The conference is an important forum to reinforce to industry, through attendance and joint participation with Communication Security Establishment (CSEC), the extent to which the Canadian Cyber Incident Response Centre (CCIRC) and Public Safety are connected to the international community. Equally, it is an opportunity to convey Canada's commitment to cyber security and international engagement to our allies, and to meet counterparts with whom it is otherwise difficult to meet.

Financial Coding – Code financier

475 PSCYBINTLENG - 500098802 Line 1,2

Estimated Total Cost / Coût total prévu

$ 19521.69 (travel)

Recommended by – Recommandé par

Signature / Date

Branch Approval – Approbation de la direction

Signature / Date

Assistant Deputy Minister – Sous-ministre adjoint

L'Allaumont — Oct 2/12

Signature / Date

Deputy Minister – Sous-ministre

Signature / Date: OCT 0 3 2012

000513

MS-18 (4/04)

Defence Signals Directorate
Reveal Their Secrets - Protect Our Own

Welcome to the 2nd DSD Cyber Security Conference

Cyber resilience - Are you ready?

The Defence Signals Directorate (DSD) will host the 2nd DSD Cyber Security Conference, from 23-24 October 2012.

The conference will provide strategic and technical perspectives on information security and the cyber threat to Australia, featuring speakers from DSD, key government agencies, industry and academia. It will provide insight into contemporary challenges in information security confronting Australia.

The conference is aimed at senior executives and IT security practitioners from across federal, state and local government, as well as critical infrastructure agencies and industry partners.

Entry to the DSD Cyber Security Conference is by invitation only.

Invitees, confirm your attendance by registering now

Speakers will include:

- Alan Paller, Director of Research, SANS Institute
- Mike Burgess, First Assistant Secretary Cyber & Information Security, Defence Signals Directorate
- Matt Thomlinson, General Manager, Product Security, Microsoft Trustworthy Computing, Microsoft
- Joe Franzi, Assistant Secretary Cyber Security, Defence Signals Directorate
- Michael Sentonas, Vice President and CTO Asia-Pacific, McAfee
- Dmitri Alperovitch, Co-founder and CTO, CrowdStrike
- Professor Craig Valli, School of Computer and Security Science, Edith Cowan University
- Dr Steve Hodgkinson, Research Director IT Asia-Pacific, Ovum.

Exhibitors will include:

- Akamai Technologies
- Apple
- Aruba Networks
- BAE Systems Stratsec
- BAE Systems Detica
- Cisco Systems
- Datacom Technical Security Systems
- Endace
- FireEye
- Good Technology
- Hewlett Packard
- IBM
- Juniper Networks
- Logica Australia
- Lumension
- McAfee
- Microsoft
- NEXTDC
- Oakton
- Palo Alto Networks
- Radware Australia
- Research in Motion (RIM)
- RSA
- Saltbush Consulting
- Secure Systems
- Shearwater
- Sophos
- SourceFire
- Symantec
- Trend Micro
- Trustwave

Learn more:

- *about Canberra, including accommodation and transport*
- about the venue, including location, directions and parking

Please contact us if you have any questions.

GOVERNMENT OF CANADA / GOUVERNE DU CANAD

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

Document No. RDIMS - N° du document SGGDI

☑ Original / Prem. demande
☐ Amended (Same levels of approval oas orginal dated)
Modifications (approbation par des agents du même niveau que

14A	Travel Authority No. (TAN) N°. d'aut de voyager (NAV)

Type 2

Name of traveller - Nom du voyageur: Robert Dick

Classification: EX-03

Part A - Partie A

Department - Ministère: Public Safety Canada

Branch / Division / Group - Direction / Division / Groupe: NS-NCSD-DGO

Address - Adresse: 11C-340 Laurier Avenue West

Telephone No. - No. de téléphone: 613-990-2661

If different address, send cheque to:
Si adresse differente, envoyer chèque à

Branch Contact - Personne ressource à la direction: Jane Hayward

Telephone No. - No. de téléphone: 613-991-182

Purpose of travel - Objet du voyage: To attend E... DSD Cyber Security Conference and Meetings with Australia and New Zealand

No. of days / ...ore de jours: 11

Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (...
☑ Yes / Oui ☐ No / Non

If no, would you like to request one? / Les cas échéant, aimener-vous en avoir une?
☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival Départ - Arrivée	Transportation Transport Mode	Transportation Transport Class	No. of meals prepaid Nbre de repas prépayés	Accommodation Hébergement	File locator number N°. de repérage du dossier
October 17 2012	Ottawa	Sydney, Australia	18:55 - 09:15 (Oct 19)	Air	Business	2	TBC	
October 21 2012	Sydney, Australia	Canberra, Australia	18:15 - 19:05	Air	Economy	0	TBC	
October 25 2012	Canberra	Wellington NZ	06:40 - 14:45	Air	Business		TBC	
October 27 2012	Wellington NZ	Sydney, Australia	06:35 - 08:15	Air	Economy	1		
October 27 2012	Sydney, Australia	Ottawa	10:30 - 18:02	Air	Business	2		

Standard - Générales Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	2,040.50 ~~$2,040.50~~	Accomodation (green page hotel) Hébergement (un des hôtels figurant 'a partie verte du répertoire)	~~$0.00~~
Mid-size car rental (collision damage waiver mandatory Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory Location d'une voiture non intermédiaire (assurance-collision du	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) *Transport à tarif supérieur (préciser la <classe> si-dessus)*	$0.00
Transportation Transport	$750.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvee par le sou-chef ou l'equiv.) 3.1.9 ☐ Assistant Deputy Head or equivalent approval) *Classe d'affaires - ou autre classe à tarif supérieur* (approuveée par le sou-chef ou l'equiv,. S'il s'agit d'une	
Meals and incidentals *Repas et frais accessoires*	$1,412.17		
Other (Specify) - Autre (préciser) business use of phone, baggage fees, internet	$310.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Business Class has been requested for long haul flights

Part D - Partie D

Estimated Cost - Coût estimatif

Prepaid - Prépayé
$15,000.00

Other - Autre
$4,521.69

Trip Total - Coût total du voyage
$19,521.69

Funding - Financement

A) Travellers cheques / Chèques de voyage
Cdn / Can $0.00
US / É.U. $0.00
Other / Autre $0.00

B) Other advance / Autre avance
...eque / Chèque $0.00
...sh / Comptant $0.00

Total funding requested (A + B)
Financement total demandé (A + B)
$0.00

Ticket pick-up date and location
Date et lieu de la collecte des billets

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Robert Dick — Signature — Sept 6/12 — Date

Recommended by (signature) - Recommandé par (signatu... — Lynda Claimont — Date: Oct 2/12

Approved by (signature) - Approuvé par (... — Graham Flack — Date: OCT 03 2012

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount Montant du chèque	Date cheque required Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicat Indicateur du fournisseur	Due Date Date d'échéance
	8 | 0					

Accounting Information / Renseignement comptables

Tyoe 4

Sub-type Sous-type	Vendor Code Code du fourn.	Departmental Ref. No. No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		THC-T9	2001-PSCYBINTLENG - 500098802	

	Description	Financial encumberance No. No. de consignation de fonds

Department pre-audit and account verification (signature)
Agent min. chargé de la vér. Préalable des comptes (signatur

Verified correct (PWGSC) (signature)
Vérifié conform (TPSGC) (signature)

Services officer (PWGSC) (signature)
Agent responsible (TPSGC) (signature)

Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment *Requisition Regulations*
Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Signature

Cheque No. - N° du chèque

Date

000515

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé

	Amount/Montant
Airfare / Frais d'avion	$15,000.00
Train / Train	$0.00
Other / Autres	$0.00
	$15,000.00

Estimated Cost - Coût estimatif: Other - Autre

		Rate / Tarif	No. / Nbre	Amount/Montant
Sydney	Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	~~$266.48~~	~~2~~	~~$532.96~~
Country #2	Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	~~$284.65~~	~~4~~	~~$1,138.60~~
Country #3	Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$188.98	2	$377.96
TOTAL Accomodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du				~~$2,049.52~~
Country #1	Accomodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du répertoire)			~~$0.00~~
Country #2	Accomodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du répertoire)			~~0.00~~
Country #3	Accomodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du répertoire)			$0.00
TOTAL Accomodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du rép				~~0.00~~
				$0.00

Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire			$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour emp	0.555	0.0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$25.00	$750.00
	Airport - Hotel / Meetings		$200.00	
	Hotel - Airport		$200.00	
	Airport to Home		$25.00	
	Meeting - Meetings		$300.00	
Transportation / Transportation (No receipt)		**$10.00**		$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$750.00

Canada	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.60**	0	$0.00
Lunch / Déjeuners	**$14.85**	0	$0.00
Dinner / Dîners	**$40.85**	0	$0.00
Incidentals /Frais divers	**$17.30**	1	$17.30
		Total Canada	$17.30

Sydney	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$28.92**	3	$86.76
Lunch / Déjeuners	**$53.49**	3	$160.47
Dinner / Dîners	**$66.37**	3	$199.11
Incidentals /Frais divers	**$47.66**	4	$190.64
		Total Sydney	$636.98

Canberra	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$24.33**	3	$72.99
Lunch / Déjeuners	**$43.10**	3	$129.30
Dinner / Dîners	**$60.41**	3	$181.23
Incidentals /Frais divers	**$40.79**	3	$122.37
		Total Canberra	$505.89

New Zealand	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$20.08**	1	$20.08
Lunch / Déjeuners	**$43.78**	1	$43.78
Dinner / Dîners	**$55.79**	2	$111.58
Incidentals /Frais divers	**$38.28**	2	$76.56
		Total New Zealan	$252.00
		GRAND TOTAL	**$775.19**

Business Phone / Téléphone d'affaires	$200.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$10.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses	$100
	$310.00

Public Safety Canada / Sécurité publique Canada

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions** Travel - R Dick Australia October 17-27 2012					
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?					
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?					
	☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☒ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☒ Other Specify: ITR
☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?					
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?					
	Have I completed all the paperwork requested by the Contracting Material Management group? ☐ Is the Sole Source Checklist complete and attached? ☐ Is the Competitive Contract Checklist complete and attached?					
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.					
	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☐ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☐ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*					

	Purchase Requisition #	Purchase Order #	Funds Commitment #:	RDIMS #
			500097431 Line 1,2	682242

INSTRUCTIONS FOR COMPLETION OF SECTION 32 CHECKLIST

These instructions are meant to assist staff in the preparation of the Section 32 checklist for Grants and Contributions payments. The numbers used relate to the same number on the checklist.

Legend: ☒ = **completed or has been considered**

1) Use the Delegated Financial Signing Authorities matrix located at: http://icarchive/foryou/divisions/comptroller/dfsa/_fl/dfsa-matrix-dept-eng.pdf to ensure that the person exercising Expenditure Initiation authority has the authority delegated to his/her position.

2) Forms can be found in Microsoft Office/Excel templates when starting a new document.

3) Ensure that you have the authority to sign under Section 32: a) by using the Delegated Financial Signing Authorities matrix located at: http://icarchive/foryou/divisions/comptroller/dfsa/_fl/dfsa-matrix-dept-eng.pdf; and b) by the completion of a Financial Authority Specimen Signature Record.

4) Run a free balance report in SAP to ensure that you have sufficient unencumbered funds to legally sign Section 32.

5) These forms are applicable to the Contracting and Procurement Unit and may not be applicable to expenditures such as Hospitality and Travel.

6) Enter the commitment into the SAP system and verify that the correct g/l, cost center, amount, vendor and description are entered. When the commitment is entered and saved please provide the Fund Commitment/ Purchase Order number on the indicated line.

7) When entering into a contract for the purchase of a good, please consider if the following will be a capital asset as per the criteria stated. Please contact External Reporting Group within the Financial Services & Systems Division (FSSD) for further instruction on ensuring the proper coding/description.

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
Australian Defence Signals Department's (DSD) Cyber Security Conference and Meetings with Australia and New Zealand Cyber Officials	From - *Du* : October 17, 2012	To - *Au* : October 27, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Canberra and Sydney Australia, Wellington New Zealand.	$19,521.69	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
Details on the DSD Cyber Security Conference and proposed meeting agendas are also attached.	☒Yes/Oui	☐No/Non

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Robert Dick	National Cyber Security Directorate - NS Branch	340 Laurier Ave, 11th Floor	613-990-2661

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Public Safety Canada (PS) and the Communications Security Establishment Canada (CSEC) were invited by Australia to participate in the cyber conference at the Director General(DG) level. Mr. Dick will be the representative participant on behalf of PS as DG of National Cyber Security (NCSD).

Meetings are scheduled with counterparts from DSD, those responsible for the computer emergency readiness teams, the Cabinet Office and similar officials with the New Zealand government.

Mr. Dick will present information on cyber policy, Canada's Cyber Incident Response Centre and public/ private engagement.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

The conference is an important forum to reinforce to industry, through attendance and joint participation with CSEC, the extent to which CCIRC and Public Safety are connected to the international community. Equally, it is an opportunity to convey Canada's commitment to cyber security and international engagement to our allies, and to meet counterparts with whom it is otherwise difficult to meet.

Attendance will also allow Mr. Dick to establish and strengthen his relationships in these countries,

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

will attend the conference in Canberra as well as the scheduled meetings.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

Mr. Dick has consulted with SADM Clairmont and CSEC. All cyber related initiatives and outcomes are shared at DG, ADM and DM level meetings on cyber.

s.15(1) - Int'l
s.15(1) - Subv

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of paticipant's Director General
Nom du Directeur Générale du voyageur

Date: Sept 6/12

Reviewed by/
Examiné par :

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

Date: SEP - 7 2012

Approved by/
Approuvé par :

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date: Oct 2/12

PS023

Travel - R Dick
Australia/ New Zealand
Docket #389976
RDIMS #6855
September 5 2012

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: SEP - 5 2012

File No.: 389879
RDIMS No.: 676396

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, Corporate Management Branch

REQUEST FOR BOB GORDON TO TRAVEL TO LONDON, UNITED KINGDOM

(Decision sought)

ISSUE

Your approval is sought for Mr. Bob Gordon, Special Advisor, Cyber Security, to travel to London, United Kingdom (U.K.), from October 14 to 17, 2012, to participate as a speaker at the second Strengthening Global Cyber Security Round Table organized by the Cityforum.

BACKGROUND

Mr. Gordon has been invited by Marc Lee, Chairman, Cityforum Limited, to speak and then participate in a moderated discussion as part of the Societal Vulnerabilities section at second Strengthening Global Cyber Security Round Table on October 16, 2012 (TAB A). The morning session will begin with a "master class" held by Chris Inglis, Deputy Director, National Security Agency, United States (U.S.), under the chairmanship of the Rt Hon Baroness Pauline Neville-Jones, former U.K. Minister of Security, who will guide the discussion. Pauline will open the second session with her paper on whether we have yet developed a sufficient systematic grasp of our systemic vulnerabilities and how can we provide integrated cyber resilience. Her presentation will be followed by a round table discussion during which Mr. Gordon will provide a Canadian view on this subject. Also participating in the round table will be Chris Inglis, Dr. Michael Frater, Rector, Australian Defence Academy, Simon Dukes, Centre for the Protection of National Infrastructure, U.K. and a not yet identified private sector panelist.

Canada

.../2

The afternoon session with focus on "Managing the global risks in cyber space" with presentations by Isabel Hilton on China and Joyce Corell, Office of the Director of National Intelligence, U.S., on protecting key components of the economic system. The programme is attached (TAB B).

Mr. Gordon has also been invited to dinner for speakers and key guests the evening of October 15, 2012.

Attendance will be just over 100 and proceedings will be confidential. In addition to the organizations noted above, senior level participants will include the Government Communications Headquarters (GCHQ) and James Quinault, Director, Cabinet Office of Cyber Security and Information Assurance (OCSIA).

Mr. Gordon has previously spoken at a round table organized by Cityforum. On November 4, 2010, Mr. Gordon spoke at the Third 2010 Cityforum Round Table on Cyber Security after the Strategic Defence Security Review. That conference was attended by approximately 100 government, industry, academia and international representatives. It proved to be a very useful forum to articulate Canada's approach in dealing with cyber security issues and comments received by staff at the Canadian High Commission London who attended the session indicated that Mr. Gordon's comments were well received.

While in London, Mr. Gordon will take the opportunity to meet with staff at the Canadian High Commission to bring them up to date on activities relating to the delivery of Canada's Cyber Security Strategy.

Mr. Gordon's participation in the round table will provide a good occasion to deliver the message of Canada's commitment to cyber security to an influential audience of U.K. and U.S. officials.

CONSIDERATIONS

The estimated cost for this trip to London is $10,096.67. All costs related to this request fall within my sector's allocated Travel/Hospitality/Conference cap for this fiscal year.

s.13(1)(a)

.../3

RECOMMENDATION

It is recommended that you approve Mr. Gordon's travel to attend the Cityforum meeting in London, U.K. from October 14 to 17, 2012. Should you agree, your signature is sought on the attached Travel Authority and Advance and Request to Attend a Conference forms (TAB C). The International Travel request is enclosed for your information.

Should you require additional information, please do not hesitate to contact me at 613-990-4976, or Mr. Bob Gordon, Special Advisor, Cyber Security, at 613-949-7380.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure(s): (4)

I approve:

SEP 14 2012

Graham Flack

Prepared by: Robert Gordon

Hayward, Jane

From: Marc Lee <mlee@cityforum.co.uk>
Sent: July-20-12 7:23 AM
To: Gordon, Robert
Cc: mlee@cityforum.co.uk
Subject: Speaker Invitation - Strengthening Global Cyber Security
Attachments: Strengthening global cyber security - 28.9.11.pdf; Strengthening global cyber security - delivering on the priorities initial draft ideas 18.07.12.doc

Dear Bob

Our third Strengthening Global Cyber Security Round Table, keynoted as before by Mr Chris Inglis, Deputy Director of the NSA, is to take place in Central London on October 16, with a dinner for speakers and key guests the evening before.

This year's Round Table focuses on delivering the priorities and I would like to extend a formal invitation to you to speak and then participate in the moderated discussion that follows.

I would particularly welcome a short speech by you as part of the Societal Vulnerabilities section of the day.

The morning begins with a master class held by Chris Inglis under the chairmanship of Baroness Pauline Neville-Jones, who will guide the discussion to which we should be delighted if you would contribute.

Pauline will open the second session with her view of whether we have yet developed a sufficient systematic grasp of our systemic vulnerabilities. I would then, if you are free to join us, welcome a Canadian view of this subject. Your presence at the earlier Round Table was most welcome and Mike Theilmann advises me that your role is as lively in Ottawa as ever.

I would be delighted if you could join us and I look forward to discussing this forum with you if you are able to come. Attendance will be just over 100 senior figures from the UK, the US and elsewhere and proceedings will be confidential. I hope the forum will be as useful as the earlier ones in the serious appear to have been.

I await your response. The initial draft programme for this year is attached together with the report from the 2011 forum.

Regards
Marc

Marc Lee
Chairman
Cityforum Limited
Telephone + 44 (0) 1373 831 900
Fax + 44 (0) 1373 831 017
Email mlee@cityforum.co.uk
Website www.cityforum.co.uk

cityforum
cutting through

Second annual Cityforum information and intelligence systems Round Table

Strengthening global cyber security – delivering on the priorities

16 October 2012
Central London

Initial ideas for discussion

Proposed themes:

Morning

1. Keynote opening – overview of the priorities and requirements

Mr Chris Inglis *Deputy Director* NSA

Followed by a Round Table moderated by Baroness Pauline Neville-Jones

2. Societal vulnerabilities and cyber resilience – do we have a sufficient systematic grasp of our systemic vulnerabilities and how can we provide integrated cyber resilience? We have clearly taken strides in individual areas but are we thinking enough across the whole and what are the policy consequences?

– a paper prepared by Baroness Pauline Neville-Jones followed by a Round Table discussion featuring Mr Chris Inglis and others; including an industry viewpoint and a DHS assessment.

A Canadian official Mr Bob Gordon *Special Adviser*, Cyber Security Public Safety Canada to be invited, GCHQ and UK CPNI to be offered a role on the panel.

Afternoon

3. How should we treat China – as a competitor, collaborator, friend or foe? How strong is our interest in seeking a 'modus vivendi' with Beijing and can we succeed?

This to be introduced by a paper prepared by Professor Paul Cornish who wrote 'Chinese Cyber Espionage: Confrontation or Co-Operation?' for Cityforum.

Ms Joyce Corell *Associate Director, Acquisition Risk Directorate* Office of the Director of National Intelligence to be invited to deliver a speech on an aspect of relationships with China (this to be determined). An industry panellist to be invited.

Dr Vinh Nguyan of DoD to be invited to contribute and a British MoD official to comment.

China is in a period of significant political change and an appraisal by Ms Isabel Hilton *Editor* Chinadialogue and BBC broadcaster might be worth including. She is a serious China watcher and could be an excellent lunch guest speaker bridging the morning and afternoon sessions.

4. The issue of law and order and a discussion of what should be looked at and with a view to achieving what actual results?

The Estonian Lawyer who was at NATO Ms Eneken Tikk Ringas to be asked to prepare a paper and a British Lawyer or US expert from Garmisch to comment.

Mr Misha Glenny Broadcaster and Visiting Professor at Columbia University to be invited to contribute, developing his argument on the implications of Stuxnet, Flame etc.

A commercial perspective to be included also.

Pre-Forum Dinner

For the dinner the night before on 15 October, Cityforum proposes a discussion on the potential for malicious forces to cause trouble / panic / uncertainty by attacking the information held by states / corporates / exchanges etc. Trust and confidence in the integrity of information could become a serious risk and how we can best confront it would be the theme of the evening discussion with key figures from the following day.

ML 18.07.12

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval as orginal dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N° d'aut de voyager (NAV)	Document No. - N° du document
	LNW926813	

Part A - Partie A

Type 2	Name of traveller - Nom du voyageur	Classification
	Robert Gordon	EX-05

Department - Ministère: Public Safety Canada
Branch / Division / Group - Direction / Division / Groupe: National Security
Address - Adresse: 340 Laurier Ave. West
Telephone No. - No. de téléphone: 613-949-7380
If different address, send cheque to. / Si adresse différente, envoyer chèque à:
Branch Contact - Personne ressource à la direction: Jane Hayward
Telephone No. - No. de téléphone: 613-991-1982
Purpose of travel - Objet du voyage: To attend Cityforum conference
No. of days / Nbre de jours: 4
Do you have a Govt Trd Travel Card (ITC)? Avez-vous une carte de voyage (CVP)? ☑ Yes / Oui ☐ No / Non
If no, would you like to request one? / S'il y a lieu, aimeriez-vous en avoir une? ☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Départ	Time - Heure: Arrival - Arrivée	Transportation Transport Mode	Flight Class	No. of meals prepaid Nbre de repas prépayés	Accommodation Hébergement	File locator number N°. de
13/10/2012	Ottawa	London	23:25	11:10 next day	Air	Business	2	~~Marriott~~	
17/10/2012	London	Ottawa	15:15	17:50	Air	Business	2	Radisson	

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$960.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du repertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by. Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable. Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dussus)	$0.00
Transportation Transport	$420.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) Business class / Other-Upgraded (other than article 3.1.9	
Meals and incidentals Repas et frais accessoires	577.59 ~~$602.13~~	☑ Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Other (Specify) - Autre (préciser) Business phone, baggage, internet, cash advance	$170.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel:
The business class is required due to length of flights. Hotel cost is always higher in London.

Part D - Partie D

Estimated Cost - Coût estimatif
Prepaid - Prépayé
$7,969.08
Other - Autre
$2,152.13
Trip Total - Coût total du voyage
~~$10,121.21~~ 10,096.67

Funding - Financement

A) Travellers cheques / Chèques de voyage
Cdn / Can $0.00
US / É.U. $0.00
Other / Autre $0.00
B) Other advance / Autre avance
Cheque / Chèque $0.00
Cash / Comptant $0.00

Total funding requested (A + B) / Financement total demandé (A + B): $0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Signature: [signature] Date: 20120829

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature): [signature] Date: SEP 05 2012
Approved by (signature) - Approuvé par (signature): [signature] Date: SEP 14 2012

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0					

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		THC NCSD T24	475- PSCYBINTLENG - 500099629	

Description:

Financial encumberance No. / No. de consignation de fonds:

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature):

Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Cheque No. - N° du chèque:

Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature):

Date:

Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature):

Signature:

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé			Amount/Montant
Airfare / Frais d'avion			$7,969.08
Train / Train			$0.00
Other / Autres			$0.00
			$7,969.08
Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$320.00	3	$960.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	$0.00	0	$0.00
			$960.00
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00
	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.555	0	$0.00
	Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage		$0.00	$0.00
Taxi/Limo — Home to Airport		$60.00	$420.00
Taxi/Limo — Airport - Hotel / Meetings		$100.00	
Taxi/Limo — Hotel - Airport		$100.00	
Taxi/Limo — Airport to Home		$60.00	
Taxi/Limo — Meeting - Meetings		$100.00	
Transportation / Transportation (No receipt)			$0.00
Ferry & Miscellaneous		$0.00	$0.00
			$420.00
Canada	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$24.87	0	$0.00
Lunch / Dejeuners	$45.38	0	$0.00
Dinner / Diners	$60.51	0	$0.00
Incidentals /Frais divers	~~$41.84~~ 17.30	1	~~$41.84~~ 17.30
	Canada	Meals	$41.84
London	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits dejeuners (receipts required) Estimated rate	$24.90	3	$74.70
Lunch / Dejeuners	$45.43	3	$136.29
Dinner / Diners	$60.58	3	$181.74
Incidentals /Frais divers	$41.89	4	$167.56
	London	Meals	$560.29
Country 3	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners (receipts required) Estimated rate	$0.00	0	$0.00
Lunch / Dejeuners	$0.00	0	$0.00
Dinner / Diners	$0.00	0	$0.00
Incidentals /Frais divers	$0.00	0	$0.00
	Country 3	Meals	$0.00
	TOTAL MEALS		~~$602.13~~ 577.59
Business Phone / Téléphone d'affaires			$50.00
Airport Improvement Fee / Frais de l'Aeropart			$0.00
Cash Advance Fee / Frais d'avances			$20.00
Misc. Business Services / Diverses charges d'affaires			$0.00
Miscellaneous / Diverses -			$100.00
			$170.00

Public Safety Canada | Sécurité publique Canada

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions** Travel R Gordon - London Oct 14-17 2012
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☒ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☐ Other Specify: ITR

☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?
	Have I completed all the paperwork requested by the Contracting Material Management group? ☒ Is the Sole Source Checklist complete and attached? ☐ Is the Competitive Contract Checklist complete and attached?
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☒ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☐ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

PS-SP-#681352-v1-FINANCE_Sec_32_R_Gordon_Cityforum__London_October_2012 DOC

Public Safety Canada / Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: August 28 2012

To – A

Graham Flack
A/Deputy Minister
Public Safety Canada

Requested by – Demandé par

Robert Gordon
Special Advisor
NS-NCSD

Name of Conference – Titre de la conférence

Strengthening Global Cyber Security Round Table

Type of Conference – Genre de conférence

☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

Finmeccanica, Northrop Grumman

Official Host – Hôte officiel

Cityforum

Duration of Conference – Durée de la conférence

From / Du: October 14 2012 To / À: October 17 2012

Location - Adresse

London, England

Agenda – Ordre du jour

Conference information is attached.

Purpose of Participation - Object de la participation

Mr. Gordon has been invited by Marc Lee, Chairman, Cityforum Limited, to speak and then participate in a moderated discussion as part of the Societal Vulnerabilities section at second Strengthening Global Cyber Security Round Table on October 16, 2012 (TAB A). The morning session will begin with a "master class" held by Chris Inglis, Deputy Director, National Security Agency, United States (U.S.), under the chairmanship of the Rt Hon Baroness Pauline Neville-Jones, former U.K. Minister of Security, who will guide the discussion. Pauline will open the second session with her paper on whether we have yet developed a sufficient systematic grasp of our systemic vulnerabilities and how can we provide integrated cyber resilience. Her presentation will be followed by a round table discussion during which Mr. Gordon will provide a Canadian view on this subject. Also participating in the round table will be Chris Inglis, Dr. Michael Frater, Rector, Australian Defence Academy, Simon Dukes, Centre for the Protection of National Infrastructure, U.K. and a not yet identified private sector panelist.
While in London, Mr. Gordon will take the opportunity to meet with staff at the Canadian High Commission to bring them up to date on activities relating to the delivery of Canada's Cyber Security Strategy

Financial Coding – Code financier

475 PSCYBINTLENG - 500099629 Line 1 and 2

Estimated Total Cost / Coût total prévu

$ ~~10,121.21~~ 10,096.6

Recommended by – Recommandé par

Signature _____ Date _____

Branch Approval – Approbation de la direction

Signature _____ Date _____

Assistant Deputy Minister – Sous-ministre adjoint

Signature _____ Date SEP 05 2012

Deputy Minister – Sous-ministre

Signature _____ Date SEP 14 2012

MS-18 (4/04)

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
Strengthening Global Cyber Security Round Table	From - *Du* : October 14, 2012	To - *Au* : October 17, 2012
Location (City, Country) - *Lieu (Ville, Pays)*: London, England	Estimated total cost - *Coût total prévu*: ~~$10,121.21~~ 10,096.67	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*: Program information is attached.	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?* ☒Yes/Oui ☐No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Robert Gordon	National Cyber Security Directorate - NS Branch	340 Laurier Ave, 11th Floor	613-949-7380

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Mr. Gordon has been invited by Marc Lee, Chairman, Cityforum Limited, to speak and then participate in a moderated discussion as part of the Societal Vulnerabilities section at second Strengthening Global Cyber Security Round Table on October 16, 2012 (TAB A). The morning session will begin with a "master class" held by Chris Inglis, Deputy Director, National Security Agency, United States (U.S.), under the chairmanship of the Rt Hon Baroness Pauline Neville-Jones, former U.K. Minister of Security, who will guide the discussion. Pauline will open the second session with her paper on whether we have yet developed a sufficient systematic grasp of our systemic vulnerabilities and how can we provide integrated cyber resilience. Her presentation will be followed by a round table discussion during which Mr. Gordon will provide a Canadian view on this subject. Also participating in the round table will be Chris Inglis, Dr. Michael Frater, Rector, Australian Defence Academy, Simon Dukes, Centre for the Protection of National Infrastructure, U.K. and a not yet identified private sector panelist.

While in London, Mr. Gordon will take the opportunity to meet with staff at the Canadian High Commission to bring them up to date on activities relating to the delivery of Canada's Cyber Security Strategy

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

Mr. Gordon's participation in the round table will provide a good occasion to deliver the message of Canada's commitment to cyber security to an influential audience of U.K. and U.S. officials.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

There will be no other Canadian representatives at the event. Other countries will be represented.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

There has been no other consultation.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

Name of paticipant's Director General
Nom du Directeur Générale du voyageur

Date 24/08/2012

Reviewed by/
Examiné par :

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

Date 30.8.12

Approved by/
Approuvé par :

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date SEP 0 5 2012

PS023

Request for Bob Gordon to Travel to
London, United Kingdom Oct 14-17, 2012
Docket # 389879 RDIMS # 676396
CONFIDENTIAL

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

 UNCLASSIFIED

DATE: SEP 0 5 2012

File No.: 389785
RDIMS No.: IS1860-673287

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
via: Gary Robertson, Assistant Deputy Minister, Corporate Management Branch

INTERNATIONAL TRAVEL AUTHORITY FOR ALEXANDRE GRIGSBY TO ATTEND THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS DUBAI, UNITED ARAB EMIRATES, DECEMBER 3-14, 2012

(Decision sought)

ISSUE

Alexandre Grigsby, Analyst, Policy and Issues Management, National Cyber Security Directorate, is requesting international travel authority to attend the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates, December 3-14, 2012.

BACKGROUND

The WCIT aims to revise the 1988 International Telecommunication Regulations (ITR), a treaty that governs the arrangements for exchanging international telecommunications traffic among countries. Canada has ratified the ITR and any revisions to the document are legally binding.

Given the binding nature of the WCIT outcome, countries are aggressively promoting their specific telecommunications related interests. [redacted]

Canada, supported by its like minded allies, is opposed to these efforts as they threaten the openness and accessibility that has allowed cyberspace, and the Internet in particular, to foster growth and innovation in the digital economy and connect societies. As such, Canada seeks [redacted] in the ITR.

Canada

.../2

s.15(1) - Int'l

CONSIDERATIONS

Industry Canada (IC), as the federal department responsible for interactions with the ITU, will lead the Canadian delegation. Mr. Grigsby is the most appropriate member of the National Cyber Security Directorate to participate in the delegation as a subject matter expert on cyber security. Mr. Grigsby has closely followed the over one hundred WCIT proposals, compared these to existing treaty language and international statements, and liaised with IC in crafting Canada's position going into negotiations. IC officials have specifically requested his presence in order to draw on his expertise on the ground as discussions proceed.

[redacted]

This trip falls within the 2012-2013 travel cap for the National Security Branch, and will cost approximately $6,830.00.

