



Public Safety Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

COPY

SECRET

DATE: ~~FEB~~ **FEB 04 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

SECRET

- 2 -

- \$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 sunseting 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.


Francis Guimont

Enclosure: (1)

Prepared by: Nancy Brunet

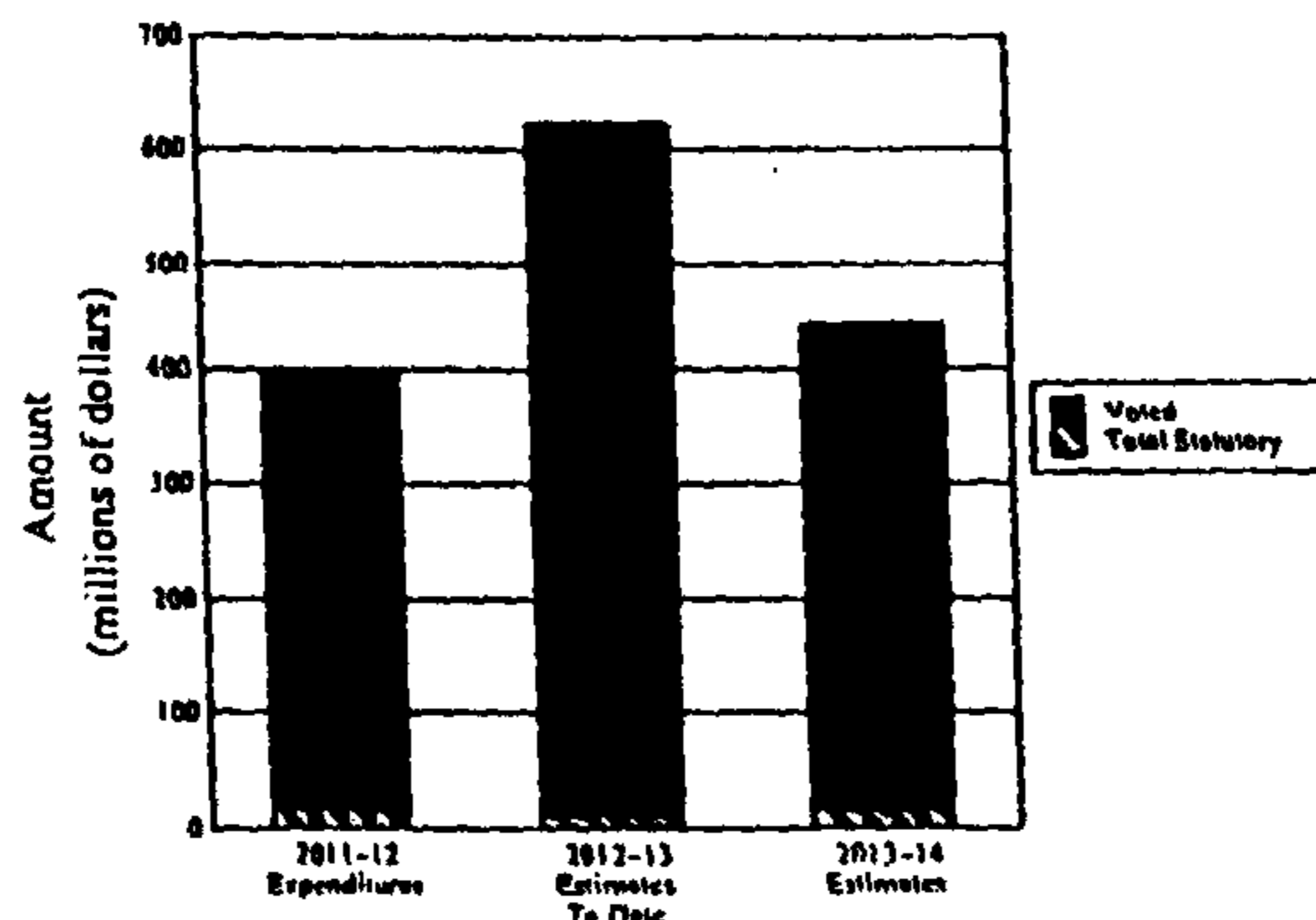
Public Safety and Emergency Preparedness

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 | 2012-13 | | 2013-14 |
|----------------------------|--------------------|--------------------|--------------------|--------------------|
| | Expenditures | Main Estimates | Estimates To Date | Estimates |
| | | (dollars) | | |
| Budgetary Voted | | | | |
| 1 Operating expenditures | 141,648,763 | 124,671,421 | 128,028,599 | 124,342,801 |
| 5 Grants and contributions | 244,162,360 | 292,939,791 | 479,440,792 | 300,623,590 |
| Total voted | 385,811,123 | 417,611,212 | 607,469,391 | 424,970,891 |
| <i>Total Statutory</i> | <i>15,753,673</i> | <i>15,133,901</i> | <i>15,133,901</i> | <i>15,970,032</i> |
| Total budgetary | 401,564,796 | 432,745,113 | 622,603,292 | 440,940,929 |

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.

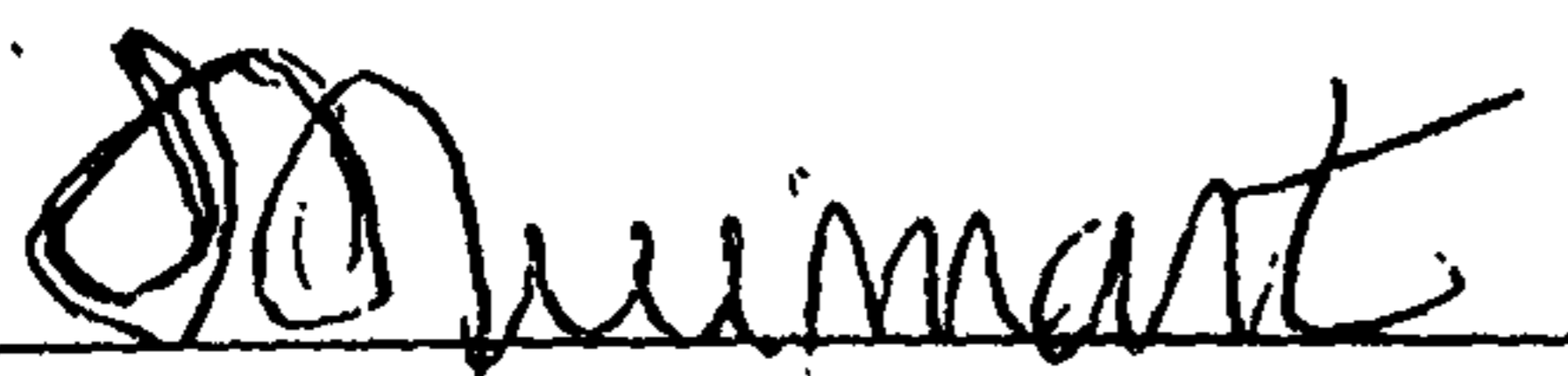
The net spending increase of \$8.2 million or 1.9 % is due to a decrease in operating funding of \$0.3 million, an increase of \$0.8 million in Employee Benefit Plans costs, a decrease in grants of \$7.7 million, as well as an increase in contributions of \$15.4 million.

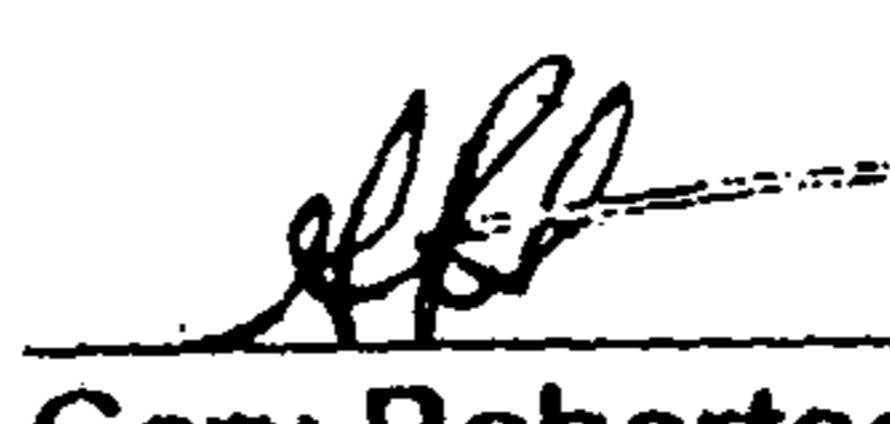
Border Strategies

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 sunseting 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 sunseting 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.

Main

| Expenditures by Strategic Outcome and Program | 2011-12 Expenditures | 2012-13 Main Estimates | 2013-14 Estimates |
|--|---------------------------------|---------------------------------------|------------------------------|
| | <i>(dollars)</i> | | |
| Budgetary | | | |
| <i>A safe and resilient Canada.</i> | | | |
| 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 |
| <i>The following program supports all strategic outcomes within this organization.</i> | | | |
| 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 | | 2013-14 Estimates |
|---|-------------------------|--------------------|--|----------------------|
| | | Main Estimates | Estimates To Date | |
| | | (dollars) | | |
| Grants | | | | |
| Grants in support of the Safer Communities Initiative | 939,518 | 3,460,000 | 3,460,000 | 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 | 500,000 |
| 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 78,484,148 | 105,184,330 |
| Contributions to the provinces for assistance related to natural disasters | 99,970,212 | 100,000,000 | 280,000,000 | 1,000,000,000 |
| Contributions in support of the Safer Communities Initiative | 42,279,554 | 40,139,899 | 40,139,899 37,650,899 | 38,984,516 |
| Financial Support to Provinces and Territories for 2011 Flood Mitigation Investments | | | 50,000,000 | 50,000,000 |
| Biology Casework Analysis Contribution Program | 6,900,000 | 6,900,000 | 6,900,000 | 6,900,000 |
| Kanishka Project Research Initiative Contribution Program to Combat Child Sexual Exploitation and Human Trafficking | 48,637 | 500,000 | 500,000 | 2,146,000 |
| Aboriginal Community Safety Development Contribution Program | 1,924,365 | 1,975,600 | 1,975,600 | 2,055,600 |
| International Association of Fire Fighters, Canada | 541,903 | 690,000 | 690,000 | 690,000 |
| 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 | 410,775 | 500,000 | 500,000 | 500,000 |
| | 863,443 | 877,000 | 877,000 617,000 | 362,000 |
| Total Contributions | 232,444,696 | 272,816,647 | 502,816,647 459,317,647 | 294,672,446 |
| Total of listed Transfer Payments | 235,680,357 | 278,572,791 | 509,073,791 465,073,791 | 300,628,590 |