RECOMMENDATION

It is recommended that you approve this travel request. Should you agree, your signature is sought on the Travel Authority and Advance form (**TAB A**). The International Travel Request form is also attached for your information (**TAB B**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Robert Dick, Director General, National Cyber Security at 613- 990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security Branch

Enclosures: (2)

I approve:

SEP 1 0 2012

Graham Flack

s.15(1) - Int'l

GOVERNMENT OF CANADA / GOUVERNE DU CANAD

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval oas orginal dated)
Modifications (approbation par des agents du même niveau que

14A

Travel Authority No. (TAN) / N°. d'aut de voyager (NAV): LNW9

Document No. RDIMS - N° du document SGGDI

Type 2

Name of traveller - Nom du voyageur: Alex Grigsby

Classification: EC-03

Part A - Partie A

Department - Ministère: Public Safety Canada

Branch / Division / Group - Direction / Division / Groupe: NS-NCSD-Policy

Address - Adresse: 11C-340 Laurier Avenue West

Telephone No. - No. de téléphone: 949-4243

If different address, send cheque to: / Si adresse differente, envoyer chèque à

Branch Contact - Personne ressource à la direction: Jane Hayward

Telephone No. - No. de téléphone: 613-991-182

Purpose of travel - Objet du voyage: To attend the World Conference on Telecommunications

No. of days / Nbre de jours: 15

Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (: ☐ Yes / Oui ☑ No / Non

If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une? ☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport: Mode	Transportation Transport: Class	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
30-Nov-12	Ottawa	Dubai, United Arab Emriates	17:15-00:05 + 2 day (2-Dec)	Air	Economy	1	Novotel World Trade Center	
15-Dec-12	Dubai, United Arab Emriates	Ottawa	01:55 - 16:15	Air	Economy	2		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$2,306.78	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory Location d'une voiture intermédiaire (assurance-collision du répertoire	$0.00	Non mid-size car rental (collision damage waiver mandatory Location d'une voiture non intermédiaire (assurance-collision	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dessus)	$0.00
Transportation Transport	$280.00	☐ Prem. Classe (approuvée par le sou-chef ou l'équiv.) ☐ 9 Business class / Other-Upgraded (other than article Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit	
Meals and incidentals Repas et frais accessoires	$1,544.42		
Other (Specify) - Autre (préciser) baggage fees	$100.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Part D - Partie D

Estimated Cost - Coût estimatif

Prepaid - Prépayé

$2,598.80

Other - Autre

$4,231.20

Trip Total - Coût total du voyage

$6,830.00

Funding - Financement

A) Travellers cheques / Chèques de voyage

Cdn / Can $3,500.00

US / É.U. $0.00

Other / Autre *$0.00*

B) Other advance / Autre avance

eque / Chèque $0.00

ash / Comptant *$0.00*

Total funding requested (A + B)

Financement total demandé (A + B)

$3,500.00

Ticket pick-up date and location

Date et lieu de la collecte des billets

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Alexandre Grigsby — Signature: AGrigsby — Date: Aug 23, 2012

Recommended by (signature) - Recommandé par (signatur: Lynda Clairoux — Date: SEP 0 5 2012

Approved by (signature) - Approuvé par (: Graham Flack — Date: SEP 1 0 2012

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le
	A Grigsby, Dubai, UAE Dec 2012		

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indica / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0					

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		THC T-19	496 2001-PSCYBINTLENG - 500099484 Line 1-2	

Description

Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signatu

Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.

Cheque No. - N° du chèque

Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)

Date

Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)

Signature

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$2,598.80
Train / Train	$0.00
Other / Autres	$0.00
	$2,598.80

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE**	$164.77	14	$2,306.78
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du r			$0.00
			$2,306.78
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire			$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour emp	0.555	0.0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de peage			$0.00	$0.00
Taxi/Limo	Home to Airport		$40.00	$280.00
	Airport - Hotel / Meetings		$50.00	
	Hotel - Airport		$50.00	
	Airport to Home		$40.00	
	Meeting - Meetings		$100.00	
Transportation / Transportation (No receipt)		**$10.00**		$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$280.00

Canadian	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.60**	0	$0.00
Lunch / Déjeuners	**$14.85**	0	$0.00
Dinner / Dîners	**$40.85**	0	$0.00
Incidentals /Frais divers	**$17.30**	1	$17.30
	Total Canadian		$17.30

Frankfurt	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$20.93**	2	$41.86
Lunch / Déjeuners	**$35.29**	2	$70.58
Dinner / Dîners	**$48.60**	0	$0.00
Incidentals /Frais divers	**$33.55**	2	$67.10
	Total Frankfurt		$179.54

Dubai	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.41**	13	$200.33
Lunch / Déjeuners	**$26.90**	13	$349.70
Dinner / Dîners	**$36.22**	13	$470.86
Incidentals /Frais divers	**$25.13**	13	$326.69
	Total Dubai		$1,347.58
	GRAND TOTAL		**$1,544.42**

Business Phone / Téléphone d'affaires	$0.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses -	$100.00
	$100.00

Public Safety Canada / Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: August 24 2012

To – A

Graham Flack
Acting Deputy Minister
Public Safety Canada

Requested by – Demandé par

Alexandre Grigsby
Analyst
NS-NCSD

Name of Conference – Titre de la conférence

World Conference on International Telecommunications (WCIT)

Type of Conference – Genre de conférence

☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

United Nations

Official Host – Hôte officiel

International Telecommunications Union

Duration of Conference – Durée de la conférence

From / Du December 3, 2012 To / À December 14, 2012

Location - Adresse

Dubai, United Arab Emirates

Agenda – Ordre du jour

Included in package.

s.15(1) - Int'l

Purpose of Participation - Object de la participation

Role: Member of the Canadian Delegation (CANDEL) and principal subject matter expert on cyber security.

Purpose:

[redacted]

Financial Coding – Code financier

496- PSCYBINTLENG - 500099484

Estimated Total Cost / Coût total prévu

$ 6830.00

Recommended by – Recommandé par

Signature — Date

Branch Approval – Approbation de la direction

Signature — Date

Assistant Deputy Minister – Sous-ministre adjoint

Signature — Date: SEP 05 2012

Deputy Minister – Sous-ministre

Signature — Date: SEP 10 2012

NS-18 (4/04)

World Conference on International Telecommunications (WCIT-12)

At the request of our membership, ITU will convene the **World Conference on International Telecommunications (WCIT)** in Dubai, United Arab Emirates, from 3-14 December 2012.

This landmark conference will review the current International Telecommunications Regulations (ITRs), which serve as the binding global treaty outlining the principles which govern the way international voice, data and video traffic is handled, and which lay the foundation for ongoing innovation and market growth. The ITRs were last negotiated in Melbourne, Australia in 1988, and there is broad consensus that the text now needs to be updated to reflect the dramatically different information and communication technology (ICT) landscape of the 21st century.

Learn more >

Agendas | Participation | Documents

Agenda of WCIT-12
(Council Resolution 1317)

News Corner

Online registration *New!*

WCIT-12 Newsroom

Draft of the future ITRs
(document publicly accessible)

WCIT Background Briefs and FAQs

WCIT-12 in the News

Interview with Malcolm Johnson, Director of the ITU Telecommunication Standardization Bureau

Practical Information

WCIT-12 FAQs and Background Briefs

Dates and venue: 3-14 December 2012, Dubai, United Arab Emirates

Information for participants
(Document ADM/2)

WCIT-12 **Information Session at Council 2012**
(Council 2012 website)

Preparatory Process

Council Working Group to prepare for WCIT-12

Regional Preparatory Meetings

Proposals for the work of the conference
(Circular letter No. 64)

Briefing Sessions on Proposals submitted to WCIT-12 and WTSA-12
(Geneva, 8 9 October 2012)

Learn more >

Quick Links

World Telecommunication Standardization Assembly (WTSA-12)

ITU Plenipotentiary Conference

ITU Council

ITU Membership

ITRs

International Telecommunication Regulations
Melbourne, WATTC-88

Draft of the future ITRs
(document publicly accessible)

Host Country

United Arab Emirates will host WCIT-12

WCIT-12 Overview

The **World Conference on International Telecommunications (WCIT)** convened in Dubai, United Arab Emirates, from 3-14 December 2012, is the first ever WCIT in the history of the International Telecommunication Union.

The conference will consider a review (see PP-06 Resolution 146) of the International Telecommunication Regulations (ITRs), which define the general principles for the provision and operation of international telecommunications. **Signed by 178 countries, ITRs are a global treaty applied around the world**, which:

- Establish general principles relating to the provision and operation of international telecoms;
- Facilitate global interconnection and interoperability;
- Underpin harmonious development and efficient operation of technical facilities;
- Promote efficiency, usefulness, and availability of international telecommunication services, and
- Treaty-level provisions are required with respect to international telecommunication networks and services.

WCIT2012
Dubai, UAE

WCIT-12 presents a key opportunity to increase collaboration between countries, to help countries reach new levels of economic and social development through efficient telecom services, and to make the ITRs more relevant and valuable to ITU members, to help them respond to the challenges of a fast-evolving ICT environment.

Council 2010
Geneva, 13-22 April 2010

International Telecommunication Union

Document C10/84-E
29 April 2010
Original: English

RESOLUTION 1317

(adopted at the ninth Plenary Meeting)

Dates and Agenda of the World Conference on International Telecommunications in 2012

The Council,

Resolves,

pursuant to Resolution 146 (Antalya, 2006),

1 that the World Conference on International Telecommunications be held in 2012, in Geneva, Switzerland, in the period 5-30 November 2012, following the World Telecommunication Standardization Assembly;

2 that the duration of the conference would be from five to ten working days, depending on the degree of preparatory work;

3 that on the basis of proposals from Member States, taking into account the studies carried out during the preparatory process as presented in the final Report of the preparatory process conveyed by the Secretary-General to the Member States and submitted to the Conference (WCIT-12), to take appropriate action with respect to the following items, which constitute the agenda of the Conference:

3.1 Opening

3.2 Election of the Chairman and Vice-Chairmen

3.3 Other administrative issues including requests for participation received from international organizations, observers, etc.

3.4 Discussion and decisions regarding the structure of the Conference

3.5 Introduction of the Report of the preparatory process

3.6 Examination of the outputs of the preparatory process

3.7 Examination of proposals from Member States

3.8 Discussion of the proposed revisions to the ITRs, as appropriate

3.9 Discussion of WATTC-88 Resolutions, Recommendations, and Opinion

3.10 Adoption of the Final Acts of the Conference, including revised ITRs and Resolutions, Recommendations, and Opinions, as appropriate

3.11 Determine the date of coming into force of the Final Acts of the Conference and, if necessary, on the provisional application of certain part(s) of the Final Acts

3.12 Closure (including signing ceremony)

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
World Conference on International Telecommunications	From - *Du* : Dec 3, 2012	To - *Au* : Dec 14, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Dubai, United Arab Emirates	$6830.00	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
Revise the 1988 International Telecommunications Regulations (ITR), a treaty-binding text which provides high-level principles to govern international telecommunications. Agenda for the meeting is attached.	☒Yes/Oui ☐No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Alexandre Grigsby	National Cyber Security Directorate - NS Branch	340 Laurier Ave, 11th Floor	613-949-4243

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.) *Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)*

Role: Member of the Canadian Delegation (CANDEL) and principal subject matter expert on cyber security.

Purpose: **s.15(1) - Int'l**

[redacted]

Background:

The International Telecommunication Union (ITU), a United Nations (UN) specialised agency, will host the WCIT with the purpose of updating the 1988 International Telecommunication Regulations (ITR). The ITR is a treaty that governs the arrangements for exchanging international telecommunications traffic among countries. Canada has ratified the ITR and thus any revisions to the document are legally binding.

The upcoming WCIT is the first time since 1988 that the document has been open for review and countries are campaigning for the inclusion of amendments that would promote their specific telecommunications-related interests. Of specific relevance to cyber security, [redacted]

[redacted]

cyberspace.

Canada, supported by its like-minded allies, is opposed to these efforts as they threaten the openness and accessibility that has allowed cyberspace, and the Internet in particular, to foster growth and innovation in the digital economy and connect societies.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

As the Department works to implement the Canada's Cyber Security Strategy (RPP priority #4), participating at the WCIT will assist in mitigating any potentially negative provisions that countries are expected to insert in the ITR.

Further, the WCIT is a conference organised by the International Telecommunication Union (a Tier 2 priority under Public Safety's ISF). Finally, Canada's traditional allies (U.K., U.S., Australia) are heavily vested in this process and are working to advance shared objectives (Tier 1 priority).

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

Alexandre will support the CANDEL to be led by Industry Canada. Representatives from DFAIT and the private sector are expected to attend the WCIT.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

Industry Canada has specifically asked that Alexandre take part in the delegation given his work on the issue over the course of the past year. Relevant DFAIT officials are also aware of his attendance. As a treaty Conference, Canada's key allies (the U.S., U.K. and Australia) expect Canada to have cyber security subject matter expert on its delegation given the binding nature of the Conference's outcome.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
***Appuyé par*:** per P. Dick — 28/08/2012

Name of paticipant's Director General
Nom du Directeur Générale du voyageur

Date

Reviewed by/
***Examiné par*:** 30-8-12

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

Date

Approved by/
***Approuvé par*:** SEP 0 5 2012

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date

PS023

Public Safety Canada | Sécurité publique Canada
Senior Assistant Deputy Minister | Sous-ministre adjoint principal
Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: SEP 10 2012

File No.: 389529
RDIMS No.: 676336

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, Corporate Management Branch

REQUEST FOR BOB GORDON TO TRAVEL TO BUENOS AIRES, ARGENTINA

(Decision sought)

ISSUE

Your approval is sought for Mr. Bob Gordon, Special Advisor Cyber Security, to travel to Buenos Aires, Argentina, from October 6 to 10, 2012, to participate as a keynote speaker at the "First Awareness Conference for the Protection of Critical Infrastructures and Cybersecurity" (FACPCIC).

BACKGROUND

Mr. Gordon has been invited to participate as a keynote speaker at the FACPCIC conference that will be held on October 9, 2012, in Buenos Aires, Argentina, by Virginia Kannemann, Executive Assistant to the national Director, National Office of Information Technologies, Argentina (**TAB A**).

The conference will bring together national and international experts, including representatives from the public and private sectors, to discuss "joining forces in pursuit of generating awareness for critical infrastructure protection and Cybersecurity". Speakers have been invited from Germany, Mexico, Dominican Republic and Uruguay and the audience will be comprised of government officials and private sector chief information officers. The conference will be a public event and open to the news media. Mr. Gordon has been asked to outline the Canadian experience in cyber security and Canada's participation in the Meridian process. His presentation will be followed by a ten minute question and answer session. Opening of the conference will be undertaken by Juan Manuel Abal Medina, Chief of the Cabinet Office and Mariano Greco, Undersecretariat of Management Technologies.

Canada

.../2

[redacted] Mr. Gordon's presentation is consistent with Canada's Cyber Security Strategy that identified the essential requirement of international collaboration if cyberspace is to be secured and it will be an opportunity to highlight the Canadian approach to cyber security and the results of that effort.

Argentina will be hosting the Meridian 2013 conference. Mr. Gordon will use the occasion to indicate PS's willingness to participate as a member of the Program Committee (PC) for the conference. [redacted]

This is the second invitation from the Argentinian Government to speak on cyber security issues. Unfortunately, in March 2012, PS had to decline the invitation to speak at the Critical Information Infrastructure Protection Congress on extremely short notice and a member of the Canadian Embassy delivered the presentation on behalf of PS. [redacted]

CONSIDERATIONS

The Department of Foreign Affairs and International Trade, including the Canadian Embassy in Buenos Aires, has been consulted during the preparation of this submission and no issues were raised concerning accepting the invitation. At their request, Mr. Gordon's agenda will include a meeting with Embassy officials to brief them on the conference and generally on developments in advancing Canada's Cyber Security Strategy. This will be helpful for Embassy staff given that Argentina will be hosting the Meridian 2013 conference and PS employees will likely be invited to participate as members of the PC for that conference.

The Argentinian Government has offered to provide one airplane ticket to attend the conference however, as is the practice, the offer will be declined. You have previously approved the travel for Mr. Gordon and I to attend the Budapest Conference on Cyber Security in Budapest Hungary, from October 3 to 6, 2012. Approval is now being sought for Mr. Gordon to fly directly from Budapest to Buenos Aires rather than returning to Ottawa and thereby saving approximately $5,313.00 in airfare. The estimated additional cost for this trip to Buenos Aires, Argentina is $4,055.51. All costs related to this request fall within my Sector's allocated travel cap for this fiscal year.

RECOMMENDATION

It is recommended that you approve this travel request. Should you agree, your signature is sought on the attached Travel Authority and Advance form and Conference Authorization form (**TAB B**). The International Travel Request (**TAB C**) as well as the previous signed travel authorization (**TAB D**) are included for your information.

Should you require additional information, please do not hesitate to contact me at 613-990-4976, or Mr. Bob Gordon, Special Advisor, Cyber Security, at 613-949-7380.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure(s): (4)

I approve:

SEP 11 2012

Graham Flack

Prepared by: R. Gordon

Gordon, Robert

From: [redacted]
Sent: August-13-12 12:18 PM
To: Gordon, Robert
Subject: INVITATION TO PARTICIPATE AS SPEAKER AT THE FIRST AWARENESS CONFERENCE FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE

Importance: High

Dear Robert Gordon,

We are pleased to write to you regarding the " ***First Awareness Conference for the Protection of Critical Infrastructures and Cybersecurity***" conference that will be held on **October 9th, 2012** in Buenos Aires, Argentina.

The organizers of the conference would like to invite you to participate as a keynote speaker. We highly appreciate your participation in an event of such relevance.

There is great interest by Argentina and private sector organizations to work together, to join forces in pursuit of generating awareness for Critical Infrastructure Protection and Cybersecurity

It is worth mentioning that the opening of this event will be in charge of the Chief of the Cabinet Office, Juan Manuel Abal Medina and the Undersecretariat of Management Technologies, Mariano Greco.

The organization is providing one airplane ticket at economy fare from your country of residence to Buenos Aires, Argentina.

The conference will feature national and international experts and authorities of the public and private sectors.

We kindly ask you to confirm your attendance by replying this letter indicating whether you will be joining us as a speaker, and the estimated arrival date.

For more information regarding the conference, please feel free to contact us.

Thank you for your attention to this matter. I am looking forward to seeing you in the Congress.

Yours sincerely,

[redacted]
Oficina Nacional de Tecnologias de Información/National Office of Information Technologies
Av. Roque Sáenz Peña 511, 5 piso of 506
Tel. (54) 11 4331-4962
http://www.icic.gov.ar
http://www.biometria.gov.ar

s.19(1)

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☐ Original / Prem. demande

☑ Amended (Same levels of approval as orginal dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document
	LNW919804	

Type 2

Name of traveller - Nom du voyageur: Robert Gordon

Classification: EX-05

Part A - Partie A

Department - Ministère: Public Safety Canada

Branch / Division / Group - Direction / Division / Groupe: National Security

Address - Adresse: 269 Laurier Ave. West

Telephone No. - No de téléphone: 613-949-7380

If different address, send cheque to: / Si adresse differente, envoyer chèque à

Branch Contact - Personne ressource à la direction: Carmen Voghel

Telephone No. - No. de téléphone: 613-991-7025

Purpose of travel - Objet du voyage: To attend [redacted] (Ldn) Budapest Conf. on Cyberspace (Bud). First Awareness Conference for the Protection of Critical Infrastructure and Cyber Security

No. of days / Nbre de jours: 13

Do you have a Govt Trd Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)? ☐ Yes / Oui ☑ No / Non

If no, would you like to request one? / S cas échéant, aimerier-vous en avoir un ☐ Yes / Oui ☑ No / Non

s.15(1) - Int'l

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure Departure - Arrival / Départ - Arrivée	Transportation Transport Mode	Flight Class	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de
28/09/2012	Ottawa	London	23:25 - 11:10 next day	Air	Business	1	tbc	
02/10/2012	London	Budapest	14:30 - 18:00	Air	Business	1	tbc	
06/10/2012	Budapest	Buenos Aires	19:15 - 07:00 next day	Air	Business	1	tbc	
10/10/2012	Buenos Aires	Ottawa	18:00 - 08:00 next day	Air	Business	2		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) / Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$684.00	Accomodation (green page hotel) / Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$2,560.00
Mid-size car rental (collision damage waiver mandatory / Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory / Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: / Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable / Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (préciser la <classe> si-dussus)	$0.00
Transportation / Transport	$920.00		
Meals and incidentals / Repas et frais accessoires	$1,329.21		
Other (Specify) - Autre (préciser)	$270.00		

☐ First class (Deputy Head or equivalent approval) / Prem. Classe (approuvée par le sou-chef ou l'équiv.) Business class / Other-upgraded (other than article 3.1.9

☑ Assistant Deputy Head or equivalent approval) / Classe d'affaires - ou autre classe à tanf supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)

Approval - Approbation

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

The business class is required due to length of flights. Hotel cost is always higher in London.

Part D - Partie D

Estimated Cost - Coût estimatif

Prepaid - Prépayé

$9,366.75

Other - Autre

$5,763.21

Trip Total - Coût total du voyage

$15,129.96

Funding - Financement

A) Travellers cheques / Chèques de voyage

Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00

B) Other advance / Autre avance

Cheque / Chèque	$0.00
Cash / Comptant	$0.00

Total funding requested (A + B) / Financement total demandé (A + B): $0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.

J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Signature: [signature] Date: 20120828

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature	Date
[signature]	Sept 6/12	[signature]	

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0					

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		THC NCSD T11	475- PSCYBINTLENG - 500099177	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur gestion des finances publiques et certifié au termes de l'article du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	Date

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$9,366.75
Train / Train	$0.00
Other / Autres	$0.00
	$9,366.75

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$228.00	3	$684.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	$320.00	8	$2,560.00
			$3,244.00
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employe	0.545	0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$60.00	$920.00
	Airport - Hotel - Meetings		$300.00	
	Hotel - Airport		$300.00	
	Airport to Home		$60.00	
	Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$920.00

London	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$24.87	3	$74.61
Lunch / Déjeuners	$45.38	4	$181.52
Dinner / Dîners	$60.51	2	$121.02
Incidentals /Frais divers	$41.84	2	$83.68
	London	Meals	$460.83

Budapest	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners (receipts required) Estimated rate	$20.00	4	$80.00
Lunch / Déjeuners	$25.18	3	$75.54
Dinner / Dîners	$34.96	4	$139.84
Incidentals /Frais divers	$24.06	4	$96.24
	Budapest	Meals	$391.62

Buenos Aires	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners (receipts required) Estimated rate	$20.00	5	$100.00
Lunch / Déjeuners	$23.62	5	$118.10
Dinner / Dîners	$31.56	4	$126.24
Incidentals /Frais divers	$22.07	6	$132.42
	Buenos Aires	Meals	$476.76

TOTAL MEALS	~~$852.45~~	1,329.22
Business Phone / Téléphone d'affaires	$50.00	
Airport Improvement Fee / Frais de l'Aeropart	$0.00	
Cash Advance Fee / Frais d'avances	$20.00	
Misc. Business Services / Diverses charges d'affaires	$100.00	
Miscellaneous / Diverses - Conference Fees	$100.00	
	$270.00	

Public Safety Canada / Sécurité publique Canada

s.15(1) - Int'l

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
	From - *Du :*	To - *Au :*
First Awareness Conference for the Protection of Critical Infrastrucure and Cyber Security	October 6, 2012	October 10, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Buenos Aires, Argentina	$	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)*	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?*	
Agenda is atached.	☒Yes/Oui	☐No/Non

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Robert Gordon	National Cyber Security Directorate - NS Branch	340 Laurier Ave, 11th Floor	613-949-7380

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Mr. Gordon will participate as the keynote speaker to the conference. The conference will be a public event and open to the news media. Mr. Gordon has been asked to outline the Canadian experience in cyber security and Canada's participation in the Meridian process. His presentation will be followed by a ten minute question and answer session.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

[redacted] Mr. Gordon's presentation is consistent with Canada's Cyber Security Strategy that identified the essential requirement of international collaboration if cyberspace is to be secured and it will be an opportunity to highlight the Canadian approach to cyber security and the results of that effort.

Argentina will be hosting the Meridian 2013 conference. Mr. Gordon will use the occasion to indicate PS's willingness to participate as a member of the Program Committee (PC) for the conference. [redacted]

This is the second invitation from the Argentinian Government to speak on cyber security issues. Unfortunately, in March 2012, PS had to decline the invitation to speak at the Critical Information Infrastructure Protection Congress on extremely short notice and a member of the Canadian Embassy delivered the presentation on behalf of PS. [redacted]

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

There will be no other Canadian representatives at the event. Other countries will be represented.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

The Department of Foreign Affairs and International Trade, including the Canadian Embassy in Buenos Aires, has been consulted during the preparation of this submission and no issues were raised concerning accepting the invitation. At their request, Mr. Gordon's agenda will include a meeting with Embassy officials to brief them on the conference and generally on developments in advancing Canada's Cyber Security Strategy. This will be helpful for Embassy staff given that Argentina will be hosting the Meridian

2013 conference and PS employees will likely be invited to participate as members of the PC for that conference.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
***Appuyé par*:**

Name of paticipant's Director General
Nom du Directeur Générale du voyageur

Date: 28/06/2012

Reviewed by/
***Examiné par*:**

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

Date: 30-8-12

Approved by/
***Approuvé par*:**

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Date: Sept 6/12

PS023

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☐ Original / Prem. demande

☑ Amended (Same levels of approval as orginal dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document

Type 2	Name of traveller - Nom du voyageur	Classification
	Robert Gordon	EX-05

Part A - Partie A

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	National Security
Address - Adresse: 269 Laurier Ave. West	Telephone No. - No. de téléphone: 613-949-7380
Branch Contact - Personne ressource à la direction: Carmen Voghel	Telephone No. - No. de téléphone: 613-991-7025
	If different address, send cheque to: / Si adresse differente, envoyer chèque à

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)?	If no, would you like to request one? / Les cas échéant, aimerier-vous en avo
To attend [redacted](Ldn) Budapest Conf. on Cyberspace (Bud)	9	☐ Yes / Oui ☑ No / Non	☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport: Mode	Flight Class	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement
28/09/2012	Ottawa	London	23:25 - 11:10 next day	Air	Business		tbc
02/10/2012	London	Budapest	14:30 - 18:00	Air	Business		tbc
06/10/2012	Budapest	Ottawa	8:25 - 17:50	Air	Business		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$0.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$2,240.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dussus)	$0.00
Transportation Transport	$620.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.)	
Meals and incidentals Repas et frais accessoires	$852.45	☑ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Other (Specify) - Autre (préciser)	$270.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$7,000.00
Other - Autre	$3,982.45
Trip Total - Coût total du voyage	$10,982.45

Funding - Financement

A) Travellers cheques / Chèques de vo	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
heque / Chèque	$0.00
ash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Signature: [signature] Date: 20120808

Ticket pick-up date and location / Date et lieu de la collecte des billet

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date
[signature]	Aug 8/2012	[signature] AOUT AUG	09 2012

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier Indicat / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0				| 0	

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
			475 PSCYBINTENG 2001	

	Description	Financial encumberance No. / No. de consignation de fonds
	THC NCSD FII	~~500004279~~ 5000 99177

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requistion for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)	Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Date
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé				Amount/Montant
Airfare / Frais d'avion				$7,000.00
Train / Train				$0.00
Other / Autres				$0.00
				$7,000.00

Estimated Cost - Coût estimatif: Other - Autre		Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)		$0.00	0	$0.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)		$320.00	7	$2,240.00
				$2,240.00
Mid-size car rental / Location d'une voiture intermédiaire				$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire		$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée				$0.00
				$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.545	0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$60.00	$620.00
	Airport - Hotel : Meetings		$200.00	
	Hotel - Airport		$200.00	
	Airport to Home		$60.00	
	Meeting - Meetings		$100.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$620.00

London	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$24.87	3	$74.61
Lunch / Déjeuners	$45.38	4	$181.52
Dinner / Dîners	$60.51	2	$121.02
Incidentals /Frais divers	$41.84	2	$83.68
			$460.83

Budapest	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners (receipts required) Estimated rate	$20.00	4	$80.00
Lunch / Déjeuners	$25.18	3	$75.54
Dinner / Dîners	$34.96	4	$139.84
Incidentals /Frais divers	$24.06	4	$96.24
			$391.62

Business Phone / Téléphone d'affaires	$50.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$20.00
Misc. Business Services / Diverses charges d'affaires	$100.00
Miscellaneous / Diverses - Conference Fees	$100.00
	$270.00

Public Safety Canada | Sécurité publique Canada

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions** Robert Gordon - Travel - London, Budapest - Sept-Oct 2012
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☐ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☐ Other Specify:

☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?
	Have I completed all the paperwork requested by the Contracting Material Management group? ☐ Is the Sole Source Checklist complete and attached? ☐ Is the Competitive Contract Checklist complete and attached?
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☐ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☐ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

PS-SP-#668337-v1-NCSD_-_2012-13_-_Gordon_-_London-Budapest_-_Sept-Oct_2012_-_Section_32_checklist

Public Safety Canada / Sécurité publique Canada

NS/SN

Routing Slip / Bordereau d'acheminement

File No / No de dossier : 389529

Deadline for DM's signature / Échéancier pour la signature du S-M :

Title / Titre : International Travel Request: Robert Gordon -London, Budapest, Argentina – September 28-October 10 2012		**ACTION REQUIRED / MESURES À PRENDRE**		
Name / Nom	**Date**	**Initials / Initiales**	**Approval or signature / Approbation ou signature**	**Information**
Originator / Auteur Robert Gordon	20120828		☒	☐
Director General CS/ Directeur général CS Robert Dick	29/8/2012		☒	☐
Director General IA/ Directeur général CAI Barbara Motzney	30-8-12		☒	☐
Senior Assistant Deputy Minister NS / Sous-ministre adjointe principale SN Lynda Clairmont			☒	☐
Acting Deputy Minister / Sous-ministre par intérim Graham Flack			☒	☐

Government of Canada / Gouvernement du Canada

PROTECTED WHEN COMPLETED (for privacy Act Statement see page 2)
PROTÉGÉ UNE FOIS REMPLI (pour l'énoncé de la Loi, sur la protection des renseignements personnels, voir la page 2)

TRAINING APPLICATION AND AUTHORIZATION
DEMANDE ET AUTORISATION DE FORMATION

For PSC USE ONLY RÉSERVÉ À la CFP		

* REFER TO INSTRUCTIONS ON PAGE 2
VOIR LES INSTRUCTIONS SUR LA PAGE 2

DEPARTMENT USE ONLY RÉSERVÉ AU MINISTÈRE	2. Special needs * (enter indicator) Besoins spéciaux * (inscrire l'indicateur)
1. File number – Numéro de dossier	

X Original / Première ☐ Amendment / Modification ☐ Cancellation / Annulation

APPLICANT INFORMATION – RENSEIGNEMENTS SUR LE CANDIDAT

3. Family name – Nom de famille	Given name and initials – Prénom et initiales
GORDON	ROBERT

4. PRI – CIDP	5. Sex – Sexe	6. Classification Gr.	S.-gr.	Lev./Niv.	7. First official language – Première langue officielle
	X Male / Homme ☐ Female / Femme	EX		5	X (1) English / Anglais ☐ (2) French / Français

8. Position title – Titre du poste: Special Advisor Cyber Security

9. Employee's office telephone number – N° de téléphone de l'employé au bureau	Facsimile – Télécopieur	E-Mail – Courrier électronique
613-949-7380		Robert.gordon@ps-sp.gc.ca

10. Department name – Nom du ministère	11. Dept. Code – Code min.	12. Branch/Division – Direction/Division
Public Safety Canada		NS

13. Office, Workstation, mailing address – Adresse postale, bureau, poste de travail	City/Postal code – Ville/Code postal
269 Laurier ave West, 17-A-1400	Ottawa K1A 0P8

14. Supervisor's name and title – Nom du surveillant et titre	Telephone No. – N° de téléphone
Lynda Clairmont, SADM	613-990-4976

15. Supervisor's Office, Workstation, mailing address – Adresse postale, bureau, poste de travail du superviseur	City/Postal code – Ville/Code postal
269 Laurier ave West, 17th floor	Ottawa K1A 0P8

16. Objective of training *- Objective de la formation *

See attached memo

L Clairmont — Aug 6, 2012 — Supervisor's – Signature – Surveillant / Date

Employee's – Signature – Employé(e) — 20120808 — Date

TRAINING INFORMATION – RENSEIGNEMENTS SUR LA FORMATION

17. Course code * Code du cours *	18. Course title – Titre du cours
	Budapest Conference on Cyberspace

19. Location of training * - Lieu de formation *	20. Date of course - Date du cours						21. Departmental training program code * Code min. du programme de formation *
	From – Du			To - Au			
	Y-A	M	D-J	Y-A	M	D-J	
Budapest, Hungary	12	10	03	12	10	06	

22. Time of training - Période retenue pour la formation	23. Duration of training * (nearest half-day) Durée de la formation * (plus proche demi-journée)	24. Language of course - Langue de cours
☐ (1) Outside working hours / En dehors des heures de travail ☐ (2) During working hours / Pendant les heures de travail	3	X English / Anglais ☐ French / Français ☐ Bilingual / Bilingue ☐ Other / Autre

25. Source of training - Source de la formation	26. Transit time (person-days) * Durée des déplacements (journées-personnes)	27. Province	28. Location* Lieu *
☐ (1) TPB/PSC DGPF/CFP ☐ (2) Dept'l Min. ☐ (3) Interdept'l Intermin. ☐ (4) University/College Université/Collège X (5) Other Autre			

29. FINANCIAL AUTHORIZATION – AUTORISATION FINANCIÈRE

Cost / Coût	Financial code (include R.C. codes only if several R.C.'s are sharing the costs, otherwise complete box 30) Code financier (indiquer des codes de C.R. uniquement si plusieurs C.R. se partagent les coûts, sinon remplir la case 30)	Estimated cost (planning purposes) Coût estimatif (à des fins de planification)	Actual cost (reporting purposes) Coût réel (à des fins de compte rendu)
Tuition fee / Reimbursement * Frais de scolarité / Remboursement * ☐ 0% ☐ 50% ☐ 100%			a) *
Travel / Living Déplacement / Subsistance			b)
Other * Autres *			c) *
30. Responsibility centre (collator) code Code du centre de responsabilité (destinataire) → 475	TOTAL →	0.00	d)

Recipient organization code Code d'organization du/de la récipiendaire	Récipient référence code Code de référence du/de la récipiendaire

31. Financial signing authority (Certified that funds are available pursuant to section 32(1)FAA) * Signataire autorisé en matière financière (Attestation de la disponibilité des fonds aux termes du par. 32(1) LGFP) *	Date	32. This candidate meets course selection criteria (Manager's approval) Le candidat satisfait aux critères de sélection du cours (approbation du gestionnaire)	Date

33. DEPARTMENTAL TRAINING COORDINATOR* - COORDONNATEUR DE LA FORMATION DU MINISTÈRE *

Remarks - Observations

Signature — Date

34. DEPARTMENTAL USE CODES * - CODES À L'USAGE DU MINISTÈRE *

A	B	C	
D	E	F	R S T U V W X Y Z

GC 211 (2001-12) (Word version R-02-01)

DISTRIBUTION
Original = PSC/Finance Division/Human Resources Division — Copy = Origin
Original = CFP/Division des finances/Division des ressources humaines — Copie = Auteu

Public Safety Canada | Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: August 24 2012

To – A

Graham Flack
A/Deputy Minister
Public Safety Canada

Requested by – Demandé par

Robert Gordon
Special Advisor
NS-NCSD

Name of Conference – Titre de la conférence

First Awareness Conference for the Protection of Critical Infrastrucure and Cyber Security

Type of Conference – Genre de conférence

☒ International / Internationale ☐ National / Nationale ☐

Documents attached / Documentation jointe

☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur

Official Host – Hôte officiel

The Government of Argentina

Duration of Conference – Durée de la conférence

From / Du: October 9 2012 To / À: October 9 2012

Location - Adresse

Buenos Aires Argentina

Agenda – Ordre du jour

Attached

Purpose of Participation - Object de la participation

Mr. Gordon will participate as the keynote speaker to the conference. The conference will be a public event and open to the news media. Mr. Gordon has been asked to outline the Canadian experience in cyber security and Canada's participation in the Meridian process. His presentation will be followed by a ten minute question and answer session.

Financial Coding – Code financier

475 PSCYBINTLENG - 500099177

Estimated Total Cost / Coût total prévu

$ 4055.51 (Argentina only)

Recommended by – Recommandé par		Branch Approval – Approbation de la direction	
Signature	Date	Signature	Date
Assistant Deputy Minister – Sous-ministre adjoint		Deputy Minister – Sous-ministre	
Signature: L'Heureux	Date: Sept 6/12	Signature	Date: SEP 11 2012

Public Safety Canada / Sécurité publique Canada

AMEX TAN Number /Numéro de NAV

Issued By / Émis par: ELAJEUNESSE

Date Issued / Date d'émmision : 2012/08/14

TAN Number Info / Info numéro de NAV

Company Code / Code de société:	0880
TAN Prefix / Préfixe de NAV:	LNW9
TAN Number / Numéro de NAV:	LNW919804
Sequence Number / Numéro de séquence:	0001
Date Issued / Date d'émmision:	2012/08/14

Trip Details Info / Détails du voyage

Traveller Name / Nom du voyageur:	ROBERT GORDON
Date of Departure / Date de départ:	2012/08/22
Destination / Destination:	LONDON,BUDAPEST
Trip Purpose / Objet du voyage:	MEETING

Financial Coding Info / Info code financier

Cost Center / Centre de coûts:	475
GL Account / Compte général:	2007
Internal Order / Ordre interne:	PSABASE
Earmarked Funds / Fonds réservés:	500099177001
Name of Sec.32 Officer / Nom de l'agent Sec. 32:	GRAHAM FLACK
Estimated Travel Charge / Estimation des frais de voyage:	7,000.00

Comments / Commentaires

Text / Texte:	THC - NCSD-T11 - 05 MEETING & CYBER CONF. BUDAPEST

If you have any questions or would like to cancel this TAN please contact Elizabeth LAJEUNESSE @ 6139917004

Pour toute question ou pour annuler ce NAV, veuillez communiquer avec Elizabeth LAJEUNESSE @ 6139917004

Public Safety Canada | Sécurité publique Canada
Senior Assistant Deputy Minister | Sous-ministre adjoint principal
Ottawa, Canada
K1A 0P8

SECRET

DATE:

File No.: 389529

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, CMB

INTERNATIONAL TRAVEL AUTHORITY
FOR LYNDA CLAIRMONT AND BOB GORDON:
BUDAPEST CONFERENCE ON CYBERSPACE, BUDAPEST
[redacted] LONDON SEPTEMBER 29 TO OCTOBER 6, 2012
INTELLIGENCE POLICY FORUM , CANBERRA – SEPTEMBER 26 TO 28, 2012

(Decision sought)

ISSUE

Your approval is sought for me to attend the Intelligence Policy Forum (IPF) in Canberra, Australia, from September 26 to the 28, 2012. I also request your approval for Bob Gordon, Special Advisor Cyber Security, and I to attend the [redacted] London, United Kingdom (U.K.) September 30 to October 2, 2012 and the Budapest Conference on Cyberspace to be held in Budapest, Hungary on October 3 to 6, 2012.

BACKGROUND

Intelligence Policy Forum

[redacted]

[redacted]

.../2

Canada

s.15(1) - Int'l

[redacted]

Budapest Conference on Cyberspace

The Hungarian Government is hosting the Budapest Conference on Cyberspace in Budapest on October 3 to 6, 2012 (the Conference). The Conference is a follow-up to the London International Cyber Conference hosted by The Rt Honourable William Hague, Secretary of State for Foreign and Commonwealth Affairs on November 1 and 2, 2011, in London. I was the Head of the Canadian Delegation and Bob Gordon was a member of the delegation.

The London Conference brought together Ministers, senior government officials, industry leaders, and representatives of the Internet technical community and civil society. Approximately 700 participants from 60 countries took part. The London Conference was an important first step in building a broad international consensus on how best to realize the economic and social benefits of cyberspace. [redacted]

The Honourable John Baird, Minister of Foreign Affairs, has received an invitation from the Minister of Foreign Affairs of Hungary to attend the Conference. Background information in the invitation notes that 600 participants are expected from 70 to 75 countries. The keynote speech at the Conference will be delivered by Prime Minister Viktor Orbán.

CONSIDERATIONS

The Hungarians have provided an agenda for the Conference (**TAB A**). The Conference will focus on five themes:

1. Cyberspace and Economic Growth;
2. Cyberspace and Social Progress;
3. Cyber security: Building Frameworks for Prevention, Response and Resilience;
4. Cyberspace and International Security; and
5. Cybercrime.

In addition to the plenary and thematic sessions, some topics will be dealt with in workshops and, for some themes, three debates will be running in parallel. Based upon our experience at the London Conference, it is important that Canada is represented in all of the sessions.

The Conference is another important step in furthering the international discussion on a normative approach to cyber space. [redacted]

s.15(1) - Int'l

Canada has yet to confirm our delegation with the Hungarians. The Minister of Foreign Affairs has not yet indicated whether he will attend. I will confirm this prior to the Conference.

The estimated total cost of this trip for PS is $29,848 for me, bearing in mind that I will travel to Australia, prior to the London and Budapest' meetings and $10,982 for Bob Gordon. All costs related to this request fall within National Security's allocated Travel cap for this fiscal year.

RECOMMENDATION

It is recommended that you approve my travel to Canberra to attend the Intelligence Policy Forum from September 22 to 29. It is also recommended that you approve the travel for Bob Gordon and me to attend the Budapest Conference on Cyberspace and t London, U.K. from September 29 to October 6, 2012. Should you agree, your signature is sought on the travel request forms (**TAB B**), and enclosed conference request (**TAB C**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Bob Gordon at 613-949-7380.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures:(5)

Prepared by: Bob Gordon

I approve:

Graham Flack
Acting Deputy Minister

s.15(1) - Int'l

THE BUDAPEST CONFERENCE ON CYBERSPACE
Millenáris Park, 4-5 October 2012
DRAFT PROGRAMME

Wednesday 3 October

17:00-19:00 Registration
19:00-22:00 Opening reception and mini-concert

Thursday 4 October

08:00-09:00 Registration and welcome coffee

09:00-09:45 OPENING ADDRESSES

09:45-11:15 PLENARY SESSION I: *„Cyberspace: Dynamics and Perspectives"*

11:15-11:45 Coffee break

11:45-13:15 PLENARY SESSION II: *„Capacity-building: Policy Implications and Drivers"*

13:15-14:30 Lunch break

14:30-16:30 PARALLEL THEMATIC PANEL DISCUSSIONS 1: *„Opportunities and challenges"*

A/ Economic growth and development
B/ Social benefits
C/ Cyber security: Building Frameworks for Prevention, Response and Resilience

14:00-16:30 Youth Forum

16:30-17:00 Coffee break

17:00-18:00 Debate with the Youth Forum participants on the conclusions of three thematic panel discussions

09:00-18:00 Hungarian cyber innovation showcase

18:00-20:00 Evening reception

Friday 5 October

08:00-09:00 Registration and welcome coffee

09:00-10:30 PLENARY SESSION III: *„Sharing knowledge for global challenges" - Forum of International and Regional Organisations*

10:30-11:00 Coffee break

11:00-13:00 PARALLEL THEMATIC PANEL DISCUSSIONS 2: *„ Opportunities and challenges"*

D/ International security
E/ Cybercrime

13:00-14:30 Lunch break

14:30 CLOSING PLENARY SESSION IV

Budapest Cyber Workshops

We are currently considering possible workshops on the following topics: Children in Cyberspace; Critical Infrastructure Protection; Law Enforcement in Cyberspace; Digital Confidence; R&D on Cyberspace; E-Health; Capacity-building; and others.

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: August 29, 2012

File No.: 389338
RDIMS No.: 661418

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson. ADM, CMB

INTERNATIONAL TRAVEL AUTHORIZATION FOR FRÉDÉRIC MASSICOTTE TO ATTEND A MEETING IN HAGUE AND A CONFERENCE IN AMSTERDAM SEPTEMBER 8-15, 2012

(Signature required)

ISSUE

Your approval is sought for an international travel request for Dr. Frédéric Massicotte, Cyber Technical Support Officer, to meet with the North Atlantic Treaty Organization, NATO Consultation Command and Control Agency (NATO NC3A) in The Hague, on September 10 and to attend the Research in Attacks, Intrusions and Defenses conference (RAID) in Amsterdam from September 12-14, 2012.

BACKGROUND

RAID is an active international operational research community in the field of cyber security. This community provides Cyber Security Incident Response Teams (CSIRTs) with tools to collect and analyse malware samples and threat indicators. Lead Research and Development (R&D) teams from around the world with whom the Canadian Cyber Incident Response Centre (CCIRC) maintains operational ties, such as Symantec, Trend Micro, Virus Total, and Anubis, are also involved in this community. This conference is rated amongst the top five cyber security conferences in the world, along with others such as RSA and Institute of Electrical and Electronics Engineers (IEEE) Security and Privacy Conferences.

CONSIDERATIONS

Once Dr. Massicotte arrives in Amsterdam, he will first take the train to The Hague to visit NATO NC3A. This agency's office is close to the conference and it has extended an invitation to CCIRC to visit their site and discuss common cyber security technical challenges such as threat modeling, state of the art CSIRT capabilities, cyber security information analysis and sharing. This is an opportunity which aligns well with the RAID

conference and adds significant value to CCIRC activities such as lab capability development and operations. Developing an operational relationship with NATO Computer Incident Response Capability was identified in CCIRC's business plan for this fiscal year.

After this meeting, Dr. Massicotte will travel by train back to Amsterdam to attend the RAID conference. Dr. Massicotte will be engaged in discussions with lead R&D teams from around the world with whom CCIRC maintains operational ties in order to maintain and build trust relationships. As there are a number of presentations at RAID that are relevant to CCIRC operations, it will be very beneficial for Dr. Massicotte to participate in technical sessions, as seen in the conference agenda (**TAB A**).

The estimated total cost for this trip is $6,917.28. All costs related to this request fall within my sector's allocated Travel/Hospitality/Conference cap for this fiscal year.

RECOMMENDATION

It is recommended that you approve Dr. Massicotte's travel to the Netherlands from September 10-14, 2012 by signing the Travel Authority and Advance forms (**TAB B**) and the Training forms (**TAB C**). My approval is noted in the International Travel Request (**TAB D**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

L Clairmont

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (4)

I approve:

SEP 0 4 2012

Graham Flack
Acting Deputy Minister

Prepared by: Frédéric Massicotte

GOVERNMENT OF CANADA / GOUVERNEME DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval oas orginal dated)
Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) N°. d'aut de voyager (NAV)	Document No. RDIMS - N° du document SGGDI

Type 2 | Name of traveller - Nom du voyageur: Frederic Massicotte | Classification: CS-03

Part A - Partie A

Department - Ministère: Public Safety Canada	Branch / Division / Group - Direction / Division / Groupe: NS-NCSD-CCIRC
Address - Adresse: 257 Slater, 4th Floor	Telephone No. - No. de téléphone:
Branch Contact - Personne ressource à la direction: Jane Hayward	Telephone No. - No. de téléphone: 613-991-1982
Purpose of travel - Objet du voyage	No. of days / Nbre de jours: 8

If different address, send cheque to: / Si adresse differente, envoyer chèque à

Do you have a Govt Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CV: ☐ Yes / Oui ☑ No / Non

If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une? ☑ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport: Mode	Transportation Transport: Class	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
Sept 8 2012	Ottawa	Amsterdam	19:40 - 12:25 (next day	Air	Economy			
Sept 9 2012	Amsterdam	The Hague	15:00	Rail			Hilton the Hague	
Sept 11 2012	The Hague	Amsterdam	12:00	Rail				
Sept 15 2012	Amsterdam, NL	Ottawa	11:30 - 16:09	Air	Economy		Best Western Amsterdam	

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$653.20	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$432.38
Mid-size car rental (collision damage waiver mandatory Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory Location d'une voiture non intermédiaire (assurance-collision du	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☑ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$44.40	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus)	$0.00
Transportation Transport	$400.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) 3.1.9 ☐ Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Meals and incidentals Repas et frais accessoires	$888.64		
Other (Specify) - Autre (préciser) Business calls	$50.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Only one hotel listed in the white pages and it was too far from the meeting location. We will be saving on transportation costs.

Part D - Partie D

Estimated Cost - Coût estimatif
Prepaid - Prépayé
$4,448.66
Other - Autre
$2,468.62
Trip Total - Coût total du voyage
$6,917.28

Funding - Financement

A) Travellers cheques / Chèques de voyage
Cdn / Can
US / É.U. $0.00
Other / Autre $0.00

B) Other advance / Autre avance
Cheque / Chèque $0.00
Cash / Comptant $0.00

Total funding requested (A + B)
Financement total demandé (A + B)
$0.00

Ticket pick-up date and location
Date et lieu de la collecte des billets

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Frederic Massicotte — Signature — 03/04/2012 — Date

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signa	Date
L'Laurmont	Aug 29/12		SEP 0 4 201

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier Indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0					

Accounting Information / Renseignement comptables

Tyoe 4

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
		THC NCSD-T41	223-PSABASE 2001-500099024 Line 1 & 2	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) Vérifié conform (TPSGC) (signature)		Date
Services officer (PWGSC) (signature) Agent responsible (TPSGC) (signature)	Signature	

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$4,341.66
Train / Train	$107.00
Other / Autres	$0.00
	$4,448.66

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du ré	$163.30	4	$653.20
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERTE** du répe	$216.19	2	$432.38
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire			$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.555	80.0	$44.40

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$0.00	$400.00
	Airport - Hotel / Meetings		$100.00	
	Hotel - Airport		$100.00	
	Airport to Home		$0.00	
	Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$400.00

Canadian	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.60**		$0.00
Lunch / Déjeuners	**$14.85**		$0.00
Dinner / Dîners	**$40.85**		$0.00
Incidentals /Frais divers	**$17.30**	1	$17.30
		Total Canadian	$17.30

Hague	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$40.06**	2	$80.13
Lunch / Déjeuners	**$40.06**	3	$120.19
Dinner / Dîners	**$62.46**	2	$124.92
Incidentals /Frais divers	**$41.01**	2	$82.02
		Total Hague	$407.25

Amsterdam, Netherlands	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$40.50**	2	$81.00
Lunch / Déjeuners	**$40.50**	1	$40.50
Dinner / Dîners	**$52.32**	3	$156.96
Incidentals /Frais divers	**$37.13**	5	$185.63
		Total Amsterdam, N	$464.09
		GRAND TOTAL	**$888.64**

Business Phone / Téléphone d'affaires	$50.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses - Conference Fees	$0.00
	$50.00

Public Safety Canada / Sécurité publique Canada

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions** Travel - F Massicotte Amsterdam Sept 2012
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☐ Request to Attend Conferences Form	☒ Training Application and Authorization Form	☐ Membership Approval Form	☒ Other Specify: ITR

☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?
	Have I completed all the paperwork requested by the Contracting Material Management group? ☒ Is the Sole Source Checklist complete and attached? ☐ Is the Competitive Contract Checklist complete and attached?
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☐ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☐ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

	Purchase Requisition #	Purchase Order #	Funds Commitment #:	RDIMS #
	[redacted]	[redacted]	500099024 Line 1,2,3	664900

INSTRUCTIONS FOR COMPLETION OF SECTION 32 CHECKLIST

These instructions are meant to assist staff in the preparation of the Section 32 checklist for Grants and Contributions payments. The numbers used relate to the same number on the checklist.

Legend: ☒ **= completed or has been considered**

1) Use the Delegated Financial Signing Authorities matrix located at: http://icarchive/foryou/divisions/comptroller/dfsa/_fl/dfsa-matrix-dept-eng.pdf to ensure that the person exercising Expenditure Initiation authority has the authority delegated to his/her position.

2) Forms can be found in Microsoft Office/Excel templates when starting a new document.

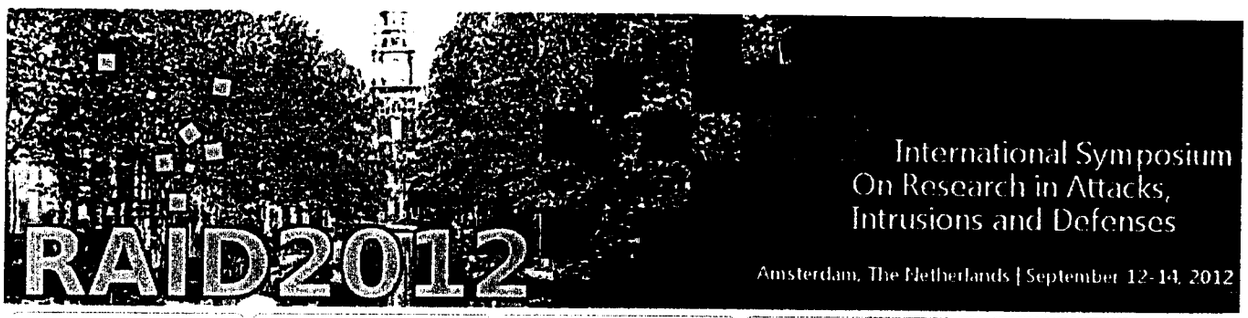
3) Ensure that you have the authority to sign under Section 32: a) by using the Delegated Financial Signing Authorities matrix located at: http://icarchive/foryou/divisions/comptroller/dfsa/_fl/dfsa-matrix-dept-eng.pdf; and b) by the completion of a Financial Authority Specimen Signature Record.

4) Run a free balance report in SAP to ensure that you have sufficient unencumbered funds to legally sign Section 32.

5) These forms are applicable to the Contracting and Procurement Unit and may not be applicable to expenditures such as Hospitality and Travel.

6) Enter the commitment into the SAP system and verify that the correct g/l, cost center, amount, vendor and description are entered. When the commitment is entered and saved please provide the Fund Commitment/ Purchase Order number on the indicated line.

7) When entering into a contract for the purchase of a good, please consider if the following will be a capital asset as per the criteria stated. Please contact External Reporting Group within the Financial Services & Systems Division (FSSD) for further instruction on ensuring the proper coding/description.



Program (really tentative)

Wednesday September 12th

Registration *Registration Desk, Ground Floor*

From 11.00 Registration is possible till 18.00.

Opening Remarks *Auditorium, First Floor*

13:00 - 13:30 TBD

Keynote *Auditorium, First Floor*

13:30 - 14:30 TBD

Session I (Virtualization) *Auditorium, First Floor*

14:30 - 15:00 **Trusted VM Snapshots in Untrusted Cloud Infrastructures**
Abhinav Srivastava, Himanshu Raj, Jonathon Giffin, Paul England

15:00 - 15:30 **Secure and Robust Monitoring of Virtual Machines through Guest-Assisted Introspection**
Martim Carbone, Matthew Conover, Bruce Montague, Wenke Lee

15:30 - 16:00 **Assessing the Trustworthiness of Drivers**
Shengzhi Zhang and Peng Liu

Break *Side Rooms, First Floor*

16:00 - 16:30 Coffee and Biscuits

Session II (Attacks and Defenses) *Auditorium, First Floor*

16:30 - 17:00 **Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat**
Olivier Thonnard, Leyla Bilge, Gavin O'Gorman, Seán Kiernan, Martin Lee

17:00 - 17:30 **Memory Errors: The Past, the Present, and the Future**
Victor van der Veen, Nitish dutt-Sharma, Lorenzo Cavallaro, Herbert Bos

17:30 - 18:00 **A Memory Access Validation Scheme against Payload Injection Attacks**
Dongkyun Ahn and Gyungho Lee

Thursday September 13th

Breakfast *Foyer, First Floor*

19:30 - 22:30 Dinner at the Restaurant In De Waag

Friday September 14th

Breakfast *Side Rooms, First Floor*

08:30 - 09:00 Dutch Breakfast

Session VI (Intrusion Detection) *Auditorium, First Floor*

09:00 - 09:30 **ALERT-ID: Analyze Logs of the network Element in Real Time for Intrusion Detection**
Jie Chu, Zihui Ge, Richard Huber, Ping Ji, Jennifer Yates, Yung-Chao Yu

09:30 - 10:00 **A Lone Wolf No More: Supporting Network Intrusion Detection with Real-Time Intelligence**
Bernhard Amann, Robin Sommer, Aashish Sharma, and Seth Hall

10:00 - 10:30 **GPP-grep: High-Speed Regular Expression Processing Engine on General Purpose Processors**
Victor C. Valgenti, Jatin Chhugani, Yan Sun, Nadathur Satish, Min Sik Kim, Changkyu Kim, Pradeep Dubey

10:30 - 11:00 **N-gram Against the Machine: On the Feasibility of the N-gram Network Analysis for Binary Protocols**
Dina Hadžiosmanović, Lorenzo Simionato, Damiano Bolzoni, Emmanuele Zambon, and Sandro Etalle

Concluding Remarks *Auditorium, First Floor*

11:00 - 11:30 TBD

Lunch *The Basket*

12:00 - 13:00 Dutch Lunch and Drinks

General Credits - Stefano Ortolani | Background banner photo - Joan Campderros-i-Canas

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
Research in Attacks, Intrusions and Defenses Conference (RAID), and North Atlantic Treaty Organization, NATO Consultation Command and Control Agency (NATO NC3A), NATO Computer Incidence Response Capability (NATO CIRC) meeting	From - *Du* : 10/09/2012	To - *Au* : 14/09/2012
Location (City, Country) - *Lieu (Ville, Pays)* The Hague and Amsterdam, Netherlands	Estimated total cost - *Coût total prévu* $6917.28	
Description of meeting (provide agenda) *Description de l'événement (joindre l'ordre du jour)* Recent Advance is Intrusion Detection (RAID) is an active international operational research community in the field of cyber security. This community provides Cyber Security Incident Response Teams (CSIRTs) with tools to collect and analyse malware samples and threat indicators.(agenda attached)	Pre-approved under Branch travel plans? *Pré-approuvé selon les directives sur les voyages de la direction générale?* ☐Yes/Oui ☒No/Non	

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Frédéric Massicotte	NS/NCSD/CCIRC	257 Slater, Ottawa, Ontario	613 991-7015

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Annual conference for RAID
Learning visit, meeting at NATO NC3A and NATO CIRC

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

The RAID conference is an opportunity to meet lead Research & Development teams from around the world with whom CCIRC maintains operational ties, such as Symantec, Trend Micro, Virus Total and Anubis, are namely involved in this community.

The meeting at NATO is an opportunity which aligns well with the RAID conference and adds significant value to CCIRC activities such as lab capability development and operations. Developing an operational relationship with NATO was identified in CCIRC business plan for this Fiscal Year.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

N/A

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

N/A

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et partager le rapport avec les représentants du MAECI et la Division des affaires internationales de Sécurité publique Canada.

Supported by/
Appuyé par :

for L. Dick — 07/08/2012

Name of paticipant's Director General
Nom du Directeur Générale du voyageur

Date

Reviewed by/

000571

Examiné par :

Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

9-8-12
Date

Approved by/
Approuvé par :

Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur

Aug 29/12.
Date

PS023

Government of Canada / Gouvernement du Canada

PROTECTED WHEN COMPLETED (for privacy Act Statement see page 2)

PROTÉGÉ UNE FOIS REMPLIE (pour l'énoncé de la Loi sur la protection des renseignements personnels, voir la page 2)

TRAINING APPLICATION AND AUTHORIZATION
DEMANDE ET AUTORISATION DE FORMATION

s.19(1)

* REFER TO INSTRUCTIONS ON PAGE 2
VOIR LES INSTRUCTIONS SUR LA PAGE 2

☒ Original Première ☐ Amendment Modification ☐ Cancellation Annulation

For PSC USE ONLY RÉSERVÉ À la CFP		

DEPARTMENT USE ONLY RÉSERVÉ AU MINISTÈRE	2. Special needs * (enter indicator) Besoins spéciaux * (inscrire l'indicateur)
1. File number – Numéro de dossier	

APPLICANT INFORMATION – RENSEIGNEMENTS SUR LE CANDIDAT

3. Family name – Nom de famille	Given name and initials – Prénom et initiales
Massicotte	Frédéric

4. PRI – CIDP	5. Sex – Sexe	6. Classification Gr.	S.-gr.	Lev.Niv.	7. First official language – Première langue officielle
[redacted]	☒ Male Homme ☐ Female Femme	CS		3	☐ (1) English Anglais ☒ (2) French Français

8. Position title – Titre du poste		
Senior Incident Handler		
9. Employee's office telephone number – N° de téléphone de l'employé au bureau: 613 991-7015	Facsimile – Télécopieur	E-Mail – Courrier électronique: frederic.massicotte@ps-sp.gc.ca

10. Department name – Nom du ministère	11. Dept. Code – Code min.	12. Branch/Division – Direction/Division
Public Safety	0880	NCSD

13. Office, Workstation, mailing address – Adresse postale, bureau, poste de travail	City/Postal code – Ville/Code postal
257 Slater, 2nd floor	Ottawa Ontario
14. Supervisor's name and title – Nom du surveillant et titre	Telephone No. – N° de téléphone
Windy Anderson, Director of CCIRC	613 944-4074
15. Supervisor's Office, Workstation, mailing address – Adresse postale, bureau, poste de travail du superviseur	City/Postal code – Ville/Code postal
257 Slater, 2nd floor	K1A 0M6

16. Objective of training * - Objective de la formation *

RAID

Engage in discussions with lead R&D teams from around the world with whom CCIRC maintains operational ties in order to build trust relationships. Participate in technical sessions.

NC3A/NCIRC

Discuss common cyber security technical challenges such as threat modeling, state-of-the-art CSIRT capabilities, cyber security information analysis and sharing.

W Anderson — Supervisor's – Signature – Surveillant
Aug 3/12 — Date
Frédéric Massicotte — Employee's – Signature – Employé(e)
03/08/2012. — Date

TRAINING INFORMATION – RENSEIGNEMENTS SUR LA FORMATION

17. Course code * Code du cours *	18. Course title – Titre du cours
	Research in Attacks, Intrusions and Defenses conference, NATO NC3A meetings

19. Location of training * - Lieu de formation *	20. Date of course - Date du cours From – Du Y-A	M	D-J	To - Au Y-A	M	D-J	21. Departmental training program code * Code min. du programme de formation *
Amsterdam, Netherlands	12	09	10	12	09	14	001

22. Time of training - Période retenue pour la formation	23. Duration of training * (nearest half-day) Durée de la formation * (plus proche demi-journée)	24. Language of course - Langue de cours
☐ (1) Outside working hours En dehors des heures de travail ☒ (2) During working hours Pendant les heures de travail	3	☐ English Anglais ☒ French Français ☐ Bilingual Bilingue ☐ Other Autre

25. Source of training - Source de la formation	26. Transit time (person-days) * Durée des déplacements (journées-personnes)	27. Province	28. Location* Lieu *
☐ (1) TPB/PSC DGPF/CFP ☐ (2) Dept'l Min. ☒ (3) Interdept'l Intermin. ☐ (4) University/College Université/Collège ☒ (5) Other Autre	2	OT	

29. FINANCIAL AUTHORIZATION – AUTORISATION FINANCIÈRE

Cost Coût	Financial code (include R.C. codes only if several R.C.'s are sharing the costs, otherwise complete box 30) Code financier (indiquer des codes de C.R. uniquement si plusieurs C.R. se partagent les coûts, sinon remplir la case 30)	Estimated cost (planning purposes) Coût estimatif (à des fins de planification)	Actual cost (reporting purposes) Coût réel (à des fins de compte rendu)
Tuition fee / Reimbursement * Frais de scolarité / Remboursement * ☐ 0% ☐ 50% ☒ 100%	5000990 24 line 3	771.40	a) *
Travel / Living Déplacement / Subsistance	5000990 24 line 1, 2	6917.28	b)
Other * Autres *			c) *
30. Responsibility centre (collator) code Code du centre de responsabilité (destinataire) 223	TOTAL	8006.72	d)

Recipient organization code Code d'organization du/de la récipiendaire	Récipient référence code Code de référence du/de la récipiendaire
0990	

31. Financial signing authority (Certified that funds are available pursuant to section 32(1)FAA) * Signataire autorisé en matière financière (Attestation de la disponibilité des fonds aux termes du par. 32(1) LGFP) *	Date	32. This candidate meets course selection criteria (Manager's approval) Le candidat satisfait aux critères de sélection du cours (approbation du gestionnaire)	Date

Public Safety Canada | Sécurité publique Canada
Senior Assistant Deputy Minister | Sous-ministre adjoint principal
Ottawa, Canada
K1A 0P8

SECRET

DATE: JUL -3 2012

File No./TD No. 388611
RDMIS 638628

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson

AMMENDMENT FOR TRAVEL TO INDIA & ISRAEL AND ATTENDANCE AT THE EAST/WEST INSTITUTE – 3RD WORLDWIDE CYBER SECURITY SUMMIT NEW DELHI, INDIA, OCTOBER 30 & 31, 2012

(Signature Required)

ISSUE

To seek your approval to amend the dates for travel to Tel-Aviv, Israel the week of October 22, 2012, for Lynda Clairmont, Robert Gordon, and John Davies. Please note that Lynda Clairmont and Robert Gordon will continue on to New Delhi, India for discussions with representatives of the Indian Government and to attend the 3rd Worldwide Cybersecurity Summit in New Delhi, October 30 and 31, 2012, organized by the EastWest Institute (EWI). You should also note that Lynda Clairmont will be flying out from Washington to Tel-Aviv, as she will be chairing the Emergency Management Consultative Group meeting on October 23.

BACKGROUND

On April 2, 2012, the former Deputy Minister, Public Safety Canada (PS), approved the travel for Lynda Clairmont, Robert Gordon, and John Davies to travel to Tel-Aviv, Israel the week of May 28, 2012, and for Lynda Clairmont and Robert Gordon to continue on to New Delhi, India. The approved memorandum is attached (**TAB A**). Due to circumstances beyond our control, it was necessary to postpone that travel. The rationale for traveling to Israel and India remains the same.

It is cost effective to schedule the timing of the visit to New Delhi to coincide with the 3rd Worldwide Cyber security Summit. PS has been represented at the previous summits organized by EWI. The First Worldwide Cyber security Summit: Protecting the Digital Economy was held in Dallas in May 2010, followed by the Second Worldwide Cyber security Summit: Mobilizing for International Action, held in London in June 2011.

Both summits provided an opportunity to discuss cyber security issues with senior private and public sector decision makers from around the world including discussing Canada's approach in advancing cyber security.

The theme for the 3rd Summit is "The Next Billion Netizens Connect: Meeting the Challenges". The summit focus on many of the current cyber security issues [redacted] such as measuring the cyber security problem, policies for multinational corporations in cyber space, harmonization of legal frameworks for cyber space, dealing with the new power structure of non-state actors in cyber space, emergency preparedness for the financial services sector in cyber space and 'rules of the road' for cyber weaponry. The summit agenda is attached (**TAB B**). These sessions will be helpful in informing the development of Canadian policy. As the summit will have simultaneous sessions, having two employees participate will ensure maximum benefit from the summit. It is anticipated that attending the summit will also facilitate further discussion with representatives of the Indian Government who will likely be attending given the high profile of the event.

The total estimated cost of this travel is $45,083.19, plus anticipated registration fees of $1,250 per person for the Cyber security Summit in New Delhi. These trips were included in the travel cap for the National Security Branch.

RECOMMENDATION

It is recommended that you approve the enclosed amended Travel Authority and Advance Form (**TAB C**) for Lynda Clairmont, Robert Gordon, and John Davies.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Robert Dick, Director General, Cyber Security Strategy, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (3)

I approve:

JUL 10 2012

Graham Flack
Acting Deputy Minister

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

Prepared by: Robert Gordon

s.15(1) - Int'l

Public Safety Canada / Sécurité publique Canada
Senior Assistant Deputy Minister / Sous-ministre adjoint principal
Ottawa, Canada K1A 0P8

SECRET

DATE: MAR 2 7 2012

File No. : 1516-1 / 386562

MEMORANDUM FOR THE DEPUTY MINISTER
via: Gary Robertson, ADM, CMB

INTERNATIONAL TRAVEL REQUEST FOR LYNDA CLAIRMONT, BOB GORDON AND JOHN DAVIES: ISRAEL AND INDIA

(Signature required)

ISSUE

To seek your approval for Lynda Clairmont, Bob Gordon, and John Davies to travel to Tel-Aviv, Israel the week of May 28, 2012, and for Lynda Clairmont and Bob Gordon to continue on to New Delhi, India.

BACKGROUND

The formal agenda for the proposed travel to Israel and India is currently under development; however the focus will be on national security.