2013-14 Main Estimates

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 | <p>Public Safety and Emergency Preparedness – Operating expenditures and, pursuant to paragraph 29.1(2)(a) of the <i>Financial Administration Act</i>, 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 <i>Salaries Act</i>, as adjusted pursuant to the <i>Parliament of Canada Act</i> and pro rata for any period of less than a year</p> <p>No additional twelfths beyond the normal three-twelfths</p> | 124,342,301 | 31,085,575.25 |
| 5 | <p>Public Safety and Emergency Preparedness – The grants listed in the Estimates and contributions</p> <p>No additional twelfths beyond the normal three-twelfths</p> | 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 <i>Financial Administration Act</i> , 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 <i>Salaries Act</i> , as adjusted pursuant to the <i>Parliament of Canada Act</i> 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 (dollars) | 2013-14 |
|--|-------------------------|--|------------|
| | | | Estimates |
| Budgetary | | | |
| Public Safety and Emergency Preparedness | | | |
| Contributions to employee benefit plans | 15,676,137 | 15,056,385 | 15,360,980 |
| Minister of Public Safety – Salary and motor car allowance | 77,536 | 77,516 | 79,102 |

Main

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.msrc-pwssc.gc.ca/rccrcn/pceaf-gwcpa/11127-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

| Budgetary | 2012-13 | | 2013-14 ^{Min} Estimates | | | | Total |
|--|----------------------|--------------------|----------------------------------|--------------|--------------------|-------------------------------|--------------------|
| | 2011-12 Expenditures | Main Estimates | Operating | Capital | Transfer Payments | Revenues and other reductions | |
| Public Safety and Emergency Preparedness | | | | | | | |
| <i>A safe and resilient Canada.</i> | | | | | | | |
| 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 |
| <i>The following program supports all strategic outcomes within this organization.</i> | | | | | | | |
| 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

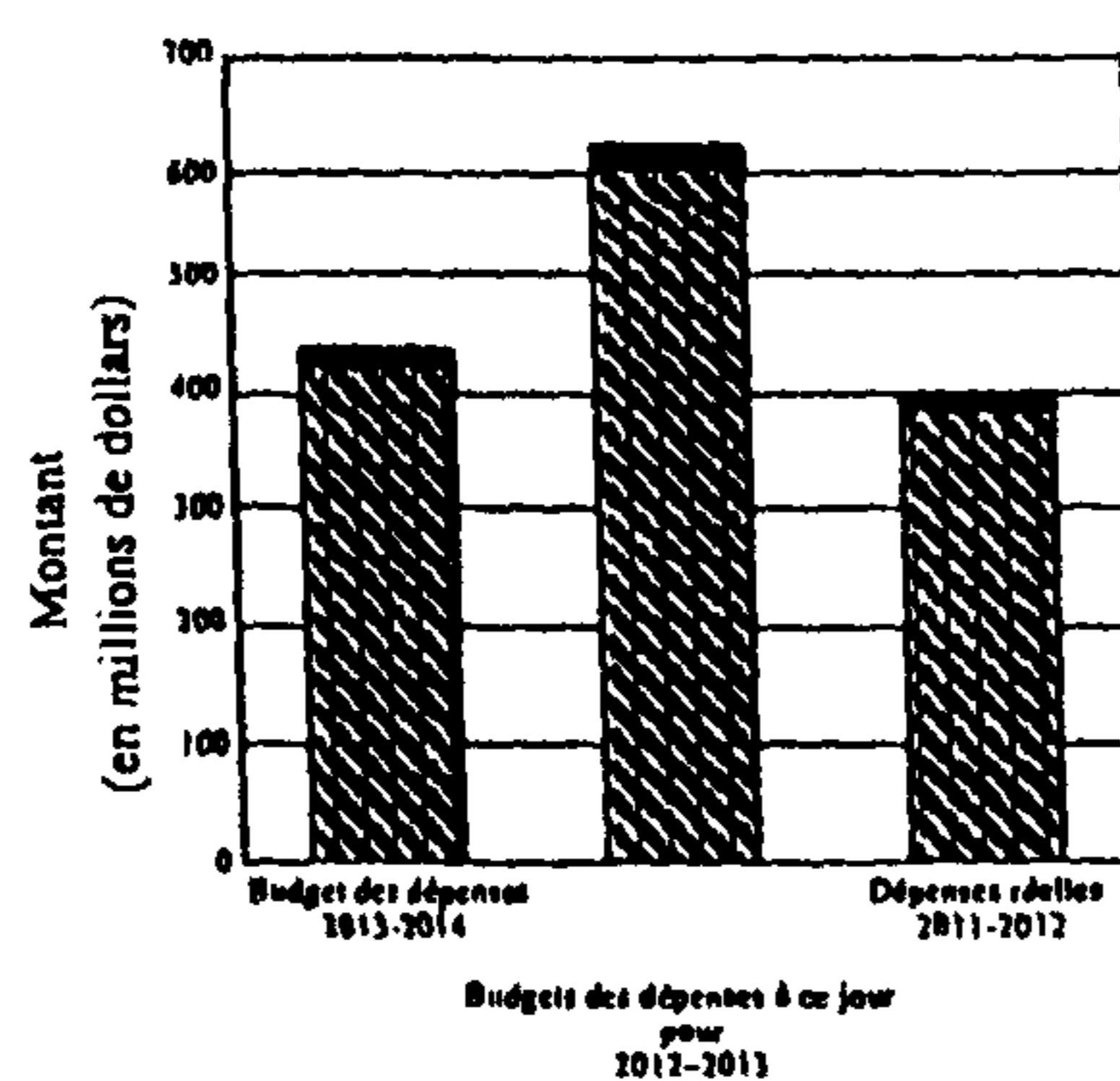
Raison d'être

→ 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

à ce jour principal

| | Dépenses réelles | | 2012-2013 | | Budget des dépenses 2010-2014 |
|---------------------------------------|--------------------|-------------------------------|---------------------|--------------------|-------------------------------|
| | 2011-2012 | Budget principal des dépenses | Budget des dépenses | | |
| | (dollars) | | | | |
| Budgétaire | | | | | |
| Crédits votés | | | | | |
| 1 Dépenses de fonctionnement | 141 648 763 | 124 671 421 | 128 028 599 | 124 542 201 | |
| 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 | 425 170 791 | |
| Total des postes législatifs | 15 753 673 | 15 133 901 | 15 133 901 | 15 133 901 | |
| Total des dépenses budgétaires | 401 564 796 | 432 745 113 | 622 603 292 | 440 304 692 | |

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 augmentations 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 le 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

| | Dépenses réelles 2011-2012 | 2012-2013 Budget principal des dépenses | Budget des dépenses 2013-2014 |
|---|-------------------------------|---|-------------------------------------|
| | (en dollars) | | |
| Budgétaire | | | |
| <i>Un Canada sécuritaire et résilient.</i> | | | |
| Lutte au crime | 170,120,151 | 209,999,507 | 189,707,922 |
| Gestion des mesures d'urgence | 143,734,990 | 139,597,608 | 66,255,003 |
| Sécurité nationale | 17,685,107 | 23,601,714 | 25,247,356 |
| Stratégies frontalières | 2,946,130 | 2,522,140 | 2,977,690 |
| <i>Le programme suivant appuie tous les résultats stratégiques de cette organisation.</i> | | | |
| Services internes | 67,078,418 | 53,024,144 | 56,402,952 |
| Total | 401,564,796 | 432,745,113 | 440,910,923 |

Principal

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.

Partie II – Budget principal des dépenses

Sécurité publique et Protection civile

à ce jour principal

Liste des paiements de transfert

| | Dépenses réelles 2011-2012 | 2012-2013 | | Budget des dépenses 2013-2014 |
|---|-------------------------------|----------------------------------|--|-------------------------------------|
| | | Budget principal des dépenses | Budget des dépenses | |
| <i>(en dollars)</i> | | | | |
| 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 | 500 000 |
| 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 | 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 | 105 841 880 |
| 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 |

Sécurité publique et Protection civile

Partie II – Budget principal des dépenses

| Dépenses réelles 2011-2012 | 2012-2013 | | Budget des dépenses 2013-2014 |
|---|----------------------------------|------------------------|-------------------------------------|
| | Budget principal des dépenses | Budget des dépenses | |
| | <i>(en dollars)</i> | | |
| Association internationale des pompiers, Canada | 410 775 | 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 | 362 000 |
| | | 617 000 | |
| | | 459 317 647 | |
| Total des contributions | 232 444 696 | 272 816 647 | 294 672 446 |
| Total de la liste des paiements de transfert | 235 680 357 | 278 572 791 | 300 628 590 |
| | | 465 073 741 | |

2013-2014 Main Estimates

Exigences en matière de crédits provisoires

Sécurité publique et Protection civile

Articles approuvés (dollars)

| N° du crédit | Libellé de crédit et explications pour les douzièmes supplémentaires | Total du Budget principal des dépenses | Montant alloué |
|--------------|--|--|----------------|
| 1 | <p>Sécurité publique et Protection civile – Dépenses de fonctionnement et, conformément au paragraphe 29.1(2) de la <i>Loi sur la gestion des finances publiques</i>, 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 <i>Loi sur les traitements</i>, rajusté en vertu de la <i>Loi sur le Parlement du Canada</i> et au prorata, pour toute période inférieure à un an</p> <p>Aucun douzième supplémentaire n'est requis en plus des trois-douzièmes habituels</p> | 124 342 301 | 31 085 575,25 |
| 5 | <p>Sécurité publique et Protection civile – Subventions inscrites au Budget des dépenses et contributions</p> <p>Aucun douzième supplémentaire n'est requis en plus des trois-douzièmes habituels</p> | 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 libellés 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 <i>Loi sur la gestion des finances publiques</i> , 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 <i>Loi sur les traitements</i> , rajusté en vertu de la <i>Loi sur le Parlement du Canada</i> 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 <i>(en dollars)</i> | Budget des dépenses 2013-2014 |
|---|-------------------------------|--|-------------------------------------|
| Budgétaire | | | |
| Sécurité publique et Protection civile | | | |
| Contributions aux régimes d'avantages sociaux des employés | 15 676 137 | 15 056 385 | 15 360 980 |
| 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.

Définitions des articles courants fournis à: <http://www.tpsgc-pwgsc.gc.ca/recgen/pccaf-gwco/11127-frs.htm>

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 | | |
| Securité 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 | 440,910,922 |

numbers are not
Formatted in French
(no comma)

BUDGET DES DÉPENSES 2013-2014

Dépenses budgétaires par résultat stratégique et programme

Budgétaire

| | <i>réelles</i> | 2012-2013 | Budget des dépenses 2013-2014 | | | | |
|---|--------------------|-------------------------------|-------------------------------|---------------------|------------------------|-------------------------------|--------------------|
| | Dépenses 2011-2012 | Budget principal des dépenses | Fonctionnement | Dépenses en capital | Paiements de transfert | Recettes et autres réductions | Total |
| Sécurité publique et Protection civile | | | | | | | |
| <i>Un Canada sécuritaire et résilient.</i> | | | | | | | |
| 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 |
| <i>Le programme suivant appuie tous les résultats stratégiques de cette organisation.</i> | | | | | | | |
| 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 committed
in French (nocome)

SPEAKING POINTS

Minister of Public Safety at the Halifax Security Forum

“Automated or Automatic: Cyber, Drones and the Future of Modern Warfare”

- I’m happy to be able to address this topic, as cyber security – which to most people means cyber insecurity – is something which affects all Canadians.