Israel

The proposed travel to Israel will provide senior Public Safety Canada (PS) officials the opportunity to engage their Israeli counterparts on a range of national security issues,

s.15(1) - Int'l

SECRET

[redacted]

India

[redacted]

.../3

s.15(1) - Int'l

[redacted]

India is also a member of the UN Group of Governmental Experts (GGE), which seeks to examine the challenges that cyberspace may pose to international peace and security. Canada joined the GGE in 2011 and is represented by the Department of Foreign Affairs and International Trade. [redacted]

The total estimated cost of this travel is $53,070.33 and it will be included in the travel cap for the National Security Branch and in the 2012-2013 travel plan.

The International Travel Request (**TAB A**) is enclosed for your information. This request is being submitted as early as possible in order to benefit from cost savings associated with early booking. When booking, all efforts will be made to ensure value for money.

RECOMMENDATION

It is recommended that you approve the enclosed Travel Authority and Advance Form (**TAB B**) for Lynda Clairmont, Bob Gordon and John Davies.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Bob Gordon, Special Advisor, Cyber Security, at 613-949-7380.

Lynda Clairmont
for Senior Assistant Deputy Minister
National Security

Enclosures: (2)

I approve:

AVR APR - 2 2012

William V. Baker

Prepared by: Terri Zygoumis

ENT GOUVERNEMEN
JA DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

approval oas orginal dated)

des agents du même niveau que
Datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document
	LNW9	

Type 2	Name of traveller - Nom du voyageur	Classification
	Robert (Bob) Gordon	EX-05

	Branch / Division / Group - Direction / Division / Groupe
nada	National Security
ve. West	Telephone No. - No. de téléphone: 613-949-7380
t - Personne ressource à la direction	Telephone No. - No. de téléphone
ward	613-991-1982

If different address, send cheque to: / Si adresse differente, envoyer chèque à

/ travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)?	Would you like to request one? / Aimerier-vous en avoir une?
et Senior officials in Tel Aviv and New Delhi to ss Cyber and CT and attend the East West Third rld Wide Cyber Summit	12	☑ Yes / Oui ☐ No / Non	☐ Yes / ☑ No / Non

art B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport Mode	Flight Class	No. of meals prepaid Nbre de	Accommodation Hébergement
22/10/2012	Ottawa	Tel Aviv	14:00 - 10:40 next day	Air	Business	2	TBD
26/10/2012	Tel Aviv	New Delhi	15:30 - 09:10 next day	Air	Business	2	TBD
02/11/2012	New Delhi	Ottawa	03:05 - 16:20	Air	Business	2	

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$0.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$3,015.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dussus)	$0.00
Transportation Transport	$520.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.)	
Meals and incidentals Repas et frais accessoires	$1,350.06	☑ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv.. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Other (Specify) - Autre (préciser)	$270.00	Approval / Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

Hotels in close proximity to meetings are above PWGSC standard rates

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$10,200.00
Other - Autre	$5,155.06
Trip Total - Coût total du voyage	$15,355.06

Funding - Financement

A) Travellers cheques / Chèques de voya	
Cdn / Can	$0.00
US / É.U.	$0.00
er / Autre	$0.00
B) Other advance / Autre avance	
/ Chèque	$0.00
Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Robert Gordon — Signature — 20120621. — Date

Ticket pick-up date and location
Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signatur	Date
Lynda Clairmont	JUL - 3 2012	Graham Flack	JUIL JUL 1 0 2012

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier ir Indicateur fournisseur	Due Date / Date d'échéance
	8 | 0				| 0	

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
			THC - T19 475- PSCYBINTENG 2001-500097675 Line 1,2	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requistion for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	Date

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé

	Amount/Montant
Airfare / Frais d'avion Business calss with additional 50% added	$10,200.00
Train / Train	$0.00
Other / Autres	$0.00
	$10,200.00

Estimated Cost - Coût estimatif: Other - Autre

	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$0.00	0	$0.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	$335.00	9	$3,015.00
			$3,015.00
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.545	0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$60.00	$520.00
	Airport - Hotel / Meetings		$100.00	
	Hotel - Airport		$100.00	
	Airport to Home		$60.00	
	Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)		**$10.00**		$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$520.00

Canadian	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.60**		$0.00
Lunch / Déjeuners	**$14.85**		$0.00
Dinner / Dîners	**$40.85**	2	$81.70
Incidentals /Frais divers	**$17.30**	2	$34.60
			$116.30

Tel Aviv	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$21.94**	3	$65.82
Lunch / Déjeuners	**$40.58**	4	$162.32
Dinner / Dîners	**$51.40**	3	$154.20
Incidentals /Frais divers	**$36.45**	4	$145.80
			$528.14

New Dehli	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$14.40**	6	$86.40
Lunch / Déjeuners	**$40.20**	4	$160.80
Dinner / Dîners	**$51.10**	5	$255.50
Incidentals /Frais divers	**$33.82**	6	$202.92
			$705.62

Business Phone / Téléphone d'affaires	$50.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$20.00
Misc. Business Services / Diverses charges d'affaires	$100.00
Miscellaneous / Diverses - i.e. Conference Fees	$100.00
	$270.00

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande

☐ Amended (Same levels of approval oas orginal dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV): DZD9	Document No. - N° du document

Part A - Partie A

Type 2	Name of traveller - Nom du voyageur	Classification
	Robert (Bob) Gordon	EX-05

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	National Security
Address - Adresse	**Telephone No. - No. de téléphone**
269 Laurier Ave. West	613-949-7380
Branch Contact - Personne ressource à la direction	**Telephone No. - No. de téléphone**
Jane Hayward	613-991-1982

If different address, send cheque to: / Si adresse differente, envoyer chèque à

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)?	If no. would you like to request one? / Les cas échéant, aimerier-vous en avoir une?
To meet Senior officials in Tel Aviv and New Delhi to discuss Cyber and CT	10	☑ Yes / Oui ☐ No / Non	☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport: Mode	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
25/05/2012	Ottawa	Tel Aviv	1:00 - 11:40 next day	Air			
30/05/2012	Tel Aviv	New Delhi	16:30 - 9:10 nex day	Air			
03/06/2012	New Delhi	Ottawa	8:20 - 17:50	Air			

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$0.00	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$2,680.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dussus)	$0.00
Transportation Transport	$520.00		
Meals and incidentals Repas et frais accessoires	$1,207.80		
Other (Specify) - Autre (préciser)	$20.00		

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel

☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.)

☑ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)

Approval - Approbation

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$17,000.00
Other - Autre	$4,427.80
Trip Total - Coût total du voyage	$21,427.80

Funding - Financement

A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Robert Gordon

Signature — Date

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0				| 0	

Tyoe 4

Accounting Information / Renseignement comptables

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
			2001-PSABASE- 475 - 500094368	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requistion for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. / Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	Date

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$17,000.00
Train / Train	$0.00
Other / Autres	$0.00
	$17,000.00

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$0.00	0	$0.00
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	$335.00	8	$2,680.00
			$2,680.00
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.545	0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$60.00	$520.00
	Airport - Hotel / Meetings		$100.00	
	Hotel - Airport		$100.00	
	Airport to Home		$60.00	
	Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)		$10.00		$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$520.00

Canadian	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$15.60	1	$15.60
Lunch / Déjeuners	$14.85	1	$14.85
Dinner / Dîners	$40.85		$0.00
Incidentals /Frais divers	$17.30	1	$17.30
			$47.75

International	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$21.30	4	$85.20
Lunch / Déjeuners	$39.40	5	$197.00
Dinner / Dîners	$49.90	5	$249.50
Incidentals /Frais divers	$35.39	5	$176.95
			$708.65

International	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$12.82	3	$38.46
Lunch / Déjeuners	$35.91	3	$107.73
Dinner / Dîners	$45.58	3	$136.74
Incidentals /Frais divers	$30.18	4	$120.72
			$451.40

Business Phone / Téléphone d'affaires	$0.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$20.00
Misc. Business Services / Diverses charges d'affaires	$0.00
Miscellaneous / Diverses - Conference Fees	$0.00
	$20.00

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: JUIN JUN 0 1 2012

File No.: 387395
RDIMS No.: 572234

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

INTERNATIONAL TRAVEL AUTHORIZATION FOR WINDY ANDERSON AND LUC BEAUDOIN TO TRAVEL TO MALTA, JUNE 15-25, 2012

(Signature Required)

ISSUE

Your approval is sought for an international travel request for Mr. Luc Beaudoin, Chief, Cyber Operations and for Mrs. Windy Anderson, Director, Canadian Cyber Incident Response Centre (CCIRC) to attend the Forum of Incident Response and Security Teams (FIRST) conference and the Computer Security Incident Response Team (CSIRT) meeting in Malta, June 15-25, 2012.

BACKGROUND

CCIRC is a member of the FIRST community. Members comprise the vast majority of international interactions that CCIRC undertakes at the tactical and operational levels. FIRST conferences are designed to promote FIRST's organizational goals of worldwide coordination and cooperation.
It serves as the foundation for the improvement of computer security worldwide by sharing goals, ideas, and information. It provides a prime opportunity for those in the operating system, computer security and networking and telecommunications industries to gain focused access to a highly influential group of computer security incident response experts from around the world. The conference attendees commonly provide computer security advice within their own CSIRTs and suggest security strategies, provide technical solutions to security problems and deliver security education and training to their constituents.

CONSIDERATIONS

At the last Usual 5 (U5) conference (United States, United Kingdom, New Zealand, Australia and Canada), all international travel to upcoming events was discussed in detail. It was noted that all five countries are strongly encouraged to have representatives at both

.../2

the U5 conferences and the FIRST conference as these are the two most important venues for our forum. For all other conferences and trips, it was agreed that those countries participating would share their trip reports on the U5 Portal thus saving money and resources for those countries unable to participate.

Mrs. Anderson will be engaged in the CERT strategic and policy related discussions where appropriate representation would be beneficial in order to build trust relationships. As there are a number of sessions and parallel forums of relevance to CCIRC operations it would be very beneficial for M. Beaudoin, Operations Manager, to participate in technical sessions, as seen in the conference agenda **(TAB A).**

The estimated total cost of this trip is $26,260.66. This provides for a possible increase in airfare during the approval process. The trip is approved under the National Cyber Security Directorate Travel, Hospitality and Conference Plan.

RECOMMENDATION

It is recommended that you approve Mrs. Anderson's and Mr. Beaudoin's travel to Malta to attend the FIRST conference and CSIRTs meeting, June 15-25, 2012 by signing the Travel Authority and Advance forms (**TAB B**) and the Conference Request/ Training forms (**TAB C**). My approval is noted in the International Travel Request (**TAB D**).

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661. Mrs. Anderson can also be reached at 613-991-7705.

for Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (4)

I approve:

Graham Flack
Acting Deputy Minister

Prepared by: Windy Anderson

AGENDA ITEMS

LOCAL HOST

mita
MALTA INFORMATION TECHNOLOGY AGENCY

PLATINUM

Microsoft

GOLD

enisa
European Network and Information Security Agency

NETWORK

cisco

View Our Sponsors

QUESTIONS?

Do you have specific questions? Please send inquiries to first-2012@first.org.

Direct line to conference office: +1 312 646 1013

Direct mailing address to conference office:
FIRST Conference Office
219 W. Chicago Avenue, Suite 300
Chicago, Illinois 60654

CONFERENCE PROGRAM

Draft agenda as of 16 February 2012. Program is subject to change.

To view an abstract, please click on titles that have the [+] indication to expand. Speaker bios will be posted soon. A print version of the agenda will also be made available shortly.

SATURDAY, 16 JUNE 2012

TBD	**Education & Training Committee Meeting** TBD

SUNDAY, 17 JUNE 2012

TBD	**Education & Training Committee Meeting** TBD
1400-2100	**Registration** TBD
1500-1600	**2012 Session Chairs Meeting** Wignacourt - Level 6 Conference Center
1830-1900	**Newbie Reception w/ FIRST Steering Committee** Hilton Poolside Gazebo FIRST Newbies (non-members) & First Time Attendees (members and non-members) are cordially invited to mix and mingle with each other and the FIRST Steering Committee. Beverages and appetizers will be served.
1900-2100	**Ice Breaker Reception sponserd by MITA** Hilton Poolside Gazebo All attendees are encouraged to attend this kick-off event.

MONDAY, 18 JUNE 2012

0800-1600	**Registration & Morning Coffee/Tea Service** TBD **Breakfast at the Hilton Malta is included in the room rate for delegates staying at the hotel. If you are not staying at the Hilton Malta, please check with the hotel you are lodging with for details on breakfast. Breakfast is typically included in lodging at most European properties.*
0900-0945	***Conference Opening & Welcome*** Grandmaster Suite - Level 6 Conference Center **Chris Gibson** Chair, FIRST.Org SVP, Citi, UK
0945-1045	***Keynote Presentation*** Grandmaster Suite - Level 6 Conference Center **Francisco Garcia Morán** Director General, Directorate General Informatics (DIGIT), European Commission (EU)
1045-1115	**Coffee & Networking Break** TBD
1100-1200	***Plenary Session: MITA Introduction*** Grandmaster Suite - Level 6 Conference Center **TBD**
1200-1330	**Lunch** Spinola Suite - Level 5 Conference Center

BREAKOUTS	DEEP TECHNICAL DIVES	TECHNICAL FOUNDATIONS	POLICY & MANAGEMENT
	TBD	**TBD**	**TBD**
1330-1415	**Poison Ivy for Incident Responders [+]**	**Who, What, Where and How: An Insider's View to**	**Leaving our island: a communication and business strategy for a National CSIRT [+]**

	Nelson Uto CPqD, BR	**Marnix Dekker** ENISA, EU	**Andrea Rigoni** Global Cyber Security Center, IT
1600-1630	***Engineering National Cyber Drill Artifacts [+]*** **Mahmud Ab Rahman** CyberSecurity Malaysia (MyCERT), MY	**Engineering Solutions for Incident Investigations and Detection [+]** **Martin Nystrom** Cisco Systems, US	**Cross-Organizational Incident Handling: An evolved *process model for improved* collaboration [+]** **Thomas Millar** US-CERT, US
1630-1700	**Journey into Android Malware [+]** ***Simon Roses*** www.simonrose.com, ES	**National Disinfection Case Study [+]** ***Mounir Kamal*** QCERT, QA	**Sharing Crime Data Across International Frontiers [+]** **Patrick Cain** APWG, US
1800-2000	**Vendor Showcase** TBD An evening to network with our conference sponsors, exhibitors and your peers (with beer and appetizers of course!)		

WEDNESDAY, 20 JUNE 2012

0830-1600	**Registration & Morning Coffee/Tea Service with Exhibits** TBD		
0930-0945	***Opening Remarks*** Grandmaster Suite - Level 6 Conference Center **Chris Gibson** Chair, FIRST.Org SVP, Citi, UK		
0945-1045	***Keynote Presentation*** Grandmaster Suite - Level 6 Conference Center ***Suleyman Anil*** Head, Cyber Defense, NATO		
1045-1115	**Coffee & Networking Break with Exhibits** TBD		
1115-1200	***Plenary: Evolution of white-hat versus botnet takedown interaction [+]*** Grandmaster Suite - Level 6 Conference Center **Eric Ziegast** SIE Progamme Manager, Internet Systems Consortium, US		
1200-1330	**Lunch** Spinola Suite - Level 5 Conference Center		
BREAKOUTS	**DEEP TECHNICAL DIVES** TBD	**TECHNICAL FOUNDATIONS** TBD	**POLICY & MANAGEMENT** TBD
1330-1415	***The rise of the Machines:* Targeted attacks and information warfare after Stuxnet [+]** **Peter Szor** McAfee, US	**NorCERT incident handling of targeted attacks [+]** **Marie Moe** **Eldar Lillevik** NorCERT, NO	**Legal challenges to information sharing of *national/governmental* CERTs in Europe [+]** **Silvia Portesi** ENISA, EU
1415-1500	**Cyber Crime & APT Hands On [+]** ***Jeffrey Brown*** **Cory Mazzola** US-CERT, US	**Post-Intrusion Problems: Pivot, Persist and Property [+]** **Cory Altheide** **Morgan Marquis-Boire** Google, US	**The Laws of Large Numbers and The Impact on IT Security [+]** **Peter Kuper** *In-Q-Tel*, US
1500-1530	**Coffee & Networking Break with Exhibits** TBD		
1530-1700	**Lightning Talks** Grandmaster Suite - Level 6 Conference Center Sign-up sheets will be available at the registration desk. 5-minute rotations. **No sales presentations.**		
1900-2400	**Conference Banquet** Location & event details TBD		

THURSDAY, 21 JUNE 2012

0830-1530	**Registration & Morning Coffee/Tea Service with Exhibits** TBD
0930-0945	***Opening Remarks*** Grandmaster Suite - Level 6 Conference Center **Chris Gibson** Chair, FIRST.Org SVP, Citi, UK
0945-1045	**Plenary: Securing Social [+]** Grandmaster Suite - Level 6 Conference Center **Chad Greene** CERT Manager, Facebook, US
1045-1115	**Coffee & Networking Break with Exhibits** Park Congress Prefunction, Ground Floor
1115-1200	**Plenary: Proactive Detection of Network Security Incidents - A Study [+]** Grandmaster Suite - Level 6 Conference Center

Chris Gibson
Chair, FIRST.Org
SVP, Citi, UK

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval oas orginal dated)
Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV)	Document No. - N° du document
Type 2	Name of traveller - Nom du voyageur: **Windy Anderson**	Classification: **EX-01**

Part A - Partie A

Department - Ministère: **Public Safety**	Branch / Division / Group - Direction / Division / Groupe: **NS - NCSD/ CCIRC**
Address - Adresse: **257 Slater Avenue**	Telephone No. - No. de téléphone: **613-991-7055**
Branch Contact - Personne ressource à la direction: **Jane Hayward**	Telephone No. - No. de téléphone: **613-991-1982**
Purpose of travel - Objet du voyage: **To attend FIRST Conference and CSIRT Meeting**	No. of days / Nbre de jours

If different address, send cheque to: / Si adresse differente, envoyer chèque à

Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)? ☑ Yes / Oui ☐ No / Non

If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une? ☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport Mode	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
June 15, 2012	Ottawa	Malta	13:00 - 11:55 (next day)	Air - Economy	1	Hilton Malta	
June 25, 2012	Malta	Ottawa	12:50 - 22:09	Air - Economy	1		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	~~$2,178.45~~	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$2178.45 ~~$0.00~~
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☑ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$54.50	Other (Specify) - Autre (préciser)	
		Upgrade transportation (specify in "Class" above) *Transport à tarif supèrieur (préciser la <classe> si-dussus)*	$0.00
Transportation Transport	$350.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) ☐ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (*approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9*)	
Meals and incidentals Repas et frais accessoires	$1,045.60		
Other (Specify) - Autre (préciser) Baggage, internet	$225.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel.

Best rate available at the present time

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$7,126.78
Other - Autre	$3,853.55
Trip Total - Coût total du voyage	$10,980.33
Funding - Financement	
A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques *interne pour les employeurs distincts) et en accepte les conditions.*

Windy Anderson — Signature: W Anderson — Date: May 4/12

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date
Lynda Clairmont			

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0				| 0	

Accounting Information / Renseignement comptables

Tyoe 4

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
			223-2007-PSABSAE - 500095662 June 14 2	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature)	*Requistion for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations.* *Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.*	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) Vérifié conform (TPSGC) (signature)		
Services officer (PWGSC) (signature) Agent responsible (TPSGC) (signature)	Signature	Date

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé				Amount/Montant
Airfare / Frais d'avion				**$7,126.78**
Train / Train				**$0.00**
Other / Autres				**$0.00**
				$7,126.78

Estimated Cost - Coût estimatif: Other - Autre		Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)		**$242.05**	**9**	$2,178.45
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)		**$0.00**	**0**	$0.00
				$2,178.45
Mid-size car rental / Location d'une voiture intermédiaire		**$0.00**	**0**	$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire		**$0.00**	**0**	$0.00
Gasoline for Rentals / Essence pour voiture louée				$0.00
				$0.00
		Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé		**0.545**	**100**	$54.50
		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			**$0.00**	$0.00
Taxi/Limo	Home to Airport (Train Station)		**$0.00**	$350.00
	Airport (Train Station) - Hotel / Meetings		**$75.00**	
	Hotel - Airport (Train Station)		**$75.00**	
	Airport (Train Station) to Home		**$0.00**	
	Meeting - Meetings		**$200.00**	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$350.00
		Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners		**$22.41**	**9**	$201.69
Lunch / Déjeuners		**$30.79**	**4**	$123.16
Dinner / Dîners		**$42.61**	**9**	$383.49
Incidentals /Frais divers		**$30.66**	**11**	$337.26
				$1,045.60
Business Phone / Téléphone d'affaires				**$50.00**
Airport Improvement Fee / Frais de l'Aeropart				**$0.00**
Cash Advance Fee / Frais d'avances				**$0.00**
Misc. Business Services / Diverses charges d'affaires				**$100.00**
Miscellaneous / Diverses				**$75.00**
				$225.00

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions**
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☒ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☐ Other Specify: [redacted]

☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?
N/A	Have I completed all the paperwork requested by the Contracting Material Management group? ☒ Is the Sole Source Checklist complete and attached? ☐ Is the Competitive Contract Checklist complete and attached?
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
N/A	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☒ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☒ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☑ Original / Prem. demande
☐ Amended (Same levels of approval oas orginal dated)
Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) N°. d'aut de voyager (NAV)	Document No. - N° du document

Part A - Partie A

Type 2	Name of traveller - Nom du voyageur	Classification
	Luc Beaudoin	CS-04

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety	NS - NCSD/ CCIRC
Address - Adresse: 257 Slater Avenue	Telephone No. - No. de téléphone: 613-991-9949
Branch Contact - Personne ressource à la direction: Jane Hayward	Telephone No. - No. de téléphone: 613-991-1982

If different address, send cheque to: / Si adresse differente, envoyer chèque à

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Gov't Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CVP)?	If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une?
To attend FIRST Conference Meeting		☑ Yes / Oui ☐ No / Non	☐ Yes / Oui ☐ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation / Transport: Mode	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de repérage du dossier
June 15, 2012	Ottawa	Malta	13:00 - 11:55 (next day)	Air - Economy	1	Hilton Malta	
June 25, 2012	Malta	Ottawa	12:50 - 22:09	Air - Economy	1		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	~~$2,178.45~~	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	~~$2178.45~~ $0.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du répertoire oblig.)	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☑ Traveller / Voyageur ☐ Employer / Employeur. Public Liability and Property Damage min $1 million. Deductibles NON reimbursable. Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$54.50	Other (Specify) - Autre (préciser)	
Transportation / Transport	$350.00	Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dussus)	$0.00
Meals and incidentals / Repas et frais accessoires	$1,045.60	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.)	
Other (Specify) - Autre (préciser) Baggage, internet, business phone	$225.00	☐ Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
		Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel.
Best rate available at the present time.

Part D - Partie D

Estimated Cost - Coût estimatif	
Prepaid - Prépayé	$7,126.78
Other - Autre	$3,853.55
Trip Total - Coût total du voyage	$10,980.33

Funding - Financement

A) Travellers cheques / Chèques de voyage	
Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00
B) Other advance / Autre avance	
Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Luc Beaudoin — Signature — 8 May 12 — Date

Ticket pick-up date and location / Date et lieu de la collecte des billets

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signature)	Date
Lynda Clairmont		Graham Flack	

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type 8 0	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur 0	Due Date / Date d'échéance

Accounting Information / Renseignement comptables

Tyoe 4

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
			223-PSABASE - 2001 - 500096267 June 14	2

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requistion for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. Demandé pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de paiements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	Date

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$7,126.78
Train / Train	$0.00
Other / Autres	$0.00
	$7,126.78

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du répertoire)	$242.05	9	$2,178.45
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertoire)	$0.00	0	$0.00
			$2,178.45
Mid-size car rental / Location d'une voiture intermédiaire	$0.00	0	$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.545	100	$54.50

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport (Train Station)		$0.00	$350.00
	Airport (Train Station) - Hotel / Meetings		$75.00	
	Hotel - Airport (Train Station)		$75.00	
	Airport (Train Station) to Home		$0.00	
	Meeting - Meetings		$200.00	
Transportation / Transportation (No receipt)				$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$350.00

	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	$22.41	9	$201.69
Lunch / Déjeuners	$30.79	4	$123.16
Dinner / Diners	$42.61	9	$383.49
Incidentals /Frais divers	$30.66	11	$337.26
			$1,045.60

Business Phone / Téléphone d'affaires	$50.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$100.00
Miscellaneous / Diverses	$75.00
	$225.00

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions**
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☐ Request to Attend Conferences Form	☒ Training Application and Authorization Form	☐ Membership Approval Form	☐ Other Specify: [redacted]

☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?
N/A	Have I completed all the paperwork requested by the Contracting Material Management group? ☒ Is the Sole Source Checklist complete and attached? ☒ Is the Competitive Contract Checklist complete and attached?
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
N/A	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☒ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☒ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

Public Safety Canada / Sécurité publique Canada

REQUEST TO ATTEND A CONFERENCE
DEMANDE DE PARTICIPATION À UNE CONFÉRENCE

Date: May 4, 2012

To – A	Requested by – Demandé par
Acting Deputy Minister Graham Flack	Windy Anderson Director CCIRC National Cyber Security Directorate

Name of Conference – Titre de la conférence

24th Annual FIRST Conference and CSIRT

Type of Conference – Genre de conférence	Documents attached / Documentation jointe
☒ International / Internationale ☐ National / Nationale ☐	☒ Yes / Oui ☐ No / Non

Sponsor - Promoteur	Official Host – Hôte officiel
Microsoft, Cisco, European Network and Info Security Agency	FIRST - Forum of Incident Response and Security Teams

Duration of Conference – Durée de la conférence	Location - Adresse
From / Du June 17, 2012 To / À June 24, 2012	Malta

Agenda – Ordre du jour

Attached

Purpose of Participation - Object de la participation

The 24th Annual FIRST Conference seeks to bridge a gap by focusing on the practical aspects of security and incident response in the face of a rush toward the adoption of cloud computing and other distributed architectures. Considering the inroads that mobile devices are making in our daily workplaces, perhaps it is time for security to redefine itself in some fundamental ways.

The Forum of Incident Response and Security Teams (FIRST) is a global non-profit organization dedicated to bringing together computer security incident response teams (CSIRTs) and includes response teams from over 240 corporations, government bodies, universities and other institutions spread across the Americas, Asia, Europe and Oceania. The annual FIRST conference provides a setting for conference participants to attend a wide range of presentations delivered by leading experts in both the CSIRT field and from the global security community. The conference also creates opportunities for networking, collaboration, and sharing technical information and management practices. The conference enables attendees to meet their peers and build confidential relationships across corporate disciplines and geographical boundaries.
The cost of the both conferences is USD $2150.00.

Financial Coding – Code financier	Estimated Total Cost / Coût total prévu
233-4083-PSABASE-500095662 Line 3	$ 13,130.33

Recommended by – Recommandé par	Branch Approval – Approbation de la direction
Signature / Date	Signature / Date
Assistant Deputy Minister – Sous-ministre adjoint	**Deputy Minister – Sous-ministre**
Signature / Date	Signature / Date

MS-18 (4/04)

LOCAL HOST

mita
MALTA INFORMATION TECHNOLOGY AGENCY

PLATINUM

Microsoft

citi 200 YEARS

GOLD

enisa
European Network and Information Security Agency

Secunia
Stay Secure

NETWORK

cisco

INTERNET

CONFERENCE PROGRAM

Draft agenda as of 13 April 2012. Program is subject to change.

To view an abstract, please click on titles that have the [+] indication to expand. Speaker bios will be posted soon.

Print Version Available!

SATURDAY, 16 JUNE 2012

0900-1630	**Education & Training Committee Meeting** Perrellos - Level 5 Conference Center

SUNDAY, 17 JUNE 2012

0900-1330	**Education & Training Committee Meeting** Perrellos - Level 5 Conference Center
1400-1630	**Becoming a Better Trainer** Perrellos - Level 5 Conference Center
1400-2100	**Registration** Main Lobby - Level 5 Conference Center
1500-1600	**2012 Session Chairs Meeting** Wignacourt - Level 6 Conference Center
1830-1900	**Newbie Reception w/ FIRST Steering Committee** Hilton Poolside Gazebo FIRST Newbies (non-members) & First Time Attendees (members and non-members) are cordially invited to mix and mingle with each other and the FIRST Steering Committee. Beverages and appetizers will be served.
1900-2100	**Ice Breaker Reception sponserd by MITA** Hilton Poolside Gazebo All attendees are encouraged to attend this kick-off networking event.

MONDAY, 18 JUNE 2012

0800-1600	**Registration & Morning Coffee/Tea Service** Main Lobby - Level 5 Conference Center **Breakfast at the Hilton Malta is included in the room rate for delegates staying at the hotel. If you are not staying at the Hilton Malta, please check with the hotel you are lodging with for details on breakfast. Breakfast is typically included in lodging at most European properties.*
0915-0945	***Conference Opening & Welcome*** Grandmaster Suite - Level 6 Conference Center **Chris Gibson** Chair, FIRST.Org SVP, Citi, UK
0945-1045	**Keynote Presentation: IT Security @ EC: Challenges & Experiences [+]** Grandmaster Suite - Level 6 Conference Center **Francisco Garcia Morán** Director General, Directorate General Informatics (DIGIT), European Commission (EU)
1045-1115	**Coffee & Networking Break** Main Lobby - Level 5 Conference Center Grandmaster Foyer - Level 6 Conference Center
1115-1200	**Plenary: Remediation of Malware at the Country Level: A Case Study [+]** Grandmaster Suite - Level 6 Conference Center **Jeff Williams** Principal Group Program Manager, Microsoft Corporation, US
1200-1330	**Lunch** Spinola Suite - Level 5 Conference Center
BREAKOUTS	

	Gavin Reid David Schwartzburg Cisco Systems, US	**Ramses Martinez** **Ismail Guneydas** Yahoo!, US	**Rod Rasmussen** Internet Identity, US
1520-1550	**Coffee & Networking Break** Main Lobby - Level 5 Conference Center Grandmaster Foyer - Level 6 Conference Center		
1555-1625	**Cryptanalysis of malware encrypted output files [+]** **Nelson Uto** CPqD, BR	**Operation black tulip: Certificate authorities loose authority [+]** **Marnix Dekker** ENISA, EU	**CSIRTs are to Product Security as Ferries are to Islands [+]** **Erka Koivunen** CERT-FI, FI **Anu Puhakainen** Ericsson, FI
1630-1700	**Engineering National Cyber Drill Artifacts [+]** **Mahmud Ab Rahman** CyberSecurity Malaysia (MyCERT), MY	**Engineering Solutions for Incident Investigations and Detection [+]** **Martin Nystrom** Cisco Systems, US	**Cross-Organizational Incident Handling: An evolved process model for improved collaboration [+]** **Thomas Millar** US-CERT, US
1705-1735	**Privacy breaches: Whipped cream won't go back in the can [+]** **Scott McIntyre** Telstra, AU	**National Disinfection Case Study [+]** **Mounir Kamal** QCERT, QA	**Sharing Crime Data Across International Frontiers [+]** **Patrick Cain** APWG, US
1800-2000	**Vendor Showcase** Main Lobby - Level 5 Conference Center Grandmaster Foyer - Level 6 Conference Center An evening to network with our conference sponsors, exhibitors and your peers (with beer and appetizers of course!)		

WEDNESDAY, 20 JUNE 2012

0830-1600	**Registration & Morning Coffee/Tea Service with Exhibits** Main Lobby - Level 5 Conference Center		
0930-0945	***Opening Remarks*** Grandmaster Suite - Level 6 Conference Center **Chris Gibson** Chair, FIRST.Org SVP, Citi, UK		
0945-1045	**Keynote: Defending Cyberspace—Global Challenges Require Global Responses [+]** Grandmaster Suite - Level 6 Conference Center **Suleyman Anil** Head, Cyber Defence/Emerging Security Challenges Division, NATO		
1045-1115	**Coffee & Networking Break with Exhibits** Main Lobby - Level 5 Conference Center Grandmaster Foyer - Level 6 Conference Center		
1115-1200	**Plenary: Evolution of white-hat versus botnet takedown interaction [+]** Grandmaster Suite - Level 6 Conference Center **David Dagon** Georgia Tech Information Security Center, US **Eric Ziegast** SIE Progamme Manager, Internet Systems Consortium, US		
1200-1330	**Lunch** Spinola Suite - Level 5 Conference Center		
BREAKOUTS	**DEEP TECHNICAL DIVES** Portomaso I+II Hilton Level 3	**TECHNICAL FOUNDATIONS** Grandmaster Suite Level 6 CC	**POLICY & MANAGEMENT** Portomaso III Hilton Level 3
1335-1420	**The ghost in the Machines: Targeted attacks and information warfare after Stuxnet [+]** **Peter Szor** McAfee, US	**NorCERT incident handling of targeted attacks [+]** **Marie Moe** **Eldar Lillevik** NorCERT, NO	**Legal challenges to information sharing of national/governmental CERTs in Europe [+]** **Silvia Portesi** ENISA, EU
1425-1510	**Cyber Crime & APT Hands On [+]** **Jeffrey Brown** Cyber Clarity, US **Cory Mazzola** US-CERT, US	**Post-Intrusion Problems: Pivot, Persist and Property [+]** **Cory Altheide** **Morgan Marquis-Boire** Google, US	**The Laws of Large Numbers and The Impact on IT Security [+]** **Peter Kuper** In-Q-Tel, US
1515-1545	**Coffee & Networking Break with Exhibits** Main Lobby - Level 5 Conference Center Grandmaster Foyer - Level 6 Conference Center		
1550-1720	**Lightning Talks** Grandmaster Suite - Level 6 Conference Center Sign-up sheets will be available at the registration desk. 5-minute rotations. **No sales presentations.**		
1815-1830	**Buses to Conference Banquet in Mdina** Additional attendee directions TBD		
1900-2400	**Conference Reception & Banquet Dinner in Mdina** Location & event details TBD		

THURSDAY, 21 JUNE 2012

	Jussi Eronen CERT-FI, FI		
1425-1510	**Sharing data's hard, here's how we did it [+]** **Wes Young** REN-ISAC, US	**FS-ISAC—A Private/Public Partnership [+]** **Kevin Thomsen** Citi, US	**How Visualization Makes it Possible [+]** **Sebastian Tricaud** Picviz Labs, FR
1515-1545	**Coffee & Networking Break with Exhibits** Main Lobby - Level 5 Conference Center Grandmaster Foyer - Level 6 Conference Center		
1550-1630	**Proposal for a new model for information sharing between CSIRTs [+]** **David Durvaux** **Christian Van Heurck** CERT.be, BE	**TBA** **TBA**	**SCADA Security: The fight to protect critical infrastructure [+]** **Kevin Hemsley** ICS-CERT, US
1635-1700	***Closing Remarks*** Grandmaster Suite - Level 6 Conference Center **Chris Gibson** Chair, FIRST.Org SVP, Citi, UK		

Response Team Support

National CSIRTs

CSIRT Development

Investigation

Forensics

Publications Catalog

Historical Documents

Authorized Users of "CERT"

CERT Coordination Center

2012 Annual Technical Meeting for CSIRTs with National Responsibility

Social Events

To provide an opportunity for attendees to interact informally, we have scheduled two social events. When registering for the annual meeting, remember to indicate whether you will be attending the events.