- Now, I don’t want to take issue with the title of the panel, but I’d like to do some context setting on cyber and what it means and why it matters.
 - And why people should care about it.

- Cyberspace has quickly emerged as something which underpins all aspects of modern life, from communication and the digital economy, to social interaction, to coordinating airline traffic, the management of power grids or other aspects of our critical infrastructure.

The Threats

- But cyberspace is not without its threats

- Cyber threats against government are reasonably well known, espionage from foreign states looking to secure diplomatic or military secrets for their own advantage.

- We are seeing an increasing rise of cyber threats against private sector interests – our companies, our universities, our researchers.
 - These are not discussed much but are getting to be better known.

- Finally, we have threats against individuals, that is, cyber crime. We have fraud, and identity theft and cyber bullying and the exploitation of children online.

- These are all cyber threats. They share the same vector, and in some ways, they even use the same tools to seek their goals.
 - They exploit our reliance on technologies, and they exploit the fact that not all of us are experts in using it.

- They exploit the speed and the anonymity to hide, and they exploit its global nature to try and frustrate bringing those responsible to account.
- And to be effective, our response to these threats need to be addressed as part of cohesive approach, which we are doing in Canada and which I will discuss in a minute.

Cyber: Its people not robots

- But before that, I should also say what these cyber threats are not: they are not automatic nor really are they automated.
- These threats come from people.
- Someone designs the software, spends time, effort and money building it, someone decides they will direct a cyber attack at a bank or a government or at hospital records, and someone starts the attack.
- These are decisions made by people for very human motivations.
- Those launching these attacks want to secure an advantage, be it in the marketplace, at the negotiating table or on the battlefield.

- And while not everyone may understand what a DDOS (“dee-doss”) is, or what a botnet does....
-they know that they expect their Government to help keep them safe.

Cyber Security Strategy

- So this is where Canada’s Cyber Security Strategy comes in.
- I released Canada’s Strategy in 2010, and it is a whole of Government approach led by Public Safety Canada.
- But like the Internet itself, it relies on connectivity to be successful.
- And that is based on one simple fact, Government cannot do cyber security all by itself
 - Not in Canada not anywhere else in the world.
- So our Strategy relies on connectivity.
- It relies on engaging our private sector to share threat information and make sure they have the best data they need to guide their practices.

- We are using the organizations established by the Critical Infrastructure Strategy to do this whenever possible, but we have also put in place new structures for things like telecommunications operators.
- It relies on connecting to the provincial and territorial governments, who regulate or even own the critical infrastructure that we all rely on.
 - By focusing the mandate of the Canadian Cyber Incident Response Centre on serving private sector and infrastructure stakeholders we are doing just that.
 - And we have recently increased the capacity of the Centre to assist that client base by expanding its hours and days of operations.
- The Strategy relies on connecting to Canadian researchers who are not only developing the next generation of technologies and solutions, but are also developing the next generation of experts.
- It relies on connecting internationally; to have partners in ensuring the cyberspace we all use is secure, open and the source of economic prosperity.

- We are doing this by working with traditional defence and security allies in NATO and elsewhere.
- We are working to have Canada ratify its signature to the Council of Europe Convention on Cybercrime – the Budapest Convention - and have the RCMP joint three dozen other national police forces in this fight.
- And the Strategy involves connecting with Canadians to get them the information they need to better keep themselves and their families safe.
 - And for this we have our GETCYBERSAFE.CA campaign.
- This year, Public Safety Canada has partnered with the Stop-Think-Connect campaign run by a not-for-profit group consisting of many of the biggest Internet and security firms in the U.S., almost all of whom operate in Canada and were eager to partner with us
- And the Strategy sets objectives in each of those connectivity and partnership areas.
- *But in none of those areas can Government do it alone. Cyber security is a shared responsibility.*

Getting the balance right

- Besides connections, cyber security relies on balances.
- You need to balance economic security with national security.
- You need to balance the need for protecting ourselves against letting cyberspace grow and be open
- The best most secure system is the one without any users.
- Some countries are going the route of restricting the internet or monitoring everything their people do online....
- You get greater security but you give up all those things which made cyberspace work, and which has made it the source for innovation and growth it is.
- We need to balance the desire from a company for trying protect its market share and investors by not admitting its been victimized, with the greater god of coming forward – even if only in a classified setting -- to talk about how they were attacked, so Government can help others take steps to defend themselves.

- You need to balance the global with the local.
 - Our diplomats and some officials from my Department are working as part of a fifteen national panel convened by the UN Secretary General to offer advice on cyber security.
 - This could help bring positive change to the threat environment we all share, but Canadians also want to know they are secure at home.
- And maybe you need to balance the offence with the defence.
 - I'm not here to speak to that, however
 - So we will all have to wait to hear what the General has to say on the subject.
- I will say though that we need to balance the proactive with the reactive.
 - Canadians don't just expect that government will investigate a cyber incident, they expect these incidents shouldn't happen at all.
- As I said when I started, they expect governments to keep them safe.

- Lastly, we need to be able to adapt. In short, we need to balance the present with the future
- We need to balance the ideas and the plans we have with the flexibility we will surely need.

Conclusion

- So hopefully I've helped you see how cyber security is about connections, and about getting that balance right.
- And both of those things will require investment, constant attention, effort and fine tuning.
- Canadians need the assurance they will be safe, our allies need to know Canada can be trusted with their secrets, and our businesses need to know that their hard work will be protected and that Canada is the place where they want to invest.
- Cyber security is already seen by some of these audiences as too costly and too complex or just too hard.