Meet and Greet Pre-Event Reception

A "Meet and Greet" pre-event reception will be held prior to the National CSIRT meeting and gives meeting attendees an opportunity to meet and to talk in a relaxed social setting.

Date: Monday, June 18
Time: 18:00-20:00
Location: Hilton Malta, Aqua Bar
Cost: No charge to registered attendees

Saturday Social Dinner

The Saturday evening social dinner is a tradition at the National CSIRT meeting.

Date: Saturday, June 23
Time: 19:00-22:00
Location: Sale e Pepe
Cost: $60 USD

Event Information

National CSIRT Meeting

- Accommodations
- Call for Papers (HTML | PDF)
- Social Events

External Sponsorship
The 2012 Annual Technical Meeting for CSIRTs with National Responsibility is sponsored in part by

Homeland Security

Last updated February 13, 2011

2012 Annual Technical Meeting for CSIRTs with National Responsibility Invitation

The CERT(R) Coordination Center invites you and your team to participate in the 2012 Annual Technical Meeting of CSIRTs with National Responsibility. This meeting provides a forum for National CSIRTs to share information, tools, techniques, and strategies that address problems unique to CSIRTs. The meeting will be held at the Hilton Malta in St. Julian's, Malta **on June 23-24, 2012**; following the 24th annual FIRST conference.[1] This meeting is restricted to staff members of authenticated national CSIRTs only.[2]

Beneficial to both new and established National CSIRTs, the meeting provides a forum for networking and collaboration. Discussions are participant-driven and often focus on current issues, tools, and methods relevant to the National CSIRT community. We will also be allocating some of the sessions for CSIRTs to give presentations on their collaborative work or research. If your team is involved in a collaborative or unique project that would be of interest to other National CSIRTs, we encourage you to consider presenting. This year our internal program committee has selected the theme "Automated Analytics" and we are encouraging presentations that focus on this topic as it applies to incident analysis, malware analysis, network flow analysis and vulnerability analysis.

There is a $300.00 USD registration fee associated with the meeting that includes lunch on both meeting days and the Meet and Greet Pre-Event Reception on Monday, June 18, 2012. Also, please plan on attending the Saturday Social dinner. The cost for the dinner is $60.00 USD and is due at the time of registration.

Due to space considerations we request that attendance be limited to two people per team. If you are from a team that needs a Visa to travel to Malta please let us know as soon as possible so that we can provide a formal invitation. Visa information for travel to Malta is available at http://www.mfa.gov.mt/Default.aspx?MDIS=530

To register for this year's meeting visit https://events.capsllc.net/certcc/welcome.

Please email any questions to cert@cert.org with INFO#653656 in the subject line. I look forward to seeing you in Malta!

Best regards,

Pat

Patrick Dempsey
Technical Manager
CERT(R) Coordination Center
Phone +1 412.268.7090
Email cert@cert.org
Twitter http://www.twitter.com/National_CSIRT

---

1 Although this meeting is usually held after the annual FIRST conference, it is not sponsored by or affiliated with the FIRST conference or the FIRST organization.

2 A "CSIRT with national responsibility" (or "national CSIRT") is a CSIRT that has been designated by a country or economy to have specific responsibilities in cyber protection for the country or economy. A national CSIRT can be inside or outside of government, but it must be specifically recognized by the government as having responsibility in the country or economy.

Response Team Support

National CSIRTs

CSIRT Development

Investigation

Forensics

Publications Catalog

Historical Documents

Authorized Users of "CERT"

CERT Coordination Center

Annual Technical Meeting for CSIRTs with National Responsibility

Since 2006, the CERT Coordination Center has been hosting an annual meeting for CSIRTs with national responsibility immediately following the FIRST conference. This meeting provides an opportunity for organizations responsible for protecting the security of nations, economies, and critical infrastructures to meet and discuss the unique challenges of their roles.

Beneficial to both new and established National CSIRTs, the meeting provides a forum for networking and collaboration. Discussions are participant-driven and often focus on current issues, tools, and methods relevant to the National CSIRT community. We will also be allocating some of the sessions for CSIRTs to give presentations on their collaborative work or research. If your team is involved in a collaborative or unique project that would be of interest to other National CSIRTs, we encourage you to consider presenting.

2012 Annual Meeting — Registration is Open

Dates: Saturday, June 23, 2012 – Sunday, June 24, 2012
Location: Portomaso St. Julilan's, Malta
Registration Fee: $300 USD

To ensure trust and open discussion, this invitation-only meeting is restricted to representatives from National CSIRTs. Invitations have been sent and registration is now available for the 2012 Annual Technical Meeting for CSIRTS with National Responsibility. The link to register for the meeting will be included in the meeting invitation. Contact us if your organization has not received an invitation and you believe that you are eligible to attend.

Additional meeting information is available in the *Event Information* section of this page.

Last updated March 20, 2012

Event Information

National CSIRT Meeting

- Accommodations
- Call for Papers (HTML | PDF)
- Social Events

External Sponsorship
The 2012 Annual Technical Meeting for CSIRTs with National Responsibility is sponsored in part by

Homeland Security

Government of Canada / Gouvernement du Canada

PROTECTED WHEN COMPLETED (for privacy Act Statement see page 2)
PROTÉGÉ UNE FOIS REMPLI (pour l'énoncé de la Loi sur la protection des renseignements personnels, voir la page 2)

TRAINING APPLICATION AND AUTHORIZATION
DEMANDE ET AUTORISATION DE FORMATION

For PSC USE ONLY RÉSERVÉ À la CFP		

s.19(1)

* REFER TO INSTRUCTIONS ON PAGE 2
VOIR LES INSTRUCTIONS SUR LA PAGE 2

DEPARTMENT USE ONLY RÉSERVÉ AU MINISTÈRE	2. Special needs * (enter indicator) Besoins spéciaux * (inscrire l'indicateur)
1. File number – Numéro de dossier	

☒ Original / Première ☐ Amendment / Modification ☐ Cancellation / Annulation

APPLICANT INFORMATION – RENSEIGNEMENTS SUR LE CANDIDAT

3. Family name – Nom de famille	Given name and initials – Prénom et initiales
Beaudoin	Luc

4. PRI – CIDP	5. Sex – Sexe	6. Classification Gr.	S.-gr.	Lev./Niv.	7. First official language – Première langue officielle
[redacted]	☒ Male / Homme ☐ Female / Femme	CS		04	☐ (1) English / Anglais ☒ (2) French / Français

8. Position title – Titre du poste		
Chief of Cyber Operations, CCIRC		
9. Employee's office telephone number / N° de téléphone de l'employé au bureau: 991-9949	Facsimile – Télécopieur	E-Mail – Courrier électronique: Luc.beaudoin@ps-sp.gc.ca

10. Department name – Nom du ministère	11. Dept. Code – Code min.	12. Branch/Division – Direction/Division
Public Safety	088	NS/NCSD

13. Office, Workstation, mailing address – Adresse postale, bureau, poste de travail	City/Postal code – Ville/Code postal
257 Slater Street, 2nd Floor	Ottawa, K1A 0M6
14. Supervisor's name and title – Nom du surveillant et titre	Telephone No. – N° de téléphone
Windy Anderson	613-991-7055
15. Supervisor's Office, Workstation, mailing address – Adresse postale, bureau, poste de travail du superviseur	City/Postal code – Ville/Code postal
257 Slater Street, 4th Floor	Ottawa, K1A 0M6

16. Objective of training * - Objective de la formation *

Gain understanding of operations of national CERT teams and their international relationships. Improve understanding of technical tools, processes and best practices used in national CERT operations.

W Anderson	8 May 12	[signature]	8 May 12
Supervisor's – Signature – Surveillant	Date	Employee's – Signature – Employé(e)	Date

TRAINING INFORMATION – RENSEIGNEMENTS SUR LA FORMATION

17. Course code * / Code du cours *	18. Course title – Titre du cours
	FIRST Conference

19. Location of training * - Lieu de formation *	20. Date of course - Date du cours From – Du Y-A	M	D-J	To - Au Y-A	M	D-J	21. Departmental training program code * / Code min. du programme de formation *
Malta							002

22. Time of training - Période retenue pour la formation	23. Duration of training * (nearest half-day) Durée de la formation * (plus proche demi-journée)	24. Language of course - Langue de cours
☐ (1) Outside working hours / En dehors des heures de travail ☒ (2) During working hours / Pendant les heures de travail	5	☒ English / Anglais ☐ French / Français ☐ Bilingual / Bilingue ☐ Other / Autre

25. Source of training - Source de la formation	26. Transit time (person-days) * Durée des déplacements (journées-personnes)	27. Province	28. Location* Lieu *
☐ (1) TPB/PSC DGPF/CFP ☐ (2) Dept'l Min. ☐ (3) Interdept'l Intermin. ☐ (4) University/College Université/Collège ☒ (5) Other Autre	2	OT	

29. FINANCIAL AUTHORIZATION – AUTORISATION FINANCIÈRE

Cost / Coût	Financial code (include R.C. codes only if several R.C.'s are sharing the costs, otherwise complete box 30) Code financier (indiquer des codes de C.R. uniquement si plusieurs C.R. se partagent les coûts, sinon remplir la case 30)	Estimated cost (planning purposes) Coût estimatif (à des fins de planification)	Actual cost (reporting purposes) Coût réel (à des fins de compte rendu)
Tuition fee / Reimbursement * / Frais de scolarité / Remboursement * ☐ 0% ☐ 50% ☒ 100%	500096267 Line 3	$2150.00	a) *
Travel / Living / Déplacement / Subsistance	500096267 Line 1 and 2	$10,980.33	b)
Other * / Autres *			c) *
30. Responsibility centre (collator) code / Code du centre de responsabilité (destinataire): 223	TOTAL	$13,130.00	d)

Recipient organization code / Code d'organization du/de la récipiendaire: 0880	Récipient référence code / Code de référence du/de la récipiendaire

31. Financial signing authority (Certified that funds are available pursuant to section 32(1)FAA) * / Signataire autorisé en matière financière (Attestation de la disponibilité des fonds aux termes du par. 32(1) LGFP) *	Date	32. This candidate meets course selection criteria (Manager's approval) / Le candidat satisfait aux critères de sélection du cours (approbation du gestionnaire)	Date

33. DEPARTMENTAL TRAINING COORDINATOR* - COORDONNATEUR DE LA FORMATION DU MINISTÈRE *

Remarks - Observations

Signature Date

34. DEPARTMENTAL USE CODES * - CODES À L'USAGE DU MINISTÈRE *

A	B	C	
D	E	F	R S T U V W X Y Z

GC 211 (2001-12) (Word version R-02-01)

DISTRIBUTION
Original = PSC/Finance Division/Human Resources Division Copy = Origin

LOCAL HOST

mita
MALTA INFORMATION TECHNOLOGY AGENCY

PLATINUM

Microsoft

citi
200
YEARS

GOLD

enisa
European Network and Information Security Agency

Secunia
Stay Secure

NETWORK

cisco

INTERNET

CONFERENCE FEES

Early Bird - Non-Member (by 18:00 GMT, 1 April 2012)	$1900 US
Early Bird - Member (by 18:00 GMT, 1 April 2012)	$1500 US
Standard - Non-Member (after 18:00 GMT, 1 April 2012)	$2300 US
Standard - Member (after 18:00 GMT, 1 April 2012)	$1850 US
Single Day Fee	$800 US
Full Time Graduate or Doctoral Computer Security Student	$900 US
60-Minute Paper Presenter (1 comp per presentation)	Complimentary
Late Fee Member & Non-Member (after 18:00 GMT, 1 June 2012)	$2500 US

Please ensure you read the **Registration Terms & Conditions**.

The Early fee US$1900 (US$1500 for members) will be available up until 18:00 GMT on 1 April 2012.
If payment has not been received and confirmed by the Registration Office by 18:00 GMT 1 April 2012, registrants will be charged the Standard conference fee (US$2299). This applies to registrants submitting *bank/wire transfers, checks, and credit card* payments that are incomplete for any reason.

The Standard conference fee US$2299 (US$1899 for members) will be available up until 18:00 GMT on 1 June 2012.
If payment has not been received by 18:00 GMT 1 June 2012, *all non-payment* standard registrations will be automatically removed from the registrant database.

Registrations entered after 18:00 GMT 1 June 2012 will be considered Late registrations.
The Late registration fee for members and non-members is US$2499.

The Student conference fee US$900 will be available through the start of the Conference.
In order to register as a Student, you must email or fax a copy of your student ID and a letter signed by your academic advisor indicating your doctoral or graduate course of study. Email to **first-2012@first.org** or fax to the conference office at +1 312 372 1427. Upon approval by FIRST, you will receive a special registration discount code â€" email any questions about this process or the status of your request to **first-2012@first.org**.

If you are an invited speaker or accepted presenter, you will be contacted by the conference staff and the appropriate discount code will be sent to you.

Accommodation costs are not included in the conference registration.

Payment must be made in USD.

register today!
#FIRST2012

WHAT DOES THE FULL FEE INCLUDE?

- Attendance to all conference sessions (except closed meetings for which you must be qualified/authorized to attend)
- Morning & afternoon breaks and lunches Monday-Friday of conference week
- One ticket to the Welcome Reception and one ticket to the Conference Banquet
- Access to the Tuesday evening Vendor Showcase
- All conference materials

WHAT DOES THE SINGLE DAY FEE INCLUDE?

- Attendance to all conference sessions **the single day** of attendance *(except closed meetings for which you must be qualified/authorized to attend)*
- Morning & afternoon breaks and lunches during conference hours
- One ticket to the Conference Banquet (if applicable)
- Access to the Tuesday Vendor Showcase *(if applicable)*
- All conference materials

Public Safety Canada / Sécurité publique Canada

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
	From - *Du* :	To - *Au* :
FIRST Conference, 24th Annual and Computer Security Incident Response Team (CSIRT) Meeting	June 17, 2012	June 24, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
Malta (part of Europe)	$26,260.66	

Description of meeting (provide agenda)
Description de l'événement (joindre l'ordre du jour)

FIRST is the world's largest organization of recognized Computer Security Incident Response Teams (CSIRTs). FIRST conferences are designed to promote the organization's goals of worldwide coordination and cooperation. It serves as the foundation for the improvement of computer security worldwide by sharing goals, ideas, and information. FIRST members, numbering over 250, include national and government CSIRTs, product vendor CSIRTS (e.g. Adobe and Cisco), and Critical Infrastructure CSIRTs (e.g. financial institutions and telcos). Conference attendees commonly provide computer security advice within their own CSIRTs and suggest security strategies, provide technical solutions to security problems, and deliver security education and training to their constituents.

Pre-approved under Branch travel plans?
Pré-approuvé selon les directives sur les voyages de la direction générale?

☒ Yes/Oui ☐ No/Non

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Windy Anderson	NS/NCSD - CCIRC	257 Slater Street	613-991-7055
Luc Beaudoin		4th Floor	613-991-9949

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

Members comprise the vast majority of international interactions CCIRC undertakes at the tactical and operational levels. Attendance, by CCIRC personnel, is essential in ensuring CCIRC is aware of and has its views heard with respect to information sharing protocols, special capabilities possessed by other CSIRTs and problems, trends and best practices. CCIRC involvement in these conferences is essential in ensuring CCIRC fulfills its mandate as Canada's National CSIRT.

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

Having a representative from Canada at this event will increase Public Safety's ability to collaborate internationally with its peer organisations to address cyber security emerging threats to Canada. This training and networking opportunity is of significant importance to build CCIRC trusted relationships with other national Cyber Emergency Response Teams (CERT), which is essential to enable effects in mitigating cyber security incidents. There will be many discussions on how other CERTs operate in other countries; this will allow the Director of CCIRC to come away from the conference with best practices that can be implemented within CCIRC. This will ultimately lead to a more effective and efficient team. Since we are concentrating on a U.S.-Canada Cyber Action Plan this year, it will also be an opportunity to meet with the United States representatives to discuss what we hear at the conference and ensure both countries are aligned with their future direction.

For M. Beaudoin, it will be an opportunity to meet and exchange ideas with highly skilled technical experts from many countries in the field of cyber security. There are two full tracks of technical information that will be passed on and discussed with the participants. M. Beaudoin is only attending the FIRST conference

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

Possibly someone from CSEC, U5 Partners are all participating

Prior Consultation within and outside Department

Public Safety Canada | Sécurité publique Canada
Senior Assistant Deputy Minister | Sous-ministre adjoint principal
Ottawa, Canada K1A 0P8

UNCLASSIFIED

DATE: MAY 15 2012

File No.: 387469
RDIMS No: 614390

MEMORANDUM FOR THE ACTING DEPUTY MINISTER
Via: Gary Robertson, Assistant Deputy Minister, Corporate Management Branch

INTERNATIONAL TRAVEL REQUEST: COREY DVORKIN FOR TRAVEL TO LONDON UNITED KINGDOM, MAY 29-JUNE 2, 2012

(Decision sought)

ISSUE

Your approval is sought for Mr. Corey Dvorkin, Senior Analyst, National Cyber Security Directorate (NCSD), to travel to London, United Kingdom (U.K.), from May 29-June 2, 2012,

BACKGROUND

Canada's Cyber Security Strategy ("the *Strategy*") identified international collaboration as an essential activity in securing cyberspace for Canada. The proposed travel directly supports the commitment made in the *Strategy* to work with the Department of Foreign Affairs and International Trade Canada (DFAIT) to advance cyber security in Canada's foreign policy and builds on Public Safety Canada's (PS) International Strategic Framework.

Canada has agreed to be among 16 countries participating in the GGE on cyberspace. This is the third GGE, and the first time Canada has participated. Canada's delegation will be led by DFAIT, who has requested that PS subject matter experts attend preparatory meetings as well as the full GGE meetings in the coming year.

Our work on the GGE is a key component of broader Canadian action in promoting norms of conduct for cyberspace, a process begun last November at the London Conference on Cyberspace.

s.15(1) - Int'l

[redacted] This conference will likely feature ministerial participation from the U.K. and the United States, and it is expected that an invitation will be issued to Canada's Minister of Public Safety.

[redacted]

CONSIDERATIONS

The estimated cost for this trip to the U.K. is $6,170.29 which allows for a possible increase of $1,295.00 in airfare. This trip will replace Mr. Dvorkin's travel to the Internet Governance Forum in Geneva, Switzerland that was included in the 2012-2013 Branch travel plan.

agreed, provided it is economy class. G.

RECOMMENDATION

It is recommended that you approve the travel request for Mr. Dvorkin. Should you agree, your signature is sought on the attached Travel Authority and Advance form (**TAB A**). My approval is noted on the International Travel Request (**TAB B**).

Should you require additional information, please do not hesitate to contact me at 613-949-7380 or Robert Dick, Director General National Cyber Security at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure(s): (2)

I approve:

MAI MAY 18 2012

Graham Flack
Acting Deputy Minister

Prepared by: Corey Dvorkin

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

☐ Original / Prem. demande

☐ Amended (Same levels of approval as orginal dated)
Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

14A	Travel Authority No. (TAN) / N°. d'aut de voyager (NAV): DZD9 02474	Document No. - N° du document

Part A - Partie A

Type 2	Name of traveller - Nom du voyageur	Classification
	Corey Dvorkin	EC-08

Department - Ministère	Branch / Division / Group - Direction / Division / Groupe
Public Safety Canada	NS / National Cyber Security Directorate

Address - Adresse	Telephone No. - No. de téléphone	If different address, send cheque to: / Si adresse differente, envoyer chèque à
340 Laurier Ave	613-990-9608	
Branch Contact - Personne ressource à la direction: Jane Hayward	Telephone No. - No. de téléphone: 613-991-1982	

Purpose of travel - Objet du voyage	No. of days / Nbre de jours	Do you have a Govt Ind Travel Card (ITC)? / Avez-vous une carte de voyage (CV	If no, would you like to request one? / Les cas échéant, aimerier-vous en avoir une?
Planning Meeting for the United Nations Group of Governmental Experts	5	☐ Yes / Oui ☑ No / Non	☐ Yes / Oui ☑ No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

Date M / D-J	From - De	To - A	Time - Heure: Departure - Arrival / Départ - Arrivée	Transportation Transport: Mode	Transportation Transport: Class	No. of meals prepaid / Nbre de repas prépayés	Accommodation / Hébergement	File locator number / N°. de référence
May 29, 2012	Ottawa	London	23:35 - 11:10	Air	Economy	1	Hilton Kensington	
June 2, 2012	London	Ottawa	15:15 -17:50	Air	Economy	1		

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

Standard - Générales: Item / Type de dépenses	Estimated cost / Coût estimatif	Non-standard - Spéciales: Item / Type de dépenses	Estimated cost / Coût estimatif
Accomodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire)	$665.52	Accomodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire)	$0.00
Mid-size car rental (collision damage waiver mandatory) Location d'une voiture intermédiaire (assurance-collision du répertoire oblig.)	$0.00	Non mid-size car rental (collision damage waiver mandatory) Location d'une voiture non intermédiaire (assurance-collision du	$0.00
Private vehicle requested by: Voiture particulière demandée par: ☐ Traveller / Voyageur ☐ Employer / Employeur Public Liability and Property Damage min $1 million. Deductibles NON reimbursable Responsabilité civile et dommages matériels (min. 1 000 000$). Les franchises NO SONT PAS remboursables.	$0.00	Other (Specify) - Autre (préciser)	$0.00
		Upgrade transportation (specify in "Class" above) Transport à tarif supèrieur (préciser la <classe> si-dessus)	$0.00
Transportation Transport	$230.00	☐ First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) Business class / Other-Upgraded (other than article 3.1.9 Assistant Deputy Head or equivalent approval) Classe d'affaires - ou autre classe à tarif supérieur (approuveée par le sou-chef ou l'équiv,. S'il s'agit d'une classe non prévue à l'article 3.1.9)	
Meals and incidentals Repas et frais accessoires	$636.50		
Other (Specify) - Autre (préciser)	$200.00	Approval - Approbation	

Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre

Part D - Partie D

Estimated Cost - Coût estimatif

Prepaid - Prépayé
$4,438.23

Other - Autre
$1,732.02

Trip Total - Coût total du voyage
$6,170.25

Funding - Financement

A) Travellers cheques / Chèques de voyage

Cdn / Can	$0.00
US / É.U.	$0.00
Other / Autre	$0.00

B) Other advance / Autre avance

Cheque / Chèque	$0.00
Cash / Comptant	$0.00
Total funding requested (A + B) / Financement total demandé (A + B)	$0.00

Part E Traveller / Partie E - Voyageur

I have access to the Treasury Board Travel Policy (internal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
J'ai accès à un exemplaire de la politique du Conseil du Trésor sur les voyages (Politiques interne pour les employeurs distincts) et en accepte les conditions.

Corey Dvorkin — Signature — May 14/12 — Date

Ticket pick-up date and location / Date et lieu de la collecte des billets: On line

Recommended by (signature) - Recommandé par (signature)	Date	Approved by (signature) - Approuvé par (signa	Date
Lynda Clairmont	2012 05 15		MAI MAY 18 2012

Part F - Request for Advance / Partie F - Demande d'avance

Type 3	Particulars (stub information) - Détail (talon)	Cheque Amount / Montant du chèque	Date cheque required / Date demandé pour le
	DZD902474 C Dvorkin - London - May 29. 2012	$1360.00	May 28 - 2012

Payment Record / Enregistrement du paiement

Type 7	Sub-type / Sous-type	P.R.I. - C.I.D.P.	Amount - Montant	Req. No. - N° de la demande	Supplier indicator / Indicateur du fournisseur	Due Date / Date d'échéance
	8 | 0					

Tyoe 4 — **Accounting Information / Renseignement comptables**

Sub-type / Sous-type	Vendor Code / Code du fourn.	Departmental Ref. No. / No. de réf. Du ministère	Coding - Cidification	Amount - Montant
			496- PSCYBINTLENG - 2001 - 500096214	

	Description	Financial encumberance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature)	Requisition for payment pursuant to section 33 of the Financial Administration Act and certified in accordance with section 7 of the Payment Requisition Regulations. Demande pour paiement conformément à l'article 33 de Loi sur la gestion des finances publiques et certifié au termes de l'article 7 du Règlement sur les réquisitions de palements.	Cheque No. - N° du chèque
Verified correct (PWGSC) (signature) / Vérifié conform (TPSGC) (signature)		Date
Services officer (PWGSC) (signature) / Agent responsible (TPSGC) (signature)	Signature	

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé	Amount/Montant
Airfare / Frais d'avion	$4,438.23
Train / Train	$0.00
Other / Autres	$0.00
	$4,438.23

Estimated Cost - Coût estimatif: Other - Autre	Rate / Tarif	No. / Nbre	Amount/Montant
Accomodation (**WHITE** page hotel) / Hébergement (un des hôtels figurant dans la partie **BLANCHE** du ré	$221.84	3	$665.52
Accomodation (**GREEN** page hotel) / Hébergement (un des hôtels figurant dans la partie **VERT** du répertc	$0.00	0	$0.00
			$665.52
Mid-size car rental / Location d'une voiture intermédiaire			$0.00
NON Mid-size car rental / Location d'une voiture **NON** intermédiaire	$0.00	0	$0.00
Gasoline for Rentals / Essence pour voiture louée			$0.00
			$0.00
	Rate / Tarif	No. / Nbre	Amount/Montant
Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé	0.545	0	$0.00

		Rate / Tarif	No. / Nbre	Amount/Montant
Parking & Tolls / stationnement et frais de péage			$0.00	$0.00
Taxi/Limo	Home to Airport		$40.00	$230.00
	Airport - Hotel / Meetings		$75.00	
	Hotel - Airport		$75.00	
	Airport to Home		$40.00	
	Meeting - Meetings		$0.00	
Transportation / Transportation (No receipt)		**$10.00**		$0.00
Ferry & Miscellaneous			$0.00	$0.00
				$230.00

Canadian	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$15.60**		$0.00
Lunch / Déjeuners	**$14.85**		$0.00
Dinner / Dîners	**$40.85**		$0.00
Incidentals /Frais divers	**$17.30**	1	$17.30
		Total Canadian	$17.30

London, UK	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$25.46**	3	$76.37
Lunch / Déjeuners	**$46.44**	4	$185.77
Dinner / Dîners	**$61.92**	3	$185.77
Incidentals /Frais divers	**$42.82**	4	$171.28
		Total London, UK	$619.20

Country #2	Rate / Tarif	No. / Nbre	Amount/Montant
Breakfast / Petits déjeuners	**$37.46**		$0.00
Lunch / Déjeuners	**$37.46**		$0.00
Dinner / Dîners	**$47.87**		$0.00
Incidentals /Frais divers	**$34.13**		$0.00
		Total Country #2	$0.00
		GRAND TOTAL	**$636.50**

Business Phone / Téléphone d'affaires	$50.00
Airport Improvement Fee / Frais de l'Aeropart	$0.00
Cash Advance Fee / Frais d'avances	$0.00
Misc. Business Services / Diverses charges d'affaires	$50.00
Miscellaneous / Diverses - Conference Fees	$100.00
	$200.00

Commitment Authority (Section 32 FAA) Checklist

(version française est disponible)

1. **The following checklist has been provided to assist you with your Section 32 FAA verification.**
2. **This checklist must be included as supporting documentation.**

KNOW WHAT YOUR COMMITMENT AUTHORITY (S32 FAA) IS IN ACCORDANCE WITH YOUR FINANCIAL AUTHORITY SPECIMEN SIGNATURE RECORD (FASSR) AND THE PUBLIC SAFETY (PS) DELEGATION OF FINANCIAL SIGNING AUTHORITIES (DFSA) INSTRUMENTS
Note: The PS DFSA Instruments can be found on InfoCentral at: http://icarchive/foryou/divisions/comptroller/dfsa/index_e.asp

Pursuant to Section 32 of the *Financial Administration Act*, a sufficient unencumbered balance must be available in an appropriation and Expenditure Initiation must be evidenced in advance of setting up a Funds Commitment (FC) or Purchase Order (PO) in the financial system SAP.

☒	**Questions**
☒	Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments?
☒	Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)?

☒ Travel Authority and Advance Form (TAA)	☐ Advanced Authorization to Extend Hospitality Form (AAEH)	☐ Request to Attend Conferences Form	☐ Training Application and Authorization Form	☐ Membership Approval Form	☐ Other Specify:

☒	Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)?
☒	Does the Free Balance Report, generated and reviewed, ensure that an **unencumbered balance** exists for the Cost Center affected? Do I have authority to approve items for that Cost Centre, as per my FASSR?
	Have I completed all the paperwork requested by the Contracting Material Management group? ☒ Is the Sole Source Checklist complete and attached? ☒ Is the Competitive Contract Checklist complete and attached?
	Have I committed the funds in the financial system (SAP) by setting up a Purchase Order (PO) or Funds Commitment (FC) in the system? ☒ Ensure that proper financial coding is entered and correct amount is committed and a description is given (g/l, cost center and description of goods or services). ☒ Include the Purchase Order (PO) or Funds Commitment (FC) number on the line below.
	Asset Acquisitions: If any of the following questions are applicable, contact the Manager, External Reporting Group within the Financial Services & Systems Division (FSSD) and request an asset template to ensure accuracy of financial coding in the system. ☒ Does the cost exceed $10k, have a useful life of more than 1 year and does Public Safety control / own the item? ☒ Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? **Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.*

Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada | Canada

PWGSC > Buying and Selling > Services For Government > Travel Services > ACRD > Accommodation Search > Accommodation List

2012 Accommodation List

To view the establishment's information, select the establishment's name in the list below.
Note: All rates are quoted in Pound Sterling (GBP) unless otherwise indicated.

Accommodation List for London: May (Single Occupancy)

Accommodation	Address	Phone	Rate	Green Leaf Rating	Green Key Rating
Accommodations Outside North America					
Guest room					
Days Hotel Hounslow Heathrow East	8-10 Lampton Rd	4402085381230	89.00	None	None
Novotel London Heathrow	J4/M4, Cherry Lane	4401895431431	95.00	None	None
Radisson Edwardian Heathrow	140 Bath Rd, Hayes Middlesex	44 0 2087596311	115.00	None	None
Radisson Edwardian Grafton	130 Tottenham Court Road	44 0 2073884131	125.00	None	None
Radisson Edwardian Vanderbilt	68-86 Cromwell Road	44 0 2077619000	125.00	None	None
Hilton London Olympia	380 Kensington High St.	44 0 2076033333	138.00	None	None
Doubletree by Hilton London - West End	92 Southampton Row	00442072422828	150.00	None	None
Melia White House Hotel	Albany Street, Regents Park	44-20-7391-3000	150.00	None	None
Hilton London Kensington	179-199 Holland Park Avenue	44 207 603 3355	156.00	None	None
Business Class					
Novotel London Heathrow	J4/M4, Cherry Lane	4401895431431	115.00	None	None
Days Hotel Hounslow Heathrow East	8-10 Lampton Rd	4402085381230	119.00	None	None
One bedroom suite					
Hilton London Olympia	380 Kensington High St.	44 0 2076033333	178.00	None	None

Date Modified: 2011-10-06

Kensington Hyde Park Oxford Street

Public Safety Canada / Sécurité publique Canada

s.15(1) - Int'l

International Travel Request
Demande de voyage international

Event title - *Titre de l'événement*	Date of event - *Date de l'événement*	
	From - *Du* :	To - *Au* :
	May 29, 2012	June 2, 2012
Location (City, Country) - *Lieu (Ville, Pays)*	Estimated total cost - *Coût total prévu*	
London, United Kingdom	$6,167.26	

Description of meeting (provide agenda)
Description de l'événement (joindre l'ordre du jour)

The notional agenda for the meeting includes:

[redacted]

Pre-approved under Branch travel plans?
Pré-approuvé selon les directives sur les voyages de la direction générale?

☒ Yes/Oui ☐ No/Non

Participant(s)

Name (s) *Nom (s)*	Directorate/Branch *Direction générale/Secteur*	Work address *Adresse au travail*	Telephone No. *N° de telephone*
Corey Dvorkin	National Cyber Security Directorate - NS	340 Laurier Ave W.	613-990-9608

Purpose of travel and role of the traveler (e.g. annual conference, keynote speaker, study/learning visit, member of Canadian delegation, etc.)
Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)

The purpose of the travel is to provide cyber security specific subject matter advice for a small Canadian delegation meeting [redacted] in support of Canada's participation at the United Nations Group of Governmental Experts (GGE) on cyber issues which will commence at the United Nations in New York on August 6, 2012. [redacted]

Description of how event advances Department's priorities and expected outcomes
Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus

[redacted] More generally, the GGE is a significant venue in which we can pursue promulgating norms of conduct for cyberspace; a key cyber security policy objective.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

The Canadian delegation will be headed by Michael Walma, Director - International Crime and Terrorism Division of DFAIT and one of his senior analysts. Also attending will be a legal expert from the Judge Advocate General Corps at DND.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

NCSD has consulted with various sections at DFAIT.

It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travelers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT and Public Safety (International Affairs) officials in post-travel report circulation.