- And maybe that would be true, if we really were facing hyper intelligent machines or science fiction villains, as suggested by the panel name.
- But we aren't.
- We are dealing with people at the other end of a keyboard.
- And while we don't always know who they are – although it is certainly getting harder for them to hide – we know what they want.
- And we have some practical things we can do to make sure they don't achieve their goals
- We can make it so difficult, and so time consuming and so expensive for them that Canada and Canadians are not their targets.
- And then we can work with friends and allies to make that situation the new global standard.
- And while we will never get to one perfect solution, I think we can get to a world where cyber security is talked about in the affirmative.
- It won't be something we worry we don't have, it will be something we know we have worked hard to achieve.

- And I am proud to be leading those efforts in Canada.

With that, I thank you for the opportunity to speak today, and look forward to questions.

UNCLASSIFIED

DATE:

File No.: 391514

RDIMS No.: 723805

MEMORANDUM FOR THE MINISTER

**THE CANADIAN CYBER INCIDENT RESPONSE
CENTRE'S QUARTERLY CYBER OPERATIONAL SUMMARY**

(Information only)

ISSUE

As requested by your office, please find attached the Canadian Cyber Incident Response Centre's (CCIRC) second iteration of the Quarterly Cyber Operational Summary (QCOS), covering the July to September 2012 reporting period (**TAB A**).

BACKGROUND

The QCOS is part of a suite of professional products and provides decision makers with relevant cyber information including products and services provided by CCIRC, noteworthy incidents, and trends. It was released to federal, provincial, territorial, and municipal governments as well as approximately 140 partners in the private sector.

CONCLUSION

Should you require additional information, please do not hesitate to contact me or Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.

François Guimont

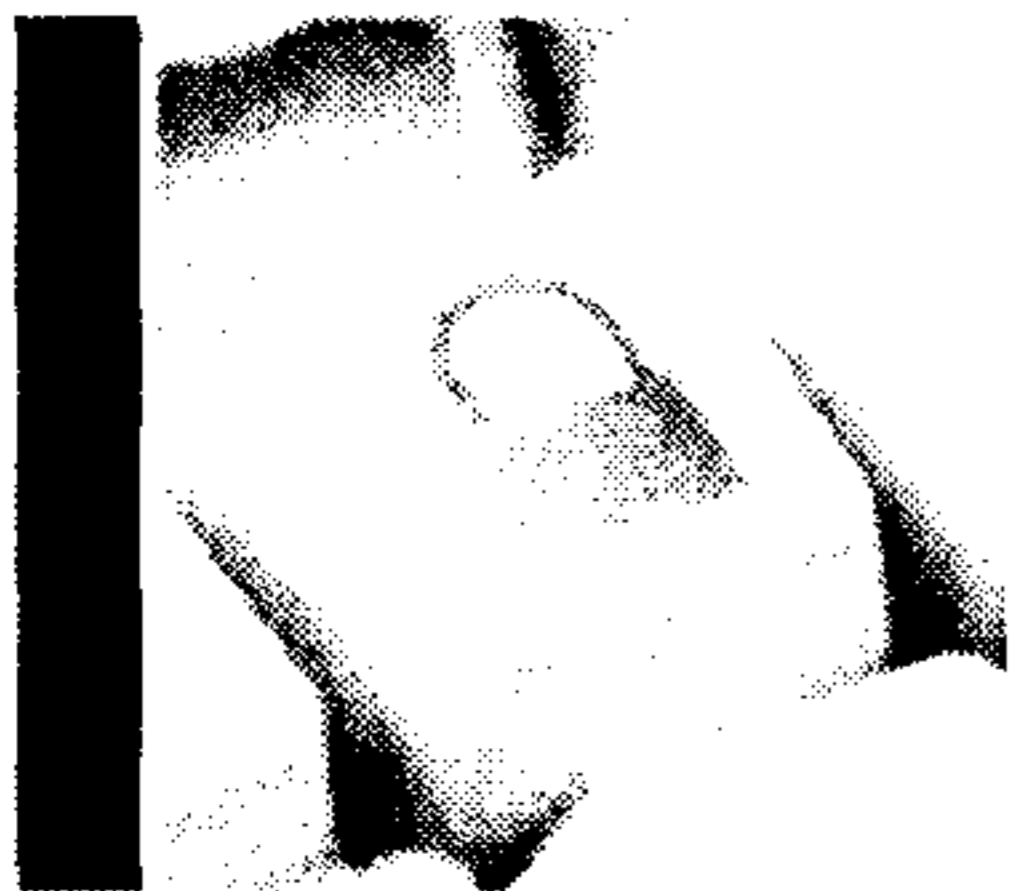
Enclosure: (1)