Il est entendu que les voyageurs devront présenter un bref rapport de 2 à 3 pages après la tenue de l'activité (y compris un synopsis, les mesures de suivi et l'avancement des priorités du Ministère) au plus tard dix jours ouvrables après leur retour. Les voyageurs devraient aviser les représentants de l'ambassade canadienne pertinente avant d'entreprendre le voyage et

Public Safety Canada / Sécurité publique Canada

AMEX TAN Number /Numéro de NAV

Issued By / Émis par: MCLISCH

Date Issued / Date d'émmision : 2012/05/23

TAN Number Info / Info numéro de NAV

Company Code / Code de société:	0880
TAN Prefix / Préfixe de NAV:	DZD9
TAN Number / Numéro de NAV:	DZD902474
Sequence Number / Numéro de séquence:	0006
Date Issued / Date d'émmision:	2012/05/23

Trip Details Info / Détails du voyage

Traveller Name / Nom du voyageur:	COREY DVORKIN
Date of Departure / Date de départ:	2012/05/29
Destination / Destination:	LONDON UK
Trip Purpose / Objet du voyage:	MEETING

Financial Coding Info / Info code financier

Cost Center / Centre de coûts:	496
GL Account / Compte général:	2007
Internal Order / Ordre interne:	
Earmarked Funds / Fonds réservés:	500096214001
Name of Sec.32 Officer / Nom de l'agent Sec. 32:	GRAHAM FLACK
Estimated Travel Charge / Estimation des frais de voyage:	0.00

Comments / Commentaires

Text / Texte:

If you have any questions or would like to cancel this TAN please contact Mike CLISCH @ 613-949-6807

Pour toute question ou pour annuler ce NAV, veuillez communiquer avec Mike CLISCH @ 613-949-6807

Public Safety Canada | Sécurité publique Canada
Deputy Minister | Sous-ministre
Ottawa, Canada
K1A 0P8

For your meeting with: Mr. Tim Page, President of the Canadian Association of Defence and Security Industries
On: December 10, 2012, 1:00 p.m. – 2:00 p.m.
At: 269 Laurier Avenue West, 19th floor

Lynda
1. Thks for the briefing
2. Let me know how things evolve.
Merci

UNCLASSIFIED

DATE:

File No.: 391785
RDIMS No.: 729734

MEMORANDUM FOR THE DEPUTY MINISTER

MEETING WITH MR. TIM PAGE, PRESIDENT, CANADIAN ASSOCIATION OF DEFENCE AND SECURITY INDUSTRIES

(For information)

ISSUE

You are scheduled to meet with Mr. Tim Page, President, Canadian Association of Defence and Security Industries (CADSI) on December 10, 2012, from 1:00 p.m. - 2:00 p.m. to discuss the SecureTech conference and opportunities for collaboration.

BACKGROUND

CADSI is composed of approximately 860 defence industry organizations and is responsible for coordinating the engagement of the defence sector on national security issues (e.g. cyber security, critical infrastructure resilience, cross border law enforcement).

CADSI's keystone event has been the CANSEC conference on military and defence technologies, held annually in Ottawa. In order to reach a larger potential market, CADSI is increasingly addressing national security topics, and these have evolved into a separate series of annual conferences known as SecureTech. The Minister of Public Safety and Departmental and Portfolio officials have routinely spoken at this event or participated in panels.

This year's SecureTech conference focused on two main topics: cyber security and perimeter security. Departmental officials worked with the conference organizers to shape the agenda to focus on cross border law enforcement and cyber security issues. The Minister delivered a keynote address, and three senior officials from Public Safety Canada (PS) participated in panels on cyber security, critical infrastructure, and cross border law enforcement. Staff from across the Department and the PS Portfolio also attended the conference. The agenda for this year's event is attached (**TAB A**).

s.19(1)

On November 6, 2012, Mr. Page wrote to you requesting a meeting to discuss his organization's security agenda. In his email,

CONSIDERATIONS

Cyber security has been a central element of SecureTech for several years. Initially, involvement by the National Cyber Security Directorate with CADSI offered a good opportunity to bring together policymakers, procurement officials and industry representatives from the national security community and generate awareness of *Canada's Cyber Security Strategy* (the Strategy). As the implementation of the Strategy has shifted from raising awareness to focus on security assessments and technical collaboration, the Department has diminished its cyber engagement with SecureTech.

While cyber security engagement has been downplayed, the Department is continuing to ramp up its engagement on critical infrastructure resilience. The defence industrial base is a key stakeholder for critical infrastructure engagement and CADSI, including the SecureTech conference, represents a good way to reach this audience. Mr. Page represented that sector in the National Cross Sector Forum at its most recent meeting on December 5, 2012. His participation in these meetings is helping to build positive momentum for the implementation of the *Action Plan for Critical Infrastructure*, and helps to shape the direction for critical infrastructure resilience in Canada.

NEXT STEPS

As CADSI is a strong voice among the critical infrastructure sectors, ongoing engagement will be important for the successful implementation of the renewed *Action Plan for Critical Infrastructure.* Key messages for your meeting with Mr. Page are attached (**TAB B**), expressing support for SecureTech and suggesting that there are ongoing opportunities for successful engagement and support in the area of critical infrastructure resilience.

Should you require additional information, please do not hesitate to contact me or Mr. Robert Dick, Director General, National Cyber Security, 613-990-2661.

for Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (2)

Prepared by: Corey Dvorkin

SecureTech 2012 Agenda

PERIMETER VISION TRACK

Canada-US Beyond the Border Initiative: Efficient Border Crossing for People - Innovative Technologies to Address Threats Early

Moderator:
Mr. Andrew Vallerand - Director, Directorate Science and Technology Public Security, Defence Research and Development Canada

Speakers:
Dr. Phil Lightfoot - Director Applied R&D Div, CBSA, Ottawa ON
Mr. Pierre Meunier - Head/Borders & Critical Infrastructure Resilience Section, DRDC Centre Security Science, Ottawa ON
Mr. Bob Bell - Director of R&D, NextGen ID Inc,
Dr. Anh Duong - Director Borders & Maritime Security , DHS S&T.
Insp. Andris Zarins - Director Border Integrity Team, RCMP, Ottawa ON

Details:

Canada and the US share responsibility for the safety, security, and resilience of Canada and of the United States in an increasingly integrated and globalized world. Canada and the U.S. have agreed to pursue a perimeter approach to security, working together within, at, and away from the borders of the two countries to enhance our security and accelerate the legitimate flow of people, goods and services between the two countries. The two countries intend to address security threats at the earliest point possible, in a manner that respects privacy, civil liberties, and human rights." Enabling trusted travelers to cross borders without cumbersome processes while ensuring that people who pose a risk are deterred from entering either country, constitutes a key element of the perimeter strategy. Achieving success depends on a complex set of integrated processes involving information gathering, analysis and intelligence sharing amongst trusted nations, while respecting fundamental human rights and privacy. Countries must increasingly innovate in intelligence analysis and train people who can correlate anomalous events to determine what it means, thereby ensuring appropriate and timely responses.

This panel will address the challenges of promoting the smooth flow of people across borders, through early identification of people who pose a risk, promoting entry-exit verification measures and greater information sharing and analysis. Panelists will explore the complex facets of early threat and hazard identification, key analysis requirements, improved technologies and options to enhance domain awareness.

The audience will gain from understanding the issues and challenges behind perimeter security issues and the impact of such measures on their business through business opportunities in simplifying the process of people and merchandise crossing.

Questions to be developed and debated:

1. The intricacies of implementing a shared border strategy – what has been achieved, what lies ahead?
2. What are the requirements for the future implementation?
3. How do we protect the privacy of people
4. How do we gather and analyze information (based on key analysis requirements)
5. What is being done in other countries (solutions, best practices)
6. What role exists for industry – where and how do they contribute?

Perimeter Security Panel 2: Technology Serving Intergrated Cross-Border Law Enforcement Operations

Moderator:
Chief Superintendent Joe Oliver - Director General Border Integrity, RCMP

Speakers:
Mr. Trevor Bhupsingh - Director General, Law Enforcement and Border Strategies, Public Safety Canada
Mr. Raul Ortiz - Deputy Chief of Operations Division, United States Border Patrol
Capt. Douglas Fears - Chief, Office of Law Enforcement Policy
Mr. Dave Kroetsch - President, Aeryon Labs
Mr. George Hawkins - RCMP Engineering Technology Program Manager

Details:

Enforcement agencies along the Canada - United States border share a long history of cooperative cross-border crime fighting. Their crime fighting strategies have evolved with time and, together, Canada and the United States have developed successful enforcement models – including Integrated Border Enforcement Teams (IBET), Shiprider and Border Enforcement Security Taskforces (BEST) – for preventing, investigating and prosecuting criminals who exploit the shared border.

On December 7, 2011, the Prime Minister of Canada and the President of the United States announced the Beyond the Border (BTB) Action Plan which sets out joint priorities for achieving the Shared Vision for Perimeter Security and Economic Competitiveness within four key areas of cooperation: addressing threats early; trade facilitation, economic growth and jobs; cross-border law enforcement; and critical infrastructure and cyber-security. In the action plan, Canada and the United States committed to build on existing bilateral law enforcement programs to develop the next generation of integrated cross-border law enforcement operations that leverage cross-designated officers and resources to jointly identify, assess and interdict persons and organizations involved in transnational crime. More specifically, Canada and the United States agreed to:

- Deploy regularized Shiprider operations;
- Implement two next generation pilot projects of integrated teams in areas such as intelligence and criminal investigations, and an intelligence-led uniformed presence between ports of entry;
- Enhance domain awareness in the air, land and maritime environments; and
- Provide interoperable radio capability for front-line law enforcement.

This panel will examine the challenges associated with seamless cross-border law enforcement operations and explore ways in which technology could be deployed to support integrated operations at the border including through enhanced domain awareness and enabling radio communications interoperability.

Questions to be developed and debated:

1. Threat assessments indicate that cross-border crime flows in both directions along the Canada-US border. For your perspective, what are the greatest threats and vulnerabilities?
2. What's required to enable integrated cross-border crime fighting?
3. What are the most significant challenges to advancing seamless cross-border law enforcement operations? What are your plans to mitigate these challenges?
4. Where are the greatest gaps in domain awareness? How might technology address these gaps?
5. What steps are being taken to address Canadians' concerns regarding sovereignty, privacy and protection of civil liberties?

Perimeter Security Panel 3: Protecting Critical Infrastructure and Developing and Incorporating Resilience Practices

Moderator:
Mr. Michael De Jong - Director, Critical Infrastructure Partnerships, Public Safety Canada

Speakers:
Mr. Francis Bradley - Vice-President, Policy Development, Canadian Electricity Association
Mr. Tim Roxey - Chief Cyber Security Officer North American Electric Reliability Corporation
Mr. Russell Stuart - Director, Health Services Emergency Management, Nova Scotia Department of Health and Wellness

Details:

Critical Infrastructure, Cyber Security and Resilience are inherently linked. Critical infrastructure sectors, such as energy, water, transportation, health, and finance, can be significantly impacted or extensively damaged by cyber attacks and other disruptions. The consequences on governments, institutions, businesses and individuals can be widespread and costly. Countries are striving to develop and maintain a secure, resilient and trusted critical infrastructure, including an electronic environment that supports national security and maximizes the benefits of the digital economy.

Questions/Topics to be developed and debated:

1. Future directions for critical infrastructure resilience
2. Strengthening cyber security
3. Reducing exposure of critical infrastructures to cyber risk
4. Methods of promoting shared situational awareness
5. Protecting critical cross-border infrastructure (measures)
6. Adopting and implementing resilience measures and plans
7. Restoring cross border flow after emergencies and disasters

Perimeter Security Panel 4: Canada - US Beyond the Border Initiative: Expedited Cargo Clearance

Moderator:
Mr. Scott Newark - Vice Chairman Operations, National Security Group

Speakers:
Mr. Jim Phillips - President Canadian American Border Trade Alliance
Dr. Anh Duong - Director Borders & Maritime Security , DHS S&T.
Mr. Arthur Mesher - Chairman of the Board and Chief Executive Officer of Descartes Software
Ms. Janet Rumball - Pre-Border Programs, Canada Border Services Agency

Details

An integrated cargo security strategy is a key element of the Beyond the Border Action Plan. Based on targeted security measures rather than simply 'more' security, the goal is expedited cargo clearance that increases efficiency while decreasing unnecessary costs of transporting commercial goods across borders. Enhanced clearance of cargo across borders requires the adoption of common standards including efficient and effective screening of inbound air and marine cargo at first point of arrival at the North American perimeter.

This panel will provide the policy rationale and expectations for expedited cargo clearance including through a 'perimeter security' strategy as well as insights into what security measures will be required and what technologies will be necessary to ensure success. The panel will also consider the institutional perspective of both the Canadian and American agencies that will deliver the enhanced and expedited screening. This is a 'don't miss' discussion for anyone involved in cross border commercial trade and the security sector whose products and services promote expedited cargo clearance that concurrently ensure the security of our borders.

Questions to be developed and debated:

1. How can coordinated and targeted security enhance cargo clearance at the NA perimeter and Canada-US border
2. What role will low risk ID programs play
3. What kind of security measures at ports of entry are contemplated
4. How and when will CBSA and CBP deploy these programs
5. How will these enhancements be funded
6. How can industry offer its suggestions to maximize program performance

CYBER SECURITY TRACK

Cyber Security Panel 1: Cyber Threat - The Way Forward

Moderator:
Mr. John Adams - Skelton-Clark Fellow, School of Policy Studies, Queen's University

Speakers:
Sir David Pepper - formerly Director, Government Communications Headquarters
Mr. Adam Hatfield - Director of Technical Advice, National Cyber Security, Public Safety Canada
Mr. Dean Turner - Director, Global Intelligence Network, Symantec Canada
Mr. Dave MacMahon - Senior Engineer, Complex Security Program, Bell Canada

Details:
Canada has embraced the Internet like no other nation in the world. And information and communications technology has contributed tremendously to Canada's economic prosperity, national security and quality of life. At the same time it has made us vulnerable to new threats. States, organized crime, non-state actors, terrorists and individuals use the Internet for a range of illegal activities. They steal our industrial and national security secrets and our personal identities, and they penetrate our critical infrastructure networks potentially disrupting our daily lives. And cyberspace is not governed by regimes of law and order that govern our physical world. Individual states can do much to improve their internal security but there are no borders in cyberspace and malicious hackers can hide among the billions of users with little fear of being identified and, if threatened, they can adjust quickly to cause harm in another form and fora. The long term objective for cyberspace must be a governance model that will impose/foster an environment where online threats are known and managed to the greatest extent possible. Achieving this will require sustained and coordinated collective action and investment by the Government of Canada (GOC), in conjunction with the provinces, its international allies, industry, academe and individual Canadians.

Questions to be developed and debated:

1. The intricacies of implementing a shared border strategy – what has been achieved, what lies ahead?
2. What are the requirements for the future implementation?
3. How do we protect the privacy of people
4. How do we gather and analyze information (based on key analysis requirements)
5. What is being done in other countries (solutions, best practices)
6. What role exists for industry – where and how do they contribute?

Cyber Security Panel 2: Big Data Analysis and Intelligence

Moderator:
Mr. Rafal Rohozinski - Principal & CEO, The SecDev Group

Speakers:
Mr. Abe Usher - Chief Innovation Officer, The HumanGeo Group
Mr. Doug Philippone - Palantir Technologies
Mr. Len Lidov - President and CEO, Morningside Analytics
Mr. Uriah Hakala - Senior Director, Professional Services and Partner Enablement

Details:

- Data points relevant to intelligence missions lie across a number of sources - public, private, open, classified, etc.
- Subject matter expertise, analysts, technical and development people, etc.
- Examples from intelligence, defence, countering fraud, analyzing world events and social/political movements.
- Future prospects for big data analysis and the relationship between industry, state

Questions/Topics to be developed and debated:
1. How do we draw out relevant insights?
2. How do we make them relevant in the larger intelligence cycle?
3. What are the skillsets required to take advantage of big data?

Cyber Security Panel 3: Secure Service Delivery: The Evolving Internet (IPV6) and the Impact to Online Service Delivery

Moderator:
Mr. Tyson Macaulay - Global VP, Telecommunications Strategy, McAfee

Speakers:
Mr. Jeff Lewis - ICT Security Team Lead, Canadian Internet Registration Authority
Mr. Ed Juskevicius - Manager, Infrastructure Security, Engineering, Planning and Standards Branch, Spectrum, Information Technologies and Telecommunications Sector, Industry Canada
Mr. Gary Cameron - Vice President, Networking and Security Solutions, Business Markets Division, Bell Canada

Details:

The Internet is migrating from the old version of the Internet Protocol (IP) called IPv4, to a new generation called IPv6. This is an urgent process. Not unlike a young person outgrowing their shoes, there is simply no space left for growth, and growth cannot be arrested or slowed without dire affects.

This panel will discuss selected the business, operational and technical challenges, requirements and solutions associated IPv6 migration and service delivery.

Questions to be developed and debated:

1. What are the business drivers and risks associated IPv6?
2. What are useful precedents and lessons learned so far?
3. When will IPv6 move from a nice-to-have technology to a must-have technology?

Cyber Security Panel 4: The Future Cyber Security Workforce –Cornerstone of Cyber Security Strategies

Moderator:
Mr. John Proctor - Consulting Services-Cyber Resilience, CGI Information Systems & Management Consultants Canada

Speakers:
Mr. Michael Doucet - Chief Information Officer, RCMP
Mr. Robert Biddle - Professor of Human-Computer Interaction, Carleton University, CIO, Financial Institutions
Mr. Stewart Cawthray - Chief Security Architect
Mr. Jim Connelly - Director, Intelligence & Operations Lockheed Martin, Computer Information Security (CIS)

Details:

Mark tweets his work day highlights... Jean-Marc meets a work deadline by burning the midnight oil at home. Maryse posts a few pics of her fender bender with a company vehicle on Facebook... Amar posts a video of his recent business trip on YouTube... Seemingly routine, daily happenings for our next gen workers but what is the other side of this instantaneous virtuality and connectivity? Is the connected workforce an asset to productivity or an expensive and critical liability?

Gathering and sharing information is key to our daily work lives. The challenge is that much of this information is unfiltered. Unfiltered in the sense that it is distributed, en masse, without the strategic lens and consideration of security, intelligence and communications. This unfiltered information can cause damage on many corporate fronts.

Questions to be developed and debated:

1. How will we create a culture of safety within the next gen workers, the Digital Natives?
2. How should we shape our regulatory and educational frameworks to embrace the digital technologies while addressing the concerns that they may present?
3. That will the full spectrum of essential cyber security skills encompass?
4. What does it take to be able to correlate anomalous events, determine their meaning and generate appropriate responses?

KEY MESSAGES

MEETING WITH MR. TIM PAGE, PRESIDENT, CANADIAN ASSOCIATION OF DEFENCE AND SECURITY INDUSTRIES

- The Department and the portfolio continue to support CADSI and the SecureTech conference and trade show.

- As you are aware, we have in the past provided significant support in helping shape the agenda and in providing speakers, including having the Minister appear.

- Working together, we have helped get the message out on the Government's cyber security strategy.

- Having largely been successful in doing that, we should look beyond SecureTech, and work on building a more robust relationship in regards to cyber security.

- Your members are an audience we are increasingly trying to reach as partners in delivering cyber security, and for critical infrastructure protection more generally.

- As such, I would like to thank you for participating in the National Cross Sector Forum, including our most recent meeting on December 5, 2012.

- As the representative of the Defence Industrial Base, your involvement in these meetings helps to build positive momentum for the implementation of the *Action Plan for Critical Infrastructure*, and helps to shape the direction for critical infrastructure resilience in Canada.

- I look forward to continuing our work together in these areas, including cross border information sharing activities, regional risk assessments, and helping to connect the Defence Industrial Base with other critical infrastructure sectors.

- Building on that work, we soon hope to begin engaging CADSI members with an eye to operationalizing information sharing, security assessments and technical collaboration on cyber security.

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister

Ottawa, Canada K1A 0P8

For your meeting with:
Canadian Cyber Incident Response Centre
On: December 6, 2012 at 10:30a.m – 11:30a.m.

UNCLASSIFIED

DATE: Dec 5, 2012

File No.: 391807
RDIMS No.: 729038

MEMORANDUM FOR THE DEPUTY MINISTER

VISIT TO THE CANADIAN CYBER INCIDENT RESPONSE CENTRE

(Information only)

SCENARIO

You will visit the Canadian Cyber Incident Response Centre (CCIRC) located at 257 Slater Street, December 6, 2012, from 10:30a.m. – 11:30a.m. Windy Anderson, Director of CCIRC, will meet you in the second floor Government Operations Centre (GOC) boardroom.

I will be accompanying you during this visit. The following people will also be attending:

- Graham Flack, Associate Deputy Minister;
- Karine Loiselle, Chief of Staff to the Deputy Minister;
- Annick Paquin, Executive Assistant to the Deputy Minister;
- Bob Gordon, Special Advisor, Cyber Security; and
- Robert Dick, Director General, National Cyber Security.

The visit will begin with a 30 minute presentation in the GOC boardroom. A copy of the presentation is attached (**TAB A**). The CCIRC management team, which consists of Luc Beaudoin, Manager, Operations, Patrick Clow, Manager, Technical Analysis and Ken Bendelier, Manager, Operational Analysis and Support will also attend the presentation.

Following this presentation, you will visit three areas of CCIRC:

- **Operations Section** – assists partners in identifying, mitigating, and managing cyber security incidents;
- **Technical Analysis Section** – provides technical analysis to support incident response and management, and operates CCIRC's lab infrastructure; and
- **Operational Analysis and Support Section** – builds and maintains operational relationships with partners, and produces operational analysis products for decision makers.

Each manager will walk you through a tour of their respective area of responsibility and introduce you to staff and describe the key functions they perform.

Should you require additional information, please do not hesitate to contact me or Robert Dick, Director General, National Cyber Security, at 613-990-2661.

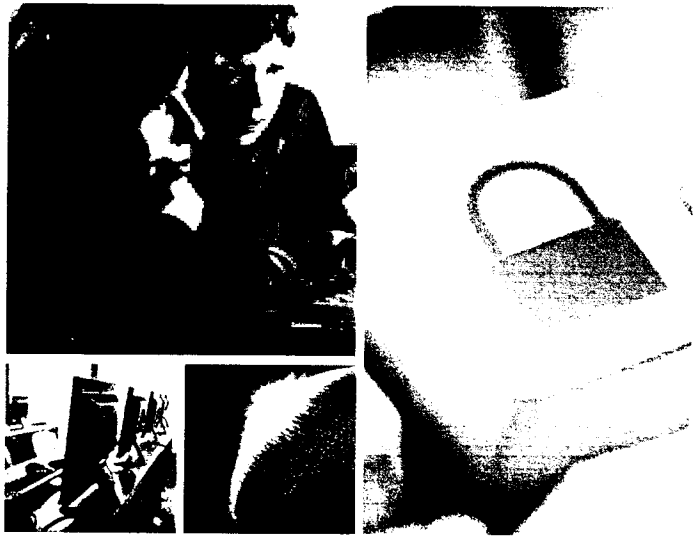
Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure: (1)

Prepared by: Véronique Proulx

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



Overview of the Canadian Cyber Incident Response Centre (CCIRC)

November 2012

RDIMS: 730396

Canada

Table of Contents

BUILDING A **SAFE** AND **RESILIENT CANADA**

Cyber Security Roles and Responsibilities within Public Safety Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

National Cyber Security Directorate (NCSD)

- Incident management, information sharing, cyber policy coordination, partnerships and engagement, and technical advice.

Critical Infrastructure and Strategic Coordination Directorate (CID)

- Critical infrastructure resilience and protection.

Communications Directorate

- Public awareness.

CCIRC Mandate

Mandate: Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events for vital systems outside of the Government of Canada.

Products and services	• Incident handling and national event coordination and assistance • Technical analysis and mitigation advice • Operational reporting and analysis
Recipients of products and services	• Provinces, territories (P/Ts), and municipalities • Critical infrastructure (CI) sectors: health, finance, information and communication technology, energy and utilities, food, water, safety, manufacturing, transportation • Vital systems of national importance
Collaboration	• P/Ts, municipalities, and CI sectors • International CERT* community, trusted vendors, academia, cyber security expert community • Security and intelligence (S&I) community

*CERT – Cyber Emergency Response Team

CCIRC Personnel and Budget

Personnel

- Salary of $2.2 million:
- 33 FTEs
  - EX-01 Director
  - 28 highly specialized computer specialists (CS) with knowledge of information technology (IT) security, computer forensics, and incident handling
  - 3 non-computer specialists for analysis of multi-source intelligence and technical data and writing strategic assessments
  - 1 administrative assistant

Budget

- Operations & Maintenance (O&M) budget of $1.1 million:
  - Training & Conferences (approximately $221K)
  - Travel (approximately $115K)
  - Software, licences & equipment (approximately $370K)
  - Translation (approximately $66K)
  - Professional Services (approximately $339K)

How CCIRC Works

BUILDING A **SAFE** AND **RESILIENT** CANADA

These partners... | *provide information to...* | *which provides these services:*

- Government Security & Intelligence community
- Critical Infrastructure
- Provinces and territories
- Five Eyes and International CERTs
- Trusted vendors
- Academia
- Cyber security expert community
- Open source

→ CCIRC →

Incident Handling and National Incident Coordination and Assistance

- Direct technical assistance to partners and coordination of Government response to cyber incidents of national significance
- Audience: operational and technical staff in partner organizations responding to cyber incidents
- Metrics: (2012 Year to Date) 1,622 events handled; 10,061 notifications to partners with compromised systems, and 103 requests issued to deactivate malicious systems.

Provision of Mitigation Advice

- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice
- Audience: technical staff in partner organizations
- Metrics: (2012 Year to Date) 18 cyber flashes, 45 advisories, and 13 other technical products.

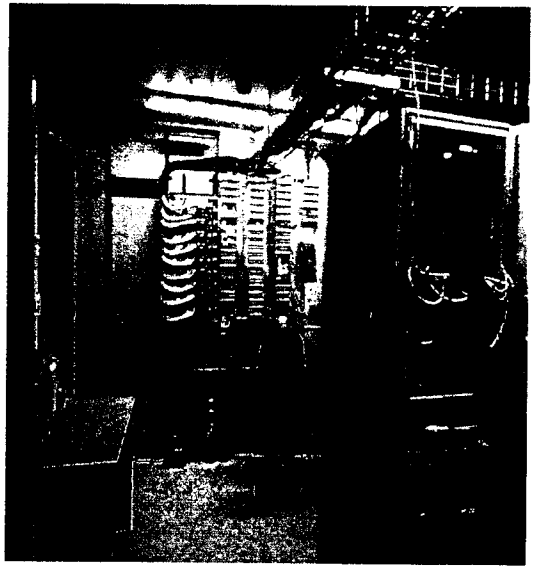
Operational Reporting and Analysis

- Daily, weekly, bi-weekly quarterly, and annual reports providing summary, trend, and operational analysis.
- Audience: technical staff and decision makers

CCIRC Services

- **Incident response centre**
  - Primary contact point into Government of Canada for domestic and international partners.
  - CCIRC subject matter experts on shift 0600-2100, 7 days a week.
  - 24/7 on-call response.

- **Computer lab**
  - Isolated from corporate network for analyzing malicious software (malware) and testing solutions.
  - Industrial control system (ICS) equipment for security testing and analysis in support of critical infrastructure (CI) sectors.



CCIRC Products

BUILDING A **SAFE** AND **RESILIENT CANADA**

Currently Produced | In Development

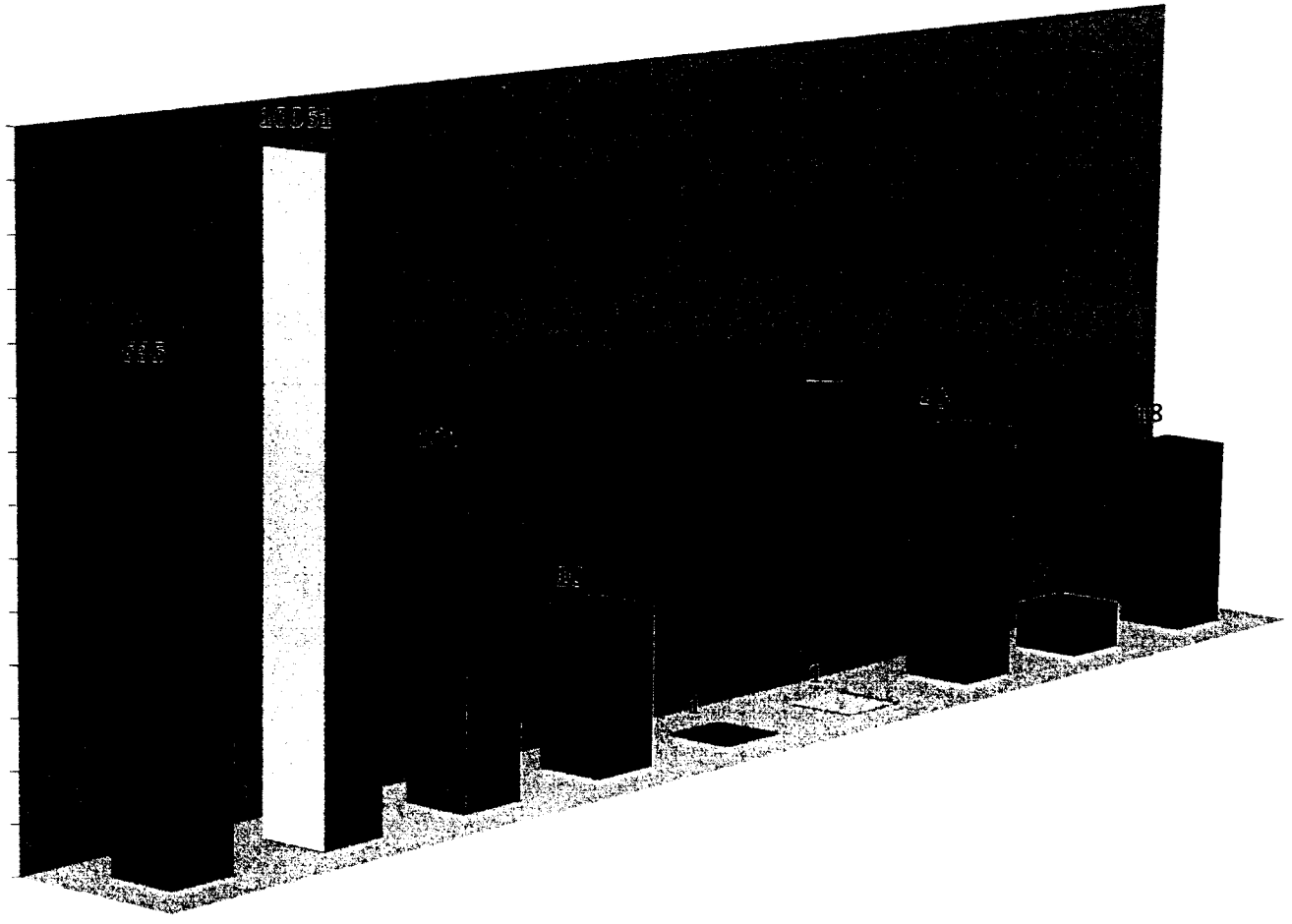
Product	Daily Report	Weekly Technical Report	Cyber Flash	Alert	Advisory	Technical Report	Information Note	Weekly Statistics Report	Cyber Operational Summary	Cyber Notifications and SITREPs	Quarterly Report	Annual Report
Description	Daily situation report	Summary of daily reports, CCIRC products / events / activities / indicators / and cyber reporting	Time sensitive reports for immediate security issues - Security fix not available	Cyber security advisory on threat and vulnerability - Security fix not available	Cyber security advisory on threat and vulnerability - Security fix available	Detailed report WRT a cyber security issue - Ad hoc	Report on significant cyber events - For general awareness	Weekly statistics of CCIRC activities / incidents / products	Notable cyber incidents / CCIRC products / open source reports	Provide senior management with timely awareness of noteworthy cyber incidents	Quarterly status report WRT to CCIRC incidents / products / trend analysis	Yearly status report WRT to CCIRC incidents / products / trend analysis
Clients	CCIRC / trusted GoC partners	P/T/CI/GoC operational contacts	P/T/CI operational contacts	P/T/CI operational contacts - Posted on website	P/T/CI operational contacts - Posted on website	P/T/CI operational contacts	P/T/CI/GoC - Posted on website	CCIRC / NCSD senior mgt	Public Safety / GoC / P/T/CI partners	Public Safety / GOC / PS Comms	Public Safety / GoC / P/T/CI partners	Public Safety / GoC / P/T/CI partners

Operational / Technical | Strategic

Summary of CCIRC Products and Services

BUILDING A **SAFE** AND **RESILIENT CANADA**

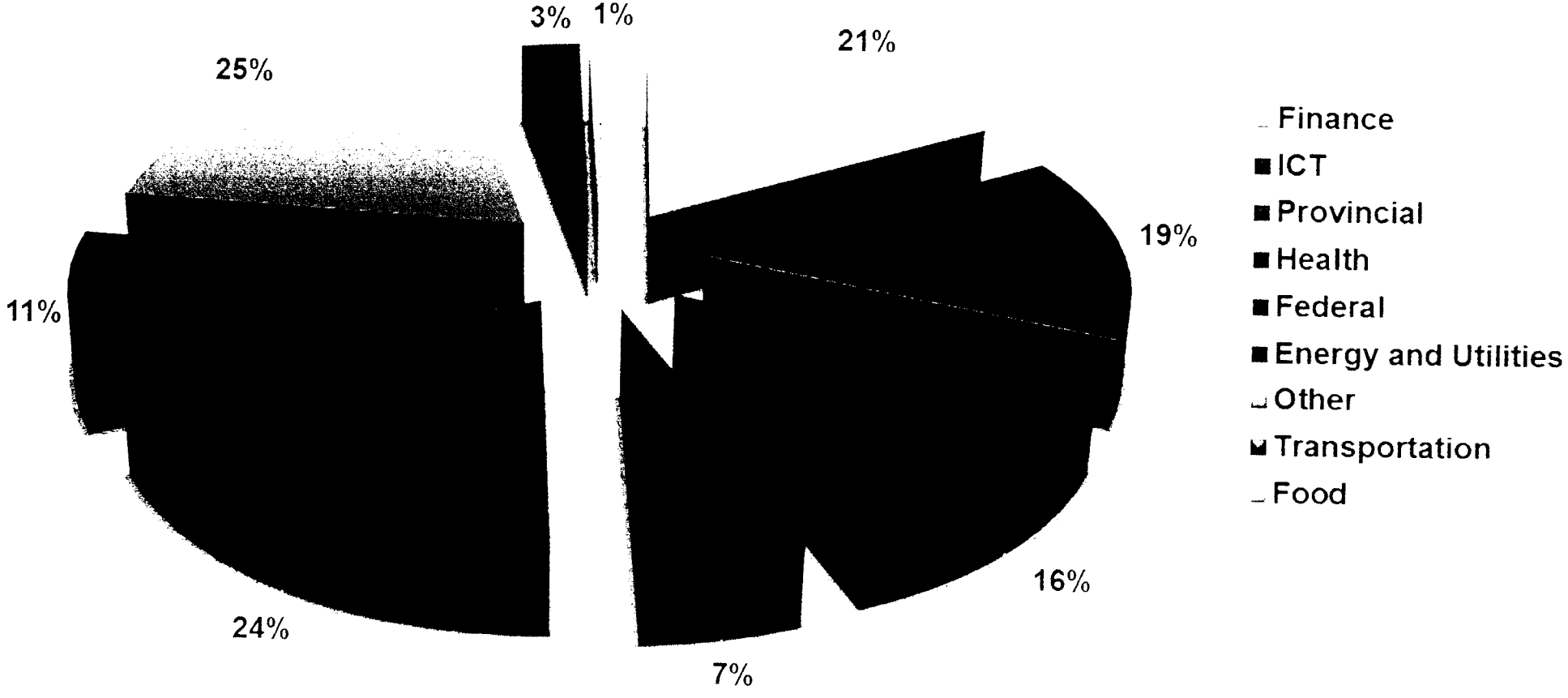
(2012 Year to Date)



Overview of Cyber Incidents by Sector

BUILDING A **SAFE** AND **RESILIENT** CANADA

April 1 - September 30, 2012:
488 incidents handled by CCIRC



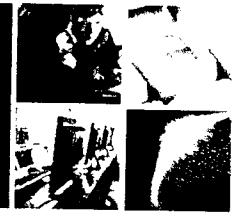
* *ICT – Information and Communications Technology*

Public Safety Canada / Sécurité publique Canada

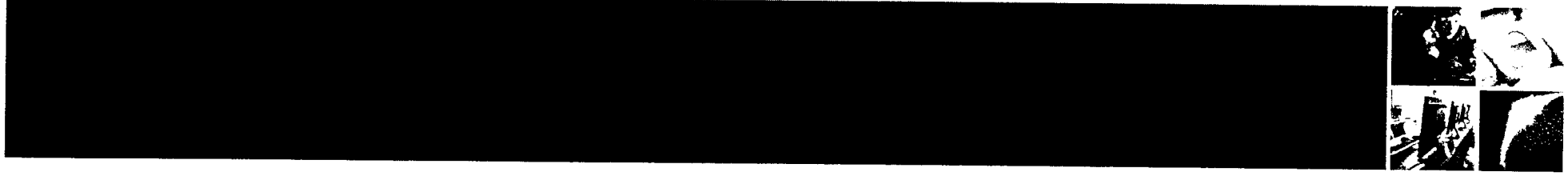
2012 – A Year of Progress

- **Strengthened CCIRC's legal, policy and process foundations**
  - Updated and focused mandate;
  - Approved CCIRC Privacy Impact Assessment.
  - Developing comprehensive suite of Standard Operating Procedures.
  - Developing standardized reporting criteria, impact assessment guidelines, and information sharing protocols.
- **Expanded collaboration with internal and external partners**
  - Enhancing trust through partner Non-Disclosure Agreements – Memorandums of Understanding;
  - Secure collaboration via the CCIRC Community Portal.
  - Tactical synchronization between CCIRC, the Government Operations Centre and PS Communications.
  - Validation through incident reporting trials with Ontario, Alberta and Manitoba.
  - Harmonization with partners via part time personnel exchanges (Department of Homeland Security, Government of Canada Cyber Threat Evaluation Centre).
  - Extension of hours of operations to 15/7.
- **Enhanced analytic capability**
  - Service consistency through the implementation of a comprehensive training package for CCIRC personnel.
  - Increased analytic capability provided by the acquisition of a world-class malware analysis lab.
  - Extended expertise and credibility with the development and deployment of an Industrial Control Systems (ICS/SCADA) test bed, which complement the Natural Resources Canada / Royal Canadian Mounted Police / Defence Research Development Centre training centre.

What CCIRC is Working Towards



- Defining criteria to identify vital systems of national importance (allies moving ahead with protecting private systems underpinning economic prosperity)
  - Complete engagement efforts with current priority sectors
  - Identify and engage with new priority sectors
  - Complete engagement efforts with partner sectors
  - Framework tabletop exercise with federal, provincial, critical infrastructure and private sector partners
- Technology: keeping pace; automation – solutions at cyber speed
  - Fully develop and operationalize CCIRC's new technology and enhanced capabilities
- Strengthened Industrial Control Systems (ICS) capability
- Accommodations: insufficient space and building closing
  - Move to new facility



Questions?

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: NOV 15 2012

File No.: 391480
RDIMS No.: 722886

MEMORANDUM FOR THE DEPUTY MINISTER

MEETING WITH MR. TIM PAGE, PRESIDENT, CANADIAN ASSOCIATION OF DEFENCE AND SECURITY INDUSTRIES

(Decision sought)

ISSUE

Meeting with Mr. Tim Page, President of the Canadian Association of Defence and Security Industries (CADSI), to discuss his security agenda.

BACKGROUND

CADSI represents over 860 member companies which comprise Canada's national defence and security industrial base. CADSI's stated mission is "to foster an environment for member firms to thrive in the international defence and security marketplace, thereby contributing to Canada's defence and security goals." Their business model has them host joint conferences and trade shows to bring together policymakers, procurement officers, and defence and security vendors at one venue.

In 2011, CADSI delivered the first instalment of its SecureTech conference and trade show which saw six key tracks – critical infrastructure, identity and access management, cyber security, maritime security, transportation security, and disaster management and emergency planning. This year, the SecureTech conference and trade show focused on two main tracks: cyber security and perimeter security.

Public Safety Canada (PS) has actively supported the SecureTech event, since its inception. The Minister of Public Safety, and departmental and portfolio officials have spoken at the event and participated in panels.

Additionally, in the lead up to this year's event, PS officials worked with the conference organizers to shape the agenda on the cyber security issue.

.../2

Canada

s.15(1) - Subv
s.19(1)
s.21(1)(a)
s.21(1)(b)

CONSIDERATIONS

On November 6, 2012, Mr. Page wrote to you [redacted]

It could be that in one instance the level of a scheduled participant dropped based on urgent matters on [redacted] However, in addition to the Minister's keynote address, three senior officials from PS participated in panels on cyber security, critical infrastructure, and cross border law enforcement. Other staff from across the Department attended the event.

[redacted]

RECOMMENDATION

Given the broad applicability of SecureTech's themes across the Portfolio, it is recommended that you meet Mr. Page. If you agree, officials from the National Security Branch will prepare the appropriate briefing materials for the meeting.

Should you require additional information, please do not hesitate to contact me or Mr. Robert Dick, Director General, National Cyber Security, 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

I approve:

François Guimont NOV 20 2012

I do not approve:

François Guimont

Prepared by: Kees Bradley

Public Safety Canada | Sécurité publique Canada

DEPUTY MINISTER'S OFFICE

UNCLASSIFIED

DATE: NOV 15 2012

File No.: 390472
RDIMS No.: 705170

MEMORANDUM FOR THE DEPUTY MINISTER
Via: Gary Robertson, ADM, Corporate Management Branch

TORONTO INDUSTRIAL CONTROL SYSTEMS SECURITY WORKSHOP

(Signature required)

ISSUE

In line with the new Directive on the Management of Expenditures on Travel, Hospitality and Conferences we are requesting your approval for the Industrial Control Systems Security Workshop which will be held in Toronto, November 19-20, 2012. The cost for the event is estimated to be $23,000 for 125 participants.

BACKGROUND

Building off the success of the recent workshop held in Calgary, Alberta, the National Cyber Security Directorate (NCSD) is preparing the first of two workshops planned for this fiscal year. Word of the workshops has begun spreading within the critical infrastructure community and there has been considerable interest and positive feedback from stakeholders. In total, Public Safety Canada (PS) and the Royal Canadian Mounted Police (RCMP) have partnered to host workshops across the country on seven separate occasions.

.../2

The events are a training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators to better secure their most critical control system and information technology assets. Invited speakers include industry experts and government officials, including representation from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation. The agenda for the workshop is attached for you information (**TAB A**).

PS regional offices, the RCMP, the Canadian Security Intelligence Service, and provinces and territories are engaged in preparing for and publicizing the Toronto workshop. The workshop has been communicated within the Government of Canada via the Control Systems Security Working Group. PS Communications and the Critical Infrastructure and Strategic Coordination Directorate have been made aware of the event.

The workshop series is a valuable tool in meeting several of NCSD outcomes including enabling PS and DHS to provide joint information sessions to key partners which is a deliverable under the Beyond the Border Action Plan and the DHS-PS Cyber Security Action Plan. The sessions also serve to increase awareness of the Canadian Cyber Incident Response Center and its services, and therefore to expand information sharing, notably in the area of industrial control systems security.

CURRENT STATUS

According to the new Directive on the Management of Expenditures on Travel, Hospitality and Conferences, your approval is requested for all events where cost is expected to be between $5,000 and $25,000. We are estimating the workshop costs would not exceed $23,000 (including HST and gratuities) for the 125 participants. The proposed event costs do not exceed the Treasury Board Maximum Cost per Person as outlined in the Treasury Board *Directive on the Management of Expenditures on Travel, Hospitality and Conferences*. All costs related to this request fall within my sector's Travel, Hospitality, and Conference Cap..

a) The workshop will take place at the Hyatt Regency in Toronto. The Hyatt was selected as it is significantly cheaper than the options in the area. A downtown Toronto location was selected to improve participation and reduce travel costs.

b) In terms of audio visual costs, three quotes were solicited and the least expensive option was selected.

c) To reduce costs and maximize value for money, no hospitality will be provided.

.../3

d) It is our estimate that the RCMP and Natural Resources Canada will incur costs not exceeding $1,500 each in travel expenses to have one of their employees present at the workshop.

RECOMMENDATION

It is recommended that you approve of the estimated budget of $23,000 for the workshop by signing this note.

Should you require additional information, please do not hesitate to contact me or Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure: (2)

I approve:

François Guimont

NOV 16 2012

I do not approve:

François Guimont

Prepared by: Guillaume Lefebvre/Tom Campbell/Ashley Bencke

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

2012 Control Systems Security Workshop
HYATT Regency, Toronto, Ontario
370 King Street West
Agenda
Monday, November 19, 2012

08:00 - 08:30	**Registration** (identification required)
08:30 - 08:45	**Welcome and Opening Remarks** TBD, Emergency Management Ontario
08:45 - 09:15	**State of Control Systems Cyber Security** Mike Chaney, Department of Homeland Security
09:15 - 10:00	**Cybercrime Threat in Control Systems** Dave Black, RCMP and John Caruthers, FBI
10:00 - 10:15	**Networking break**
10:15 - 11:00	**Current Threats and Trends** Joel Langill, SCADAhacker
11:00 - 11:45	**Canadian Cyber Incident Response Centre (CCIRC)** TBD, Canadian Cyber Incident Response Centre
11:45 - 13:00	**Lunch break**
13:00 - 13:45	**Smart Grid and Advanced Metering Infrastructure Security Research Activities** Mark Fabro, Lofty Perch
13:45 - 14:30	**Analysis first! A Model for Actionable Critical Infrastructure Cyber Intelligence** Sean McBride, Critical Intelligence
14:30 - 14:45	**Networking break**
14:45 - 15:30	**Control Systems Security Program (CSSP) cyber security products and services for owners and operators of Control Systems** Mike Chaney, Department of Homeland Security
15:30 - 16:15	**Cyber Security Partnership Program** TBD, Public Safety Canada
	National Energy Infrastructure Test Centre Dr. Felix Kwamena, Natural Resources Canada
16:15 - 16:30	**Closing remarks**

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

2012 Control Systems Security Workshop
HYATT Regency, Toronto, Ontario
370 King Street West
Agenda
Tuesday, November 20, 2012

08:00 – 08:30	**Registration** (identification required)
08:30 – 09:15	**SHODAN search engine** Bob Radvanovsky, Infracritical, Inc.
09:15 – 10:00	**Hack Session** Joel Langill, SCADAhacker
10:00 – 10:15	**Networking break**
10:15 – 11:00	**Real Time Forensics on SCADA/ICS: A Technical Case Study** Mark Fabro, Lofty Perch
11:00 – 11:45	**Exercising Security: A look inside the NERC Cyber Risk Preparedness Assessment Program** NERC (To be confirmed)
11:45 – 13:00	**Lunch**
13:00 – 13:45	José M. Fernandez (Polytechnique Montréal)
13:45 – 14:30	**Cyber Security Evaluation Tool (CSET) & Control Systems Cyber Security Training Opportunities** Mike Chaney, Department of Homeland Security
14:30 – 14:45	**Networking break**
14:45 – 15:30	**Advance Education in ICS Security** Wayne Boone, Carleton University
15:30 – 16:15	Critical Intelligence (To be confirmed)
16:15 – 16:30	**Closing remarks**

Page 648

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Subv, 16(2)(c), 21(1)(a), 21(1)(b), 21(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Page 649

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 21(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada
Deputy Minister | Sous-ministre
Ottawa, Canada
K1A 0P8

For your meeting with: DM Cyber
On: June 29, 2012
At: 2:00 p.m.

SECRET

DATE: June 20/12

File No.: 388253
RDIMS No.: Dragon 2385

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY:
PROPOSED MEETING OF JUNE 2012

(Decision Sought)

ISSUE

Proposed meeting of the Deputy Ministers Committee on Cyber Security (DM Cyber) on June 29, 2012, from 2:00 p.m. to 3:00 p.m. Your office has tentatively blocked this time in your schedule.

A proposed agenda is attached for your review and approval (**TAB A**).

BACKGROUND

The former Deputy Minister (DM) of Public Safety chaired the inaugural meeting of DM Cyber on January 12, 2012. At this meeting, it was agreed that the Committee would meet quarterly.

In January, the following issues were discussed.

- The primary objective of the meeting was to seek agreement on the membership and terms of reference for the Committee (**TAB B**). DM's approved both elements, and noted that DM colleagues from the broader interdepartmental community could be invited to participate in DM Cyber meetings when necessary.

- The Treasury Board of Canada Secretariat (TBS) spoke about the importance of network hygiene within the Government's information technology infrastructure. TBS described the challenges in protecting Government systems from threats, work undertaken in this area to date, and planned work going forward.

.../2

- Public Safety Canada (PS) provided an overview of cyber security roles and responsibilities within Government, and highlighted the level of interdependency between federal departments and agencies. DM's acknowledged the importance of improving current information sharing practices to eliminate redundancies and increase the efficiency of cyber security practices within Government. Work is ongoing in this area.
-
- DM Baker provided a debrief of the

During the roundtable, DM's expressed an interest in discussing several issues at future meetings, including:

AGENDA

Opening Remarks

During your opening remarks, you may wish to set the stage for the discussion of In addition, it is proposed that you provide an overview of the Audit on Protecting Canada's Critical Infrastructure from Cyber Threats.

Cyber Foreign Policy

Morris Rosenberg, Deputy Minister of Foreign Affairs, This is a deliverable under *Canada's Cyber Security Strategy*.

Recent Cyber Security Policy Developments

s.15(1) - Int'l
s.14(a)

s.15(1) -
s.21(1)(a)

s.15(1) - Subv

SECRET

NEXT STEPS

ADM Cyber will meet on June 27, 2012, to prepare the groundwork on cyber security issues identified on the agenda.

If you approve the agenda, briefing material and talking points will follow under separate cover.

Following the June meeting, the next DM Cyber meeting could be scheduled for August 2012. The National Security Advisor has requested that at the next DM Cyber an update on the status of *Canada's Cyber Security Strategy*, [redacted]

RECOMMENDATION

It is recommended that you approve the proposed agenda.

Should you require additional information, please do not hesitate to contact me at 613-990-4976, or Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Claimont
Senior Assistant Deputy Minister
National Security

Enclosure: (2)

Prepared by: Melanie Mohammed

I approve:

JUIN JUN 22 2012

Graham Flack
Acting Deputy Minister

Lynda,
So no good. But given team in AG audit, I think we need a dedicated agenda item. Cut my opening remarks by 5 mins

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

Deputy Ministers Committee on Cyber Security

June 29, 2012 – 14:00 to 15:00
19th floor boardroom, 269 Laurier Avenue West

AGENDA

	Time	Item	Associated Documentation
1.	14:00 *5 mins*	**Opening Remarks** Graham Flack, A/Deputy Minister, Public Safety Canada	N/A
2.	14:05 *20 mins*	**Cyber Foreign Policy** Morris Rosenberg, Deputy Minister, Foreign Affairs, Department of Foreign Affairs and International Trade *For discussion:* [redacted]	TBC
3.	14:25 *20 mins*	**Recent Cyber Security Policy Developments** Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada *For discussion:* [redacted]	TBC
4.	14:45 *10 mins*	**Draft Auditor General's Report** Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada *For information: Speak to the release of the draft Auditor General's Report.*	TBC
5.	14:55 *5 mins*	**Roundtable**	N/A

s.15(1) - Int'l
s.21(1)(b)

2012 11 15

Deputy

Sorry to be presenting this to you as a rush request. Unfortunately, the planning for the event was caught in the change in TB policy relating to approvals and some initial confusion on what this meant in practice.

Planning had been progressing nicely under the previous rules

Canada

which would have permitted approval within the branch.

Coming to you last minute is not something the National Security Branch makes a practice

Your approval of this submission is requested.

Bob Gordon.

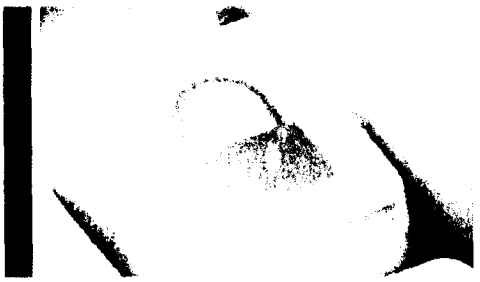
Comité des sous-ministres sur la cybersécurité

Le 29 juin 2012 – 14h00 à 15h00
Salle de conférence au 19e étage du 269, avenue Laurier ouest

ORDRE DU JOUR

	Heure	Item	Documentation connexe
1.	14h00 *5 mins*	**Mot de bienvenue** Graham Flack, Sous-ministre p/i, Sécurité publique Canada	S/O
2.	14h05 *20 mins*	**Politique étrangère cybernétique** Morris Rosenberg, Sous-ministre, Affaires étrangères, Ministère des Affaires étrangères et du Commerce international *Pour discussion:* [redacted]	À confirmer
3.	14h25 *20 mins*	**Développements récentes au niveau des politiques cybernétiques** Lynda Clairmont, Sous-ministre adjointe principale, Sécurité nationale, Sécurité publique Canada *Pour discussion:* [redacted]	À confirmer
4.	14h45 *10 mins*	**Ébauche du rapport du vérificateur général** Lynda Clairmont, Sous-ministre adjointe principale, Sécurité nationale, Sécurité publique Canada *Pour information: Parler de l'émission d'une ébauche du rapport du vérificateur général.*	À confirmer
5.	14h55 *5 mins*	**Tour de table**	S/O

s.15(1) - s.21(1)(b)



Deputy Ministers Committee on Cyber Security

Terms of Reference

Purpose

The purpose of the Deputy Ministers Committee on Cyber Security (DM Cyber) is to:

- establish policy direction;
- set priorities;
- monitor progress on the implementation of *Canada's Cyber Security Strategy*; and
- consider emerging issues.

Membership

- Chair and Secretariat:
  - Deputy Minister, Public Safety Canada

- Core members:
  - Director, Canadian Security Intelligence Service
  - Commissioner, Royal Canadian Mounted Police
  - Deputy Minister, National Defence
  - Chief of Defence Staff, Canadian Forces
  - Chief, Communications Security Establishment Canada
  - Deputy Minister, Foreign Affairs
  - Deputy Minister, Industry Canada
  - Deputy Minister and Deputy Attorney General of Canada, Department of Justice Canada
  - National Security Advisor to the Prime Minister, Privy Council Office
  - President, Shared Services Canada
  - Secretary of the Treasury Board, Treasury Board of Canada Secretariat

Governance / Relationship to other working groups and committees

DM Cyber is supported by the Assistant Deputy Ministers' Committee on Cyber Security, which is supported by the Directors General Committee on Cyber Security.

Meeting frequency

DM Cyber will meet quarterly, with *ad hoc* meetings called by the Chair as required.

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

SECRET (with attachments)

For your meetings with: Mr. Ian Fletcher
On: May 24, 2012
At: 7:00 pm at Le Cordon Bleu Bistro @ Signatures, 453 Laurier Avenue East and
On: May 25, 2012
At: 2:15 – 3:15 pm, Deputy Minister's Boardroom, 269 Laurier Avenue West

DATE: MAI MAY 2 2 2012

File No.: 387835
RDIMS No.: 617826

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

ATTENDANCE AT A DINNER IN HONOUR OF MR. IAN FLETCHER, AND A COURTESY CALL WITH MR. FLETCHER

(Information Only)

ISSUE

You will be attending a dinner in honour of Mr. Ian Fletcher, Director, Government Communications Security Bureau (GCSB), New Zealand on May 24, 2012. A list of the attendees for the dinner is attached (**TAB A**). You will also be meeting (courtesy call) with Mr. Fletcher on May 25, 2012. Mr. Fletcher will be accompanied by Mr. Tim Portland, Deputy Liaison Officer, Washington and Felicity Buchanan, Deputy New Zealand High Commissioner. Mr. Robert Gordon, Acting Senior Assistant Deputy Minister, National Security will also attend.

BACKGROUND

Mr. John Forster, Chief of the Communications Security Establishment Canada (CSEC), will be hosting a dinner in honour of Mr. Ian Fletcher on May 24, 2012, at 7:00 p.m. at Le Cordon Bleu Bistro @ Signatures, 453 Laurier Avenue East. Background information relating to GCSB is attached (**Tab B**). A classified briefing note for the courtesy call is also attached (**Tab C**). Biographical information for Mr. Fletcher is attached (**Tab D**).

.../2

GCSB is responsible for a number of functions, including foreign signals intelligence, cryptologic services, and cyber security for critical infrastructure. It is also both the national computer emergency response team (CERT) and the government CERT. These functions are handled by different organizations in Canada.

Canada and New Zealand collaborate on cyber issues through a number of international mechanisms, including: the Usual 5 (U5), a working group of CERTs of the Five Eyes countries; the Ottawa 5 (O5), a group of Five Eyes allies that focuses on coordinating international cyber and Internet policy; and the Strategic Alliance Group (SAG), which is made up of Five Eyes federal and national law enforcement organizations.

CURRENT STATUS

The dinner will be informal, but business attire is requested. There is no formal discussion scheduled, though informal discussions surrounding topics of mutual interest may take place. The courtesy call will provide an opportunity to discuss topics of mutual interest in greater detail.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Attachments: (4)

Prepared by: Ian Anderson

List of Attendees
Dinner in honour of Ian Fletcher
Thursday May 24th, 2012

John Forster, Chief CSEC
Toni Moffa, Deputy Chief ITS (CSEC)
Shelly Bruce, Deputy Chief SIGINT (CSEC)
Ian Fletcher, Dir GCSB NZLD
Tim Portland, Deputy Liaison Officer Washington
Felicity Buchanan, Deputy High Commissioner, New Zealand High Commission
Richard Fadden, Director CSIS
Stephen Rigby, National Security Advisor to the Prime Minister
Rennie Marcoux, Assistant Secretary, Security and Intelligence, Office of the National Security Advisor
Matthew King, Associate Deputy Minister, National Defence Canada
Graham Flack, A/Deputy Minister, Public Safety Canada

Venue: Le Cordon Bleu Bistro at Signatures
Address : 453 Laurier Ave East
Room : Declaration Room (Private Room – Main Floor – Left Side)
Time: 7:00 pm
Dress Code: Business Attire (Suit/Tie)
Parking: Free on Premises

BACKGROUNDER: DINNER IN HONOUR OF, AND COURTESY CALL WITH, MR. IAN FLETCHER, DIRECTOR OF THE GOVERNMENT COMMUNICATIONS SECURITY BUREAU, NEW ZEALAND

The Government Communications Security Bureau

The Government Communications Security Bureau (GCSB) is New Zealand's signals intelligence agency, and it is also responsible for information security. Mr. Fletcher is its director. New Zealand's National Cyber Security Centre (NCSC) is housed within GCSB, and acts as both the national cyber emergency response team (CERT) and the government CERT.

GCSB has multiple functions that are fulfilled by different organizations in Canada. The table below summarizes these functions and the Canadian counterparts who perform similar functions.

	New Zealand	Canada
Foreign signals intelligence, cryptologic services	GCSB	CSEC
Cyber security support for vital systems, including critical infrastructure (CI)	NCSC, under GCSB	CCIRC
Government CERT (information security)	NCSC, under GCSB	Cyber Threat Evaluation Centre (CTEC), under CSEC
National CERT	NCSC, under GCSB	CCIRC

New Zealand avoids duplication of technical capabilities by having cryptologic and CERT functions housed within the same organization, GCSB. This also enables GCSB to leverage intelligence material to accelerate the mitigation of cyber attacks. Cyber security-related support to critical infrastructure (CI) is also a function of NCSC. They use a reduced set of CI sectors which includes finance, telecommunications, and supervisory control and data acquisition (SCADA) systems.

New Zealand's Cyber Security Strategy

New Zealand's Cyber Security Strategy was released in June 2011. The strategy outlines the main cyber threats facing New Zealand and presents measures to address them. It identifies four key cyber threats facing New Zealand: cyber crime; cyber espionage; hacktivism; and terrorist use of the Internet. The strategy highlights the need for the New Zealand Government to develop and maintain partnerships with local governments,

private industry, non-governmental organisations (NGOs), and international partners to promote cyber security

Canada is closely following New Zealand's policy development on cyber security, including their cyber roles and responsibilities.

Relevance to Canada

New Zealand is increasingly reliant on cyber technologies for economic and social development, facing many of the same cyber issues and questions Canada does. Also, New Zealand's cyber strategy, similar to Canada's, focuses on three priority areas: protecting government systems; improving the government's capacity to plan and respond to cyber threats to its national critical infrastructure; and increasing awareness about cyber security issues and promoting safe online practices for businesses and individuals.

Canada and New Zealand collaborate on cyber issues via a working group of the Five Eyes countries known as the Usual 5 (U5). The U5 comprises the CERTs of each country. Members are working to develop common metrics and terminology to enable cross country comparison and develop data on trends being observed globally.

Collaboration also occurs through the Strategic Alliance Group (SAG), which is made up of Five Eyes federal and national law enforcement organizations. The Canadian member is the RCMP. There are three working groups under the SAG, including the Cybercrime Working Group. The SAG's work includes addressing evolving cybercrime threats, and information sharing among partners.

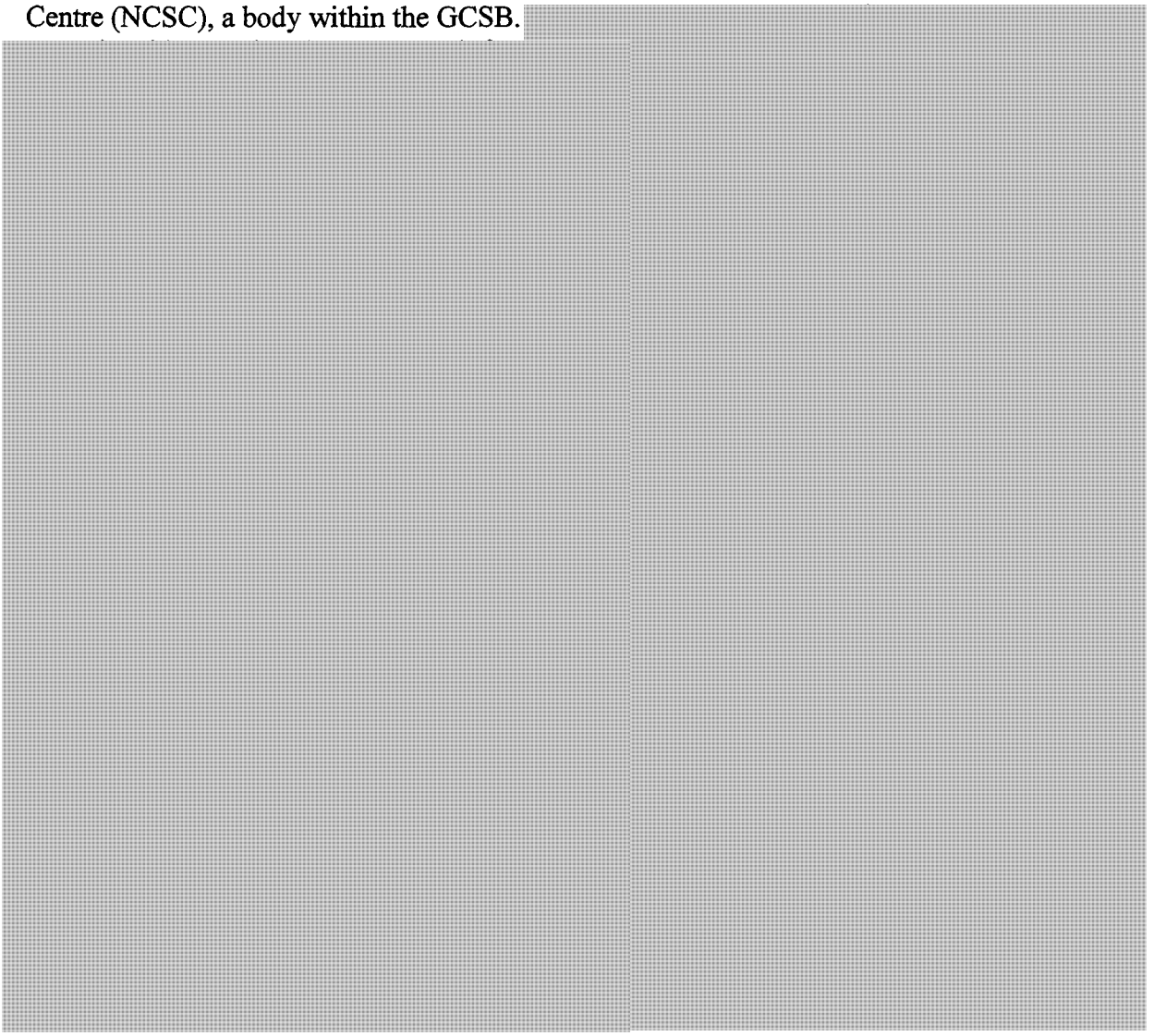
New Zealand also works with close allies, including Canada, to coordinate cyber and internet issues internationally. These allies have committed to harmonizing, to the extent possible, their approaches to international policy challenges.

COURTESTY CALL WITH MR. IAN FLETCHER, DIRECTOR OF GCSB

This classified briefing note provides information on collaboration between Canada and New Zealand and a recent initiative of CCIRC. Canada and New Zealand collaborate on cyber security and Internet issues through the Usual 5 (U5) and the Ottawa 5 (O5). Additionally, CCIRC is developing a web portal to facilitate interaction with its clients and Five Eyes counterparts.

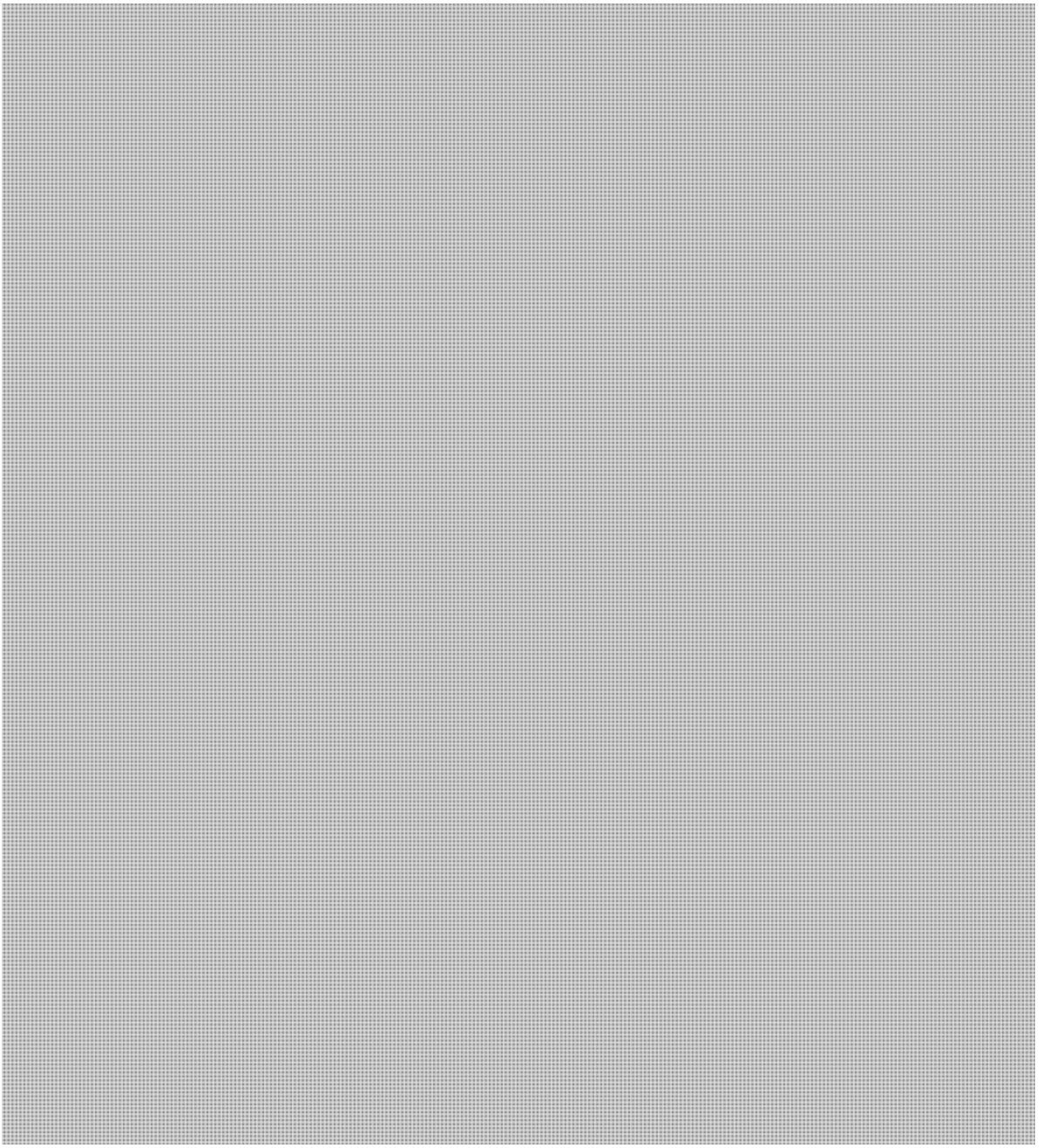
The Usual 5 (U5)

CERT to CERT collaboration takes place between Canada and New Zealand through the U5, a collection of the Five Eyes countries' national CERTs. Canada is represented at the U5 by CCIRC, while New Zealand is represented by their National Cyber Security Centre (NCSC), a body within the GCSB.



s.15(1) - Int'l

The Ottawa 5 (O5)



CERT Operations

The Government of Canada has recently approved a second set of initiatives and funding for Canada's Cyber Security Strategy. CCIRC is expanding its operational capacity and its ability to support industry and government partners across the country and internationally. CCIRC's operational coverage will expand to 15 hours per day, 7 days per week from the current 8 hours per day, 5 days per week. CCIRC will also bring on additional technical and analytical personnel and will upgrade and expand its technical laboratory. No formal announcement of this new funding is currently planned.

s.15(1) - Int'l

As it expands operations, CCIRC is considering how best to engage its client base, which handles CI and systems of vital importance. For example, CCIRC is developing a web portal to allow approved clients to access obtain general information, as well as specific, compartmentalized information relevant to their sector of work.

Possible discussion item:

- How does NCSC interact with its private sector and CI clients? What can be learned from New Zealand's experience and applied to the Canadian context?

BIOGRAPHY OF IAN FLETCHER, DIRECTOR OF THE GOVERNMENT COMMUNICATIONS SECURITY BUREAU (GCSB), NEW ZEALAND

In early 2012, Ian Fletcher took up the appointment of Director, Government Communications Security Bureau. Ian [redacted] has spent a good deal of his career as a senior public service executive in Australia and the United Kingdom. Prior to his role at GCSB, he was the Director-General and Chief Executive Officer of the Queensland State (Australia) Department of Employment, Economic Development and Innovation. Before that, he served in a number of roles, including: Chief Executive of the UK's Intellectual Property Office; Managing Director of UK Trade and Investment; and the Principal Private Secretary to the Cabinet Secretary and Head of the Home Civil Service. He has also worked for the European Commission [redacted] for the UN Administration [redacted]

[redacted] moving to the UK civil service in 1989. Ian has had extensive policy and operational experience, especially in relation to economic and trade issues.

Ian has been appointed for a five year term. [redacted]

s.19(1)

Public Safety Canada
Sécurité publique Canada

Senior Assistant Deputy Minister
Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

For your meeting with: Mr. Ian McKenzie
On: May 10, 2012, 7:00 p.m.
At: Social Restaurant, 537 Sussex Drive

DATE: MAY 09 2012

File No.: 387575
RDIMS No.: 610834

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

ATTENDANCE AT A DINNER IN HONOUR OF MR. IAN MCKENZIE

(Information only)

ISSUE

You will be attending a dinner in honour of Mr. Ian McKenzie, Director, Defence Signals Directorate (DSD), Australia on May 10, 2012. Also attending are; Richard Fadden, Director of the Canadian Security Intelligence Service, Stephen Rigby, National Security Advisor to the Prime Minister, Rennie Marcoux, Assistant Secretary, Security and Intelligence, Office of the National Security Advisor, and Matthew King, Associate Deputy Minister, Department of National Defence.

BACKGROUND

Mr. John Forster, Chief of the Communications Security Establishment Canada (CSEC), will be hosting a dinner in honour of Mr. Ian McKenzie on May 10, 2012, at 7:00 p.m. at Social Restaurant, 537 Sussex Drive. Background information relating to DSD is attached (**Tab A**). Biographical information for Mr. McKenzie is included (**Tab B**), which is classified as Confidential.

DSD and the Australian Security Intelligence Organization (ASIO) are counterparts to CSEC and CSIS, respectively. DSD's Cyber Security Operations Centre (CSOC) provides resources to assist government agencies, such as ASIO, in mitigating cyber threats to Australia's national security. It may also assist the Australian Federal Police (AFP) in their fight against cybercrime, which is a role played by the Royal Canadian Mounted Police (RCMP) in Canada.

.../2

Canada

Canada and Australia collaborate on cyber issues through a number of international mechanisms, including: the Usual 5 (U5), a working group of Computer Emergency Response Teams (CERT) of the Five Eyes countries; and the Strategic Alliance Group (SAG), the federal/national law enforcement organizations of the Five Eyes countries.

CURRENT STATUS

The dinner will be informal, but business attire is requested. There is no formal discussion scheduled, though informal discussions surrounding topics of mutual interest may take place.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (2)

Prepared by: Ian Anderson

BACKGROUNDER: DINNER IN HONOUR OF MR. IAN MCKENZIE, DIRECTOR OF THE DEFENCE SIGNALS DIRECTORATE, AUSTRALIA

The Defence Signals Directorate

The Defence Signals Directorate is Australia's signals intelligence agency, and it is also responsible for information security.

In January 2010, Australia created a National Cyber Security Operations Centre (CSOC) within the Defence Department and moved its cyber emergency response team (CERT) from the private sector to the public sector, where it is hosted by the Attorney General's Department. CSOC focuses on the highly sophisticated attacks against government departments while CERT Australia manages all of the other parts of the cyber incident response spectrum, including national and international response. These organizations are similar to the Communications Security Establishment, and the Canadian Cyber Incident Response Centre, respectively.

Of the Five-Eyes allies, the United States, the United Kingdom, and Australia have a mandate to pursue offensive cyber operations outside of military operations.

Australia's Cyber Security Strategy

Australia's *Cyber Security Strategy* was released in November 2009. The aim of Australia's strategy is "the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy."

The guiding principles of Australia's strategy focus on national leadership, shared responsibilities and partnerships, active international engagement, risk management, and preserving Australian societal values, such as privacy.

Canada is closely following Australia's policy development on cyber security, from its 2008 *E-Security Review,* to the release of its *Cyber Security Strategy*, to the announced forthcoming White Paper on cyberspace.

Relevance to Canada

Canada's Cyber Security Strategy aims to secure and make resilient our electronic infrastructure to foster economic prosperity. This is being achieved by securing government systems, collaborating to secure vital cyber systems outside the federal government, and helping Canadians to be secure online. The Strategy establishes federal leadership on cyber security, while building credibility and capability.

The convergence of objectives and principles between the two strategies suggests there are significant opportunities for shared work and cooperation in this field to achieve our shared desired outcomes.

Canada and Australia collaborate on cyber issues via a working group of the Five Eyes countries known as the Usual 5 (U5). The U5 comprises the CERTs of each country. Members are working to develop common metrics and terminology to enable cross country comparison and develop data on trends being observed globally.

Collaboration also occurs through the Strategic Alliance Group (SAG), which is made up of Five Eyes federal/national law enforcement organizations. The Canadian member is the RCMP. There are three working groups under the SAG, including the Cybercrime Working Group. The SAG's work includes addressing evolving cybercrime threats, and information sharing among partners.

Australia is also a member of a small group of close Canadian allies that coordinates cyber and internet issues internationally. All members have committed to harmonizing, to the extent possible, their approaches to international policy challenges.

Pages 671 to / à 672

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Graham

Attached article may serve as a discussion topic with Jon.

Bob

Canada

Department of Defence media release

30 March 2012

iPhones and iPads now certified for classified government use

The Defence Signals Directorate (DSD) has certified the use of government owned iPhones and iPads for classified Australian government communications.

DSD has led the way to safely enable devices running the latest Apple operating system (iOS version 5), and that are owned by Australian government agencies, to communicate and store classified information up to the PROTECTED level.

Mr Mike Burgess, Acting Director DSD said that DSD has been working closely with industry to develop practical instructions for government to securely use the latest technologies.

"Embracing new technologies, such as smart phones and tablet PCs, provides government with a genuine opportunity to conduct its business more efficiently."

"However the threat of government information being stolen or compromised is also very real," he said.

"DSD is continuously working to help agencies better protect valuable government information, while still enabling them to benefit from the advantages of these devices."

The iOS5 successfully passed an evaluation using a stringent and intensive security assessment to ensure it met Australian Government information security requirements.

The formal security evaluation, the first of its kind for iOS5, covers devices that are owned and managed by Australian government agencies that have implemented specific DSD security advice.

An accompanying security hardening guide is available at the DSD website along with more information on the outcome of the evaluation: http://www.dsd.gov.au

Media contact:

Defence Media Operations 02 6127 1999

Subscribe to our RSS Feed

Public Safety Canada | Sécurité publique Canada
Senior Assistant Deputy Minister | Sous-ministre adjoint principal
Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:
MAI MAY 11 2012
File No.: 387437
RDIMS No.: 608773

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

REVIEW OF THE MEMORANDUM OF UNDERSTANDING CONCERNING CYBER SECURITY ROLES AND RESPONSIBILITIES

(Signature required)

ISSUE

Your approval of the review of the Memorandum of Understanding (MOU) between the Communications Security Establishment Canada (CSEC) and Public Safety Canada (PS) concerning cyber security roles and responsibilities (**TAB A**).

BACKGROUND

On June 15, 2011, PS and CSEC signed a MoU (**TAB B**) that established a general framework agreement which sets out the principles of cooperation that guide the realignment of cyber security roles between PS and CSEC. As part of that agreement, PS and CSEC committed to undertake a review to assess the implementation of the MoU.

A thorough review of the commitments made under the MOU was conducted by a joint CSEC and PS team. The review confirms that the spirit and intent of the MoU is being followed and includes several recommendations for PS and CSEC going forward.

s.15(1) - Subv

[redacted] at CSEC and I have approved the review document and the list of action items going forward for our respective departments.

RECOMMENDATION

Should you agree with the findings of the MoU review, it is recommended that you approve the document by signing the two copies attached. The document will be provided to the Office of the Auditor General as part of their audit of protecting critical infrastructure from the cyber threat.

.../2

Canada

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure(s): (2)

Prepared by: Jeffrey Bonvie

SIX MONTH REVIEW

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

AND

PUBLIC SAFETY CANADA

CONCERNING CYBER SECURITY ROLES AND RESPONSIBILITIES

PURPOSE

On June 15, 2011, a Memorandum of Understanding (MoU) was signed between the Communication Security Establishment Canada (CSEC) and Public Safety Canada (PS) to realign roles and responsibilities for the Government of Canada Cyber Threat Evaluation Centre (GC CTEC) at CSEC and the Canadian Cyber Incident Response Centre (CCIRC) at PS. As called for in the MoU, a review was conducted that assessed the implementation of the MoU.

APPROACH

A thorough review of the commitments made under the MoU was conducted by a joint CSEC and PS team. The review primarily focused on the actions noted in Section 4, *Transfer of Responsibilities of Cyber Incident Management for Government Networks*, Section 5, *Cooperation Principles in Relation to Cyber Security Roles*, and Section 6, *Administration and Management*. Other portions of the MoU were included where appropriate. The review considered the following:

1. Determine if the parties met the commitments outlined in the MoU.
   - Identify if the commitment was completed and where required, note what more should be done to meet the commitment.
   - Identify, where applicable, alternative approaches that have been utilized to meet the commitments.
   - Outline any commitments that have yet to be addressed and provide advice, recommendations and other comments as appropriate.

2. Identify changes in the operational environment that may necessitate updating the MoU.
   - Identify changes that have occurred and are currently impacting the MoU as written.

- Identify, where possible, forthcoming changes that are anticipated to have an impact on the MoU.

Overall, we found that both parties have respected the spirit and intent of the MoU. However, changes to the operating environment necessitate some adjustments. The review findings led to the development of several recommendations, both for immediate benefit and for strategic planning consideration.

IMPLEMENTATION OF REQUIREMENTS

The findings are outlined below according to the respective sections within the MoU.

Transfer of Responsibilities of Cyber Incident Management for Government Networks

The transfer of responsibilities of the MoU occurred as scheduled on June 20, 2011. GC CTEC became the focal point for GC cyber incident management and CCIRC focused on the non-federal domain for its primary client base. Both GC CTEC and CCIRC are currently operating as per the division of effort described in the MoU and good collaborative steps have been established during this first year that will continue to mature. Respective stakeholders are receiving informed advice and assistance, and the products and services of both entities are continuing to evolve. Interaction between the teams for situational awareness began at a tactical level but has progressed to include strategic international efforts that will expand over time.

Both organizations have recognized that their specific functions are inaccurately depicted in the existing Government of Canada Information Technology Incident Management Plan (IMP). Changes in the IMP need to be aligned in keeping with the more recent Shared Services Canada (SSC) responsibilities as this centralized IT management department becomes fully operational. More clarity is required regarding the terminology used and the responsibilities that are implied under the IMP. For example, definitions of fundamental terms and clearer responsibilities for incident mitigation versus recovery need to be articulated.

The IMP revision, once concluded, will provide a central reference that frames all incident response mechanisms, those of the standard IT scope through the range of cyber-related developments. The IMP's terminology will also need to be consistent with a national cyber incident management framework under development by PS as part of its emergency management remit, and with this MoU. Revisions will help to underpin the collaboration among Shared Services Canada, PS, CSEC, and Treasury Board Secretariat (TBS) and support the MoU.

Cooperation Principles in Relation to Cyber Security Roles

The cooperation principles outlined in Section 5 of the MoU include the creation of joint products, coordination where appropriate on international engagement activities and respect for each entity to maintain domestic non-government relationships and related

information sharing. In all of these areas GC CTEC and CCIRC have made good progress in meeting the functional and underlying intent described in the MoU.

- *Creation of joint products:* GC CTEC and CCIRC generate different products and these are shared between them. Emerging or urgent developments that warrant broad notification are prepared collaboratively to ensure that maximum analysis supports the advice. This ongoing process will continue to evolve as each team expands products and services and overall capacity.

- *International engagement:* Both parties have worked to coordinate their respective frequent and regular interactions with international partners. In addition, GC CTEC and CCIRC have had joint representation at international meetings during this first year which has been to the benefit of both parties. This close coordination on an ongoing basis is more effective in a dynamic partner environment than relying on a static Statement of Intent.

- *Domestic non-government engagement:* As part of CSEC's and PS' broader roles and responsibilities, there are operational divisions within each organization other than CCIRC and GC CTEC that regularly engage non-federal partners, including the private sector. While GC CTEC and CCIRC confer on developments and engagements with non-federal partners, it is recognized that there is a need for more regular and timely awareness and/or context across the two organizations in instances where specific cyber security discussions are at play to prevent potential confusion, especially during response to a significant cyber incident.

- There is a recognized need to improve mechanisms for more regular sharing of highly sensitive information.

s.15(1) - Def
s.16(2)

- Weekly operational meetings at the Director level have been established to discuss cyber incidents of interest.

- CCIRC and GC CTEC have collaborated on the development of scenarios and conduct of cyber exercises.

- All of the above will be facilitated through cross-team integration, the first of which will be a CCIRC to be in place by fall of 2012.

Administration and Management

The MoU envisioned the creation of a Joint Senior Management Team (JSMT). Upon further consideration, the Directors General responsible for CCIRC and GC CTEC are meeting on a bi-weekly basis to exchange information, oversee interactions, and provide guidance and conflict resolution. Going forward it is recommended that the Directors

General responsible for CCIRC and GC CTEC inform their respective Assistant Deputy Ministers of progress made against priorities and work plans.

Activities Listed in Annex B of the MoU

All of the activities identified in Annex B of the MoU have been commented on elsewhere in this document save the implementation of a communications plan. However, the transition was communicated through multiple channels including email announcements and presentations made to key government IT stakeholders at various levels. Government websites are also being updated.

CHANGES IN GOVERNMENT

Since the signing of the MoU, there have been changes within the Government cyber operations landscape.

Governance

- A committee of Deputy Ministers was established.
- The Directors General Cyber Operations Group (DG Cyber OPS), consisting of representatives of PS, CSEC, the Royal Canadian Mounted Police, and the Canadian Security Intelligence Service, was established and meets regularly on broader issues concerning cyber incident management functions within Government.

Creation of Shared Services Canada

- On August 4, 2011, the Government of Canada announced the creation of Shared Services Canada, a singular entity under which the consolidation of federal information technology management would occur. The role of SSC in IT and cyber incident management will be articulated in the revised IMP.

Revision of the IMP

- The IMP is being revised by TBS and will reflect this MoU.

Public Safety Organizational Changes

- On November 14, 2011 CCIRC transitioned from the Operations Directorate of the Emergency Management and Regional Operations Branch to the National Cyber Security Directorate of the National Security Branch. The recommended change to Annex A reflects this reporting change.

OVERALL ASSESSMENT

GC CTEC and CCIRC have made great progress on meeting the requirements and cooperation principles outlined in the MoU. There are some improvements that can be made as noted in the recommendations below.

RECOMMENDATIONS

1) Confer on the Director General, National Cyber Security, the responsibilities attributed to the Director General Operations as noted in Section 6(2) for PS.

2) Ensure that by November 30, 2012, GC CTEC and CCIRC standard operating procedures are amended to provide the necessary information-sharing guidance to staff.

3) Use the upcoming [redacted] to inform future considerations for additional i[redacted] collaboration. A report will be provided to Directors General six months following the start date of the [redacted]

s.15(1) - Def
s.16(2)

4) A review of this MoU is recommended in fiscal year 2014/15 when SSC will have begun operating the FIPC.

5) [redacted]

6) [redacted]

ACTION PLAN

The responsible Assistant Deputy Ministers have accepted the results of this review and agree to implement all of its recommendations upon approval of the Deputy Ministers.

8 May 12

Toni Moffa
Deputy Chief, IT Security
Communications Security Establishment
Canada

2012 05 08

Lynda Clairmont
Senior Assistant Deputy Minister,
National Security
Public Safety Canada

Approved by:

John Forster
Chief
Communications Security Establishment
Canada

MAY 11 2012

Graham Flack
Acting Deputy Minister
Public Safety Canada

ORIGINAL DOCUMENT

Memorandum of Understanding Between The Communications Security Establishment Canada and Public Safety Canada Concerning Cyber Security Roles and Responsibilities

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

AND

PUBLIC SAFETY CANADA

Collectively referred to as the "Participants"

CONCERNING CYBER SECURITY ROLES AND RESPONSIBILITIES

1 PURPOSE

1.1 This Memorandum of Understanding (MoU) between the Communications Security Establishment Canada (CSEC) and Public Safety Canada (PS) delivers on the commitments in Canada's Cyber Security Strategy to secure Government of Canada (GC) systems and vital systems outside the Government by establishing a general framework arrangement which sets out the cooperation principles that guide the realignment of cyber security roles between the Participants and specifically the transfer of responsibilities of cyber incident management for Government of Canada networks from PS to CSEC.

1.2 Going forward, this MoU sets out the division of cyber security roles and responsibilities:

1.2.1 CSEC will perform cyber security operations and cyber incident management for electronic information and infrastructures of importance to the Government and shall hereafter refer to this undertaking as 'Government of Canada Cyber Threat Evaluation Centre' or 'GC CTEC.'

1.2.2 PS will perform cyber security management in the non-federal domain, which generally comprises provinces, territories and industry, and shall hereafter refer to this undertaking as 'Canadian Cyber Incident Response Centre' or 'CCIRC.' PS will perform the lead role in circumstances where cyber security management requires coordination across federal and non-federal domains.

1.3 This MoU acknowledges that the Participants share a common interest in close cooperation, consultation and coordination in accordance with strategic priorities and respective mandates.

1.4 Should other arrangements, including Memoranda of Understanding, be concluded between CSEC and PS pursuant to this MoU, they are to be considered annexes and set out in a list at Annex A.

2 MANDATES

2.1 CSEC is mandated in the *National Defence Act* (NDA) to provide foreign intelligence in accordance with Government of Canada intelligence priorities, to help protect electronic information and information systems of importance to the Government of Canada and to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. CSEC is the technical authority for information technology security within the Government as per the Policy on Government Security (PGS).

2.2 As directed in the *Emergency Management Act*, the Minister of PS exercises leadership relating to emergency management in Canada, which includes cyber incident management, by coordinating emergency management activities among government institutions and in cooperation with the provinces and other entities, including the provision of information to partners and other activities in support of mitigation, preparedness, response and recovery. Canada's Cyber Security Strategy designated the Minister of PS the federal coordination lead for cyber security and set out a long term framework for uniting the Government's cyber security activities.

3 BACKGROUND

3.1 Cyber threats have expanded in intensity and complexity, affecting commerce, intellectual property, critical infrastructure, government operations, delivery of government services to Canadians and the daily lives of Canadians. These threats are increasingly characterized by blurred distinctions between geographic boundaries, state and non-state actions, and law enforcement and defence/intelligence realms. Measures taken by Canada and Allies include enhanced intra-government and inter-government coordination on cyber security and strengthened policy and technical capacities to detect, defend and respond to cyber threats.

3.2 To remain effective in the face of these complex security threats and rapidly changing technology, Canada's security and intelligence community seeks to improve the results of its activities, including enhanced coordination, cooperation and appropriate information sharing among its members. Accordingly, CSEC and PS have developed a multi-faceted relationship that encompasses interactions across many levels in both organizations. Specifically, the institutional relationship exists in three aspects:

3.2.1 Information sharing on cyber security matters, situational awareness, and respective international cyber security relationships;

3.2.2 PS Information Protection Centre within the CIO organization as a client of the CTEC at CSEC; and

3.2.3 CSEC as an active contributor to the policy and coordination role played by PS in many areas such as achieving the objectives in Canada's Cyber Security Strategy.

3.3 The PGS designated CSEC as the National Authority for SIGINT and COMSEC and assigned responsibility to CSEC for providing leadership and coordination of departmental activities that help ensure the protection of electronic information and information systems of importance, including developing policy instruments on information technology security for approval by the Treasury Board Secretariat (TBS), providing advice and guidance to departments on the Government's Information Technology (IT) infrastructure, providing services to departments for handling and mitigation of sophisticated IT security incidents and representing the Government on national and international initiatives related to IT security and SIGINT.

3.4 Government institutions manage national security and other activities based on their own authorities, but must also implement the processes outlined in the Federal Emergency Response Plan (FERP), which defines the structures and processes to be used to ensure a whole-of-government response to natural and man-made hazards as well as national security events such as acts of terrorism and cyber events.

3.5 The Government's IT Incident Management Plan (IMP) lays out the Government's processes and identifies departmental roles and responsibilities for reporting actual and potential incidents and for reporting when Government services and operations are interrupted or are otherwise affected by an IT incident.

4 TRANSFER OF RESPONSIBILITIES OF CYBER INCIDENT MANAGEMENT FOR GOVERNMENT NETWORKS

4.1 Transfer of responsibilities of cyber incident management for Government networks from CCIRC to GC CTEC will be effective on 20 June, 2011.

4.2 There will be no transfer of equipment, staff, budget, financial resources or obligations and liability from any legally binding agreements that CCIRC has entered into with other entities prior to 20 June, 2011.

4.3 This arrangement will not transfer Ministerial Responsibilities such as contemplated by the *Public Service Rearrangement and Transfer of Duties Act*, R.S., 1985, c. P-34.

4.4 The Participants acknowledge the following roles as they relate to cyber security management, effective 20 June, 2011:

GC CTEC

4.4.1 GC CTEC is the point of contact for cyber security operations, cyber incident management and source of IT security advice for electronic information and infrastructures of importance to the Government, including entities under Schedule I, I.1, II, III, IV and V of the *Financial Administration Act*.

4.4.2 GC CTEC is responsible for cyber incident management for the Government, including the provision of mitigation advice and the issuance of alerts and notifications to the Government.

4.4.3 GC CTEC provides diagnostic, analytical assistance and expert technical support to CCIRC upon request as priorities and resources permit.

CCIRC

4.4.4 CCIRC is the point of contact and source of advice in the non-federal domain, including other levels of government and the private sector. This includes the provision of mitigation advice, issuance of alerts and notifications.

4.4.5 CCIRC leads public awareness and outreach activities to inform Canadians of the potential risk they face and the action they can take to protect themselves.

4.4.6 CCIRC provides information at the technical and strategic levels to various audiences, at various classification levels.

4.4.7 CCIRC conducts technical and intelligence analysis and produces and disseminates products such as guidelines, security flashes, notifications and strategic guidance for non-federal audiences.

5 COOPERATION PRINCIPLES IN RELATION TO CYBER SECURITY ROLES

5.1 The Participants acknowledge that their respective cyber security mandates are complementary and strive to leverage each other's capabilities and eliminate unnecessary duplication.

5.2 For the purposes of efficiency and consistency of messaging, the Participants intend to collaborate on the development of strategic cyber situational awareness products to be used in fulfilling their respective mandates.

5.3 The Participants acknowledge that PS leads and coordinates policy and communications for cyber security for the Government while CSEC conducts cyber security operations and acts as the technical authority for information technology security within the Government as per the PGS. Accordingly, PS is responsible for coordinating the national response to any cyber security incident while CSEC will inform PS of relevant cyber security activities coordinated through TBS CIOB with the Government CIO and IT communities, where appropriate.

5.4 The Participants acknowledge that they maintain separate relationships with the private sector and other levels of government (where applicable) in keeping with the Participants' respective legal authorities and mandates.

5.5 The Participants intend to jointly maintain relationships with international counterparts, such as organizations that serve national and government Cyber Emergency Response Team (CERT) functions, and intelligence agencies or groupings thereof (e.g., Usual 5) involved in cyber security and incident management, and to carry out these relationships in a manner that is conducive to setting forth and maintaining a coherent Government

representation with respect to cyber security and incident management in the Canadian context.

5.6 The Participants intend to provide each other with timely situational awareness of cyber security issues to enable the Participants to fulfill their respective responsibilities.

5.7 The Participants intend to develop and continually improve mechanisms to share information in a manner that is timely, cost-effective, standardized and secure, where applicable as necessary.

5.8 The Participants intend to consult each other in advance, where reasonable, on decisions and actions that impact the Participants' respective cyber security roles and responsibilities.

6 ADMINISTRATION AND MANAGEMENT

6.1 The Participants intend that the Joint Senior Management Team (JSMT), established by this MoU, will establish and oversee joint committees and working groups involving personnel from both organizations and delegate operational responsibilities to these groups as necessary.

6.2 A Joint Senior Management Team (JSMT) with representation from both agencies is comprised of:

For CSEC:	Deputy Chief, Information Technology Security (Co-Chair, JSMT)
	Director General, Cyber Defence
	Director General, Policy and Communications
	Director, Cyber Threat Evaluation Centre
For PS:	Assistant Deputy Minister, Emergency Management and National Security (Co-Chair, JSMT)
	Director General, Operations
	Director General, Communications Branch
	Director, Canadian Cyber Incident Response Centre

6.3 The goal of the JSMT is to act as the focal point for the Participants to discuss and set priorities and workplans and advance them to successful conclusion. Accordingly, the JSMT is responsible for adding, modifying and confirming priority activities identified in Annex B, and using joint delegated groups as necessary to perform priority activities and ongoing operational responsibilities.

6.4 The JSMT meets on a semi-annual basis, or more frequently if necessary.

6.5 Director, CTEC, CSEC, and Director, CCIRC, PS, will co-ordinate meetings of the JSMT and will report to the JSMT on progress and outstanding issues, providing recommendations as necessary.

6.6 The Participants intend to conduct a review of the effectiveness of this MoU six months from its effective date and produce a report for the Deputy Minister of PS and the Chief of CSEC. Thereafter, the Participants intend to monitor the performance and results of this MoU by conducting a JSMT-level review as deemed necessary by the Co-Chairs.

7 REPRESENTATION

7.1 CSEC and PS will designate Director, CTEC, CSEC, and Director, CCIRC, PS, to ensure regular and ongoing engagement on matters relating to this MoU. These representatives may establish working groups to provide recommendations on specific issues relating to the priority activities for enhanced cooperation.

8 DISPUTE RESOLUTION PROCESS

8.1 Any dispute arising from the interpretation or operation of this MoU shall be referred to the Chief, CSEC and Deputy Minister of PS for resolution.

9 FINANCIAL AND ADMINISTRATIVE ARRANGEMENTS

9.1 This MOU will not impose any financial responsibilities on its Participants, except that CSEC and PS will be responsible for any costs incurred to meet their respective administrative obligations contained within this MoU, including:

9.1.1 Maintaining secure office facilities, including the acquisition of approved security containers, telecommunications equipment, electronic equipment, room and building design; and

9.1.2 Ensuring that all personnel seeking access to either Participant's information are legally bound to keep confidences and have the appropriate security clearance.

9.2 CSEC and PS will be responsible for ensuring that financial authorities and authorizations are identified and confirmed prior to undertaking any cooperative arrangements having financial implications.

10 CONFIDENTIALITY AND USE OF INFORMATION

CSEC and PS will:

10.1 Use the information provided by the other Participant solely for the purpose for which it was provided.

10.2 Not disseminate the information to any third party without the prior written consent of the supplying Participant, except as required by law in which case prior notice must be provided where possible to the supplying Participant.

10.3 Limit access to the information to those of its employees whose duties require such access, who are legally bound to keep confidences and who have the appropriate security clearance.

10.4 Ensure that all Protected and Classified information exchanged or generated between Participants in connection with this MoU be safeguarded through the creation, maintenance, release, transmittal, transportation, declassification, handling, use, storage and disposal in accordance with the guidelines outlined in the PGS, and all relevant PS and CSEC security and information handling policies.

11 INFORMATION MANAGEMENT

11.1 The information disclosed under this arrangement shall be administered and maintained, and disposed of in accordance with the law that applies to record retention and personal information and all applicable policies and guidelines. This includes the *Privacy Act*, the *National Archives of Canada Act* and the PGS.

Each Participant will:

11.2 Promptly notify the other of any unauthorized use or disclosure of the information exchanged under this arrangement and furnish the other Participant with details of such unauthorized use or disclosure. In the event of such an occurrence, the Participant responsible for the safeguarding of the information shall take all reasonably necessary steps to limit the damage of the incident and prevent a re-occurrence. Upon request by either Participant, an investigation must take place.

11.3 Upon recognition that unauthorized use or disclosure has occurred and/or upon the request of the other participant, immediately return any such information and ensure that no copies or extracts are retained.

11.4 Immediately notify and consult the other if either receives a request under the *Privacy Act, the Access to Information Act* or other lawful authority, for information provided under this arrangement. If requested, the Participant shall endeavour to protect the information from disclosure to the extent permitted by law.

12 ACCURACY OF INFORMATION

CSEC and PS will:

12.1 Use their best efforts to verify accuracy and completeness of their information to the other Participant.

12.2 Promptly notify the other Participant if it learns that inaccurate or potentially unreliable information may have been provided or received.

13 EFFECTIVE DATE/ AMENDMENT/ TERMINATION

13.1 This MoU:

13.1.1 will enter into effect upon the signature of both Participants, the effective date being the date of the second signature;

13.1.2 upon entering into effect immediately replaces any previous Memoranda of Understanding between the Participants;

13.1.3 will be reviewed as required by the Participants to ensure that it remains current with regard to the agreed principles and expectations;

13.1.4 may be amended at any time by written agreement of both Participants; and

13.1.5 may be terminated at any time by providing, in writing, 60 days notice of intention to terminate by either Participant. Termination does not release a Participant from any obligations which accrued while the arrangement was in effect and the obligations of confidentiality shall survive the expiry or termination of this arrangement.

Signed by the authorized officers of the Participants:

John Adams
Chief
Communications Security Establishment Canada

10 Jun 2011
Date

William V. Baker
Deputy Minister
Public Safety Canada

JUN 15 2011
Date

ANNEX A

The following arrangements are annexes to this MOU:

[ed. note: items under Annex A are considered operational arrangements that may require regular updating as circumstances change, and typical level of approval for these arrangements are DG]

1.

Updated on:

ANNEX B

PRIORITY ACTIVITIES FOR ENHANCED COOPERATION

[ed. note: items under Annex B are considered ongoing areas of cooperation or items to be concluded in near future. Items in Annex B will form part of the agenda for the regular JSMT meetings between the two organizations]

1. Conduct a review of the effectiveness of this MoU as per 6.6 by January 2012.

2. Develop information sharing arrangements between GC CTEC and CCIRC as per 5.7 by 31 August 2011.

3. Develop and maintain ongoing arrangement (e.g., work plan) concerning strategic cyber situational awareness products as per 5.2.

4. Develop Statement of Intent on management of international relationships as per 5.5 by 31 August 2011.

5. Implement the Government's communications plan on implementation of transition by 31 August 2011.

Updated on: June 10, 2010

Pages 694 to / à 697

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l, 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 698

is withheld pursuant to section

est retenue en vertu de l'article

15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 699 to / à 706
are withheld pursuant to section
sont retenues en vertu de l'article

16(2)(c)

of the Access to Information
de la Loi sur l'accès à l'information