Prepared by: Nate Klassen



Public Safety
Canada

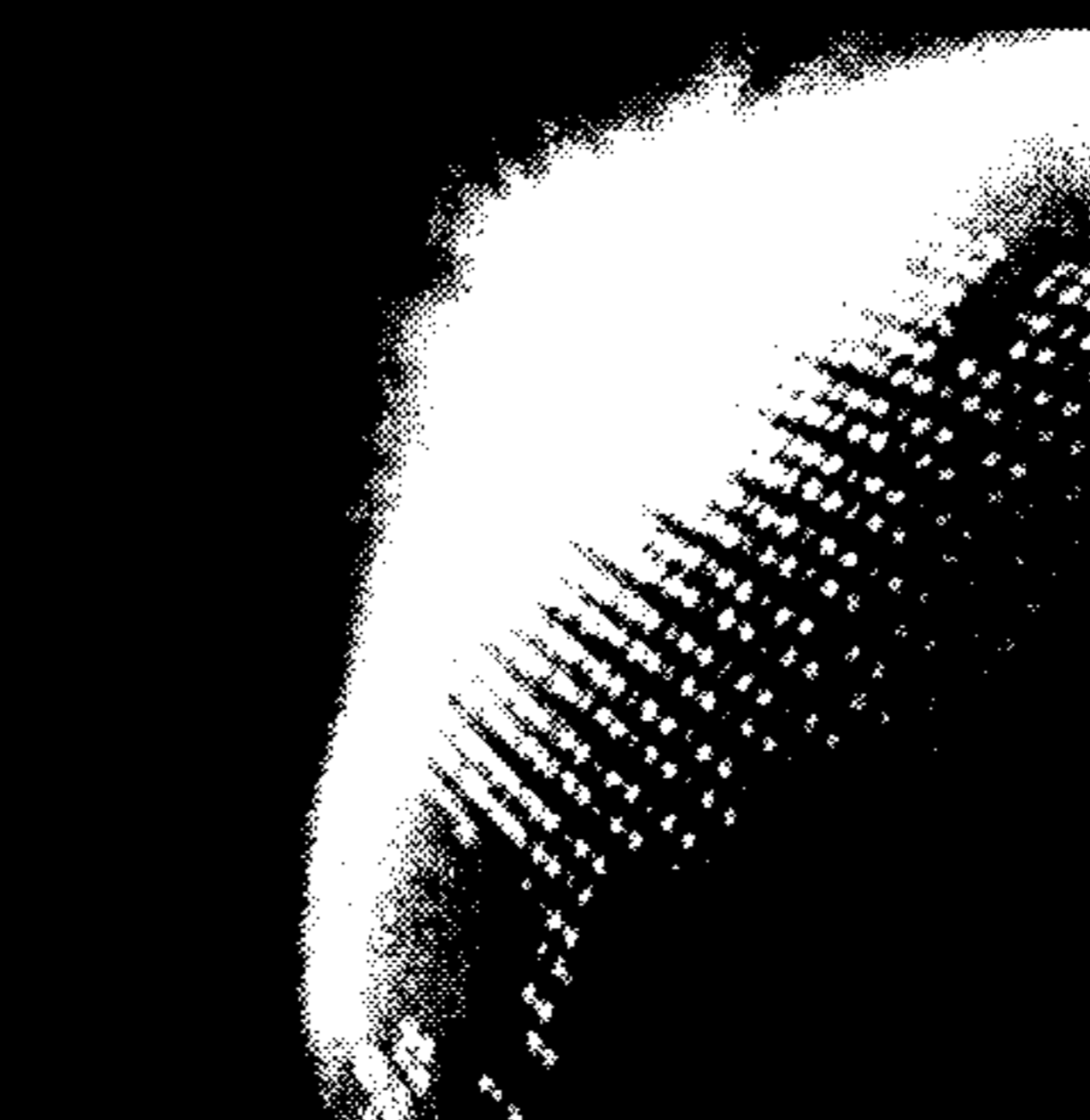
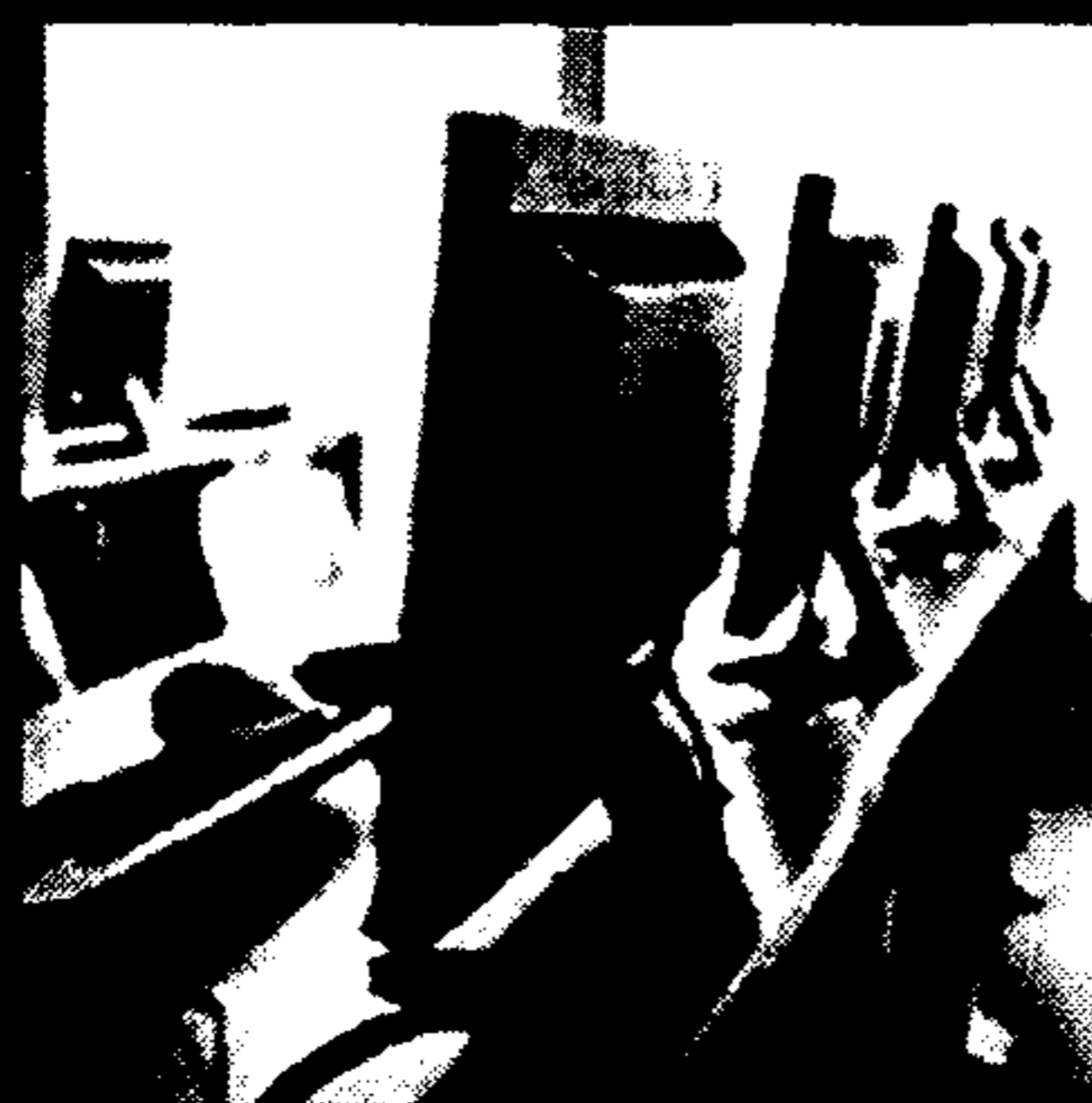
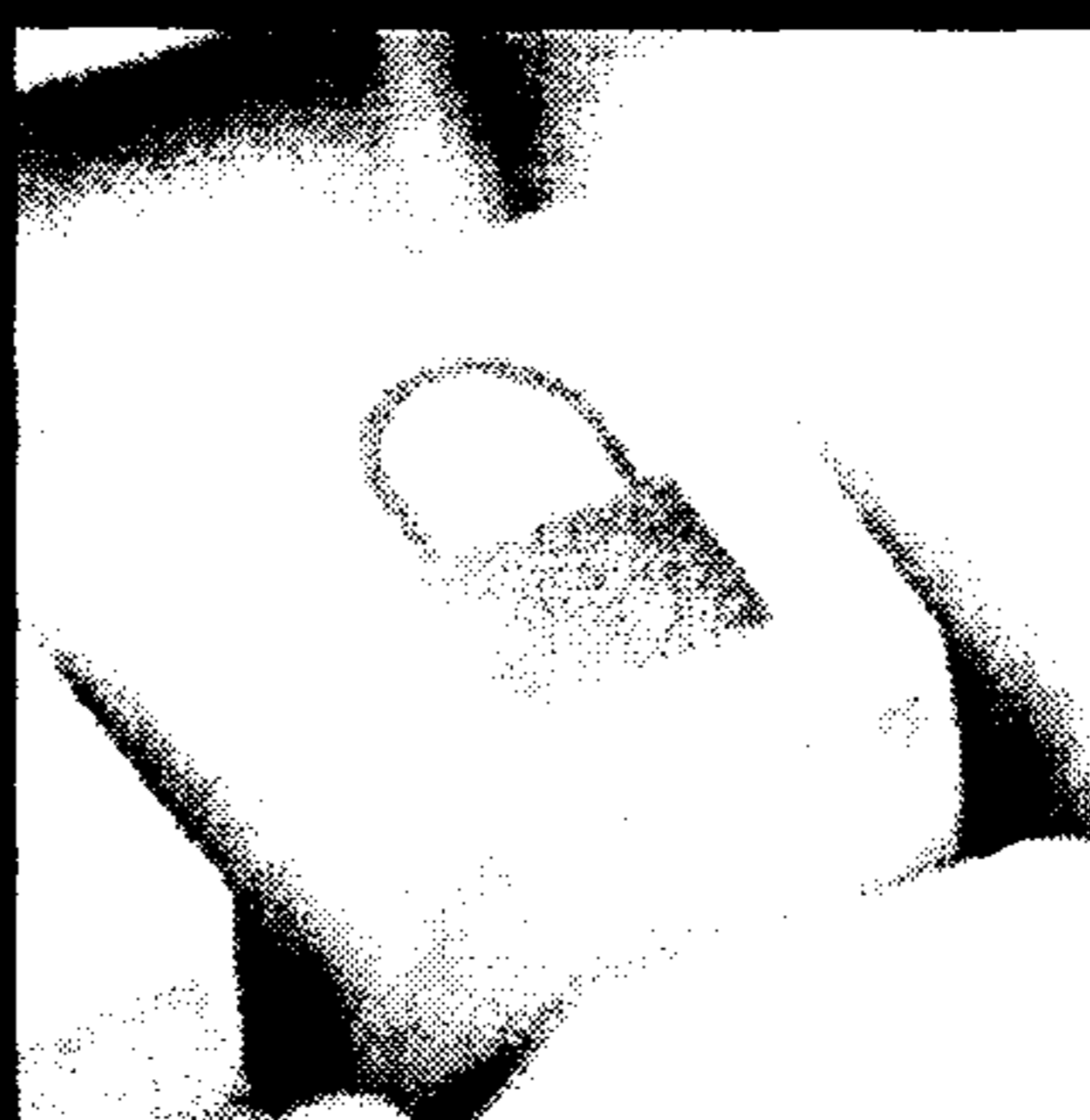
Sécurité publique
Canada



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

Partnering to Secure Vital Cyber Systems



Quarterly Operational Summary – July to September

Public Safety Canada

This document provides a quarterly summary of the cyber incidents observed by the Canadian Cyber Incident Response Centre (CCIRC).

DISCLAIMER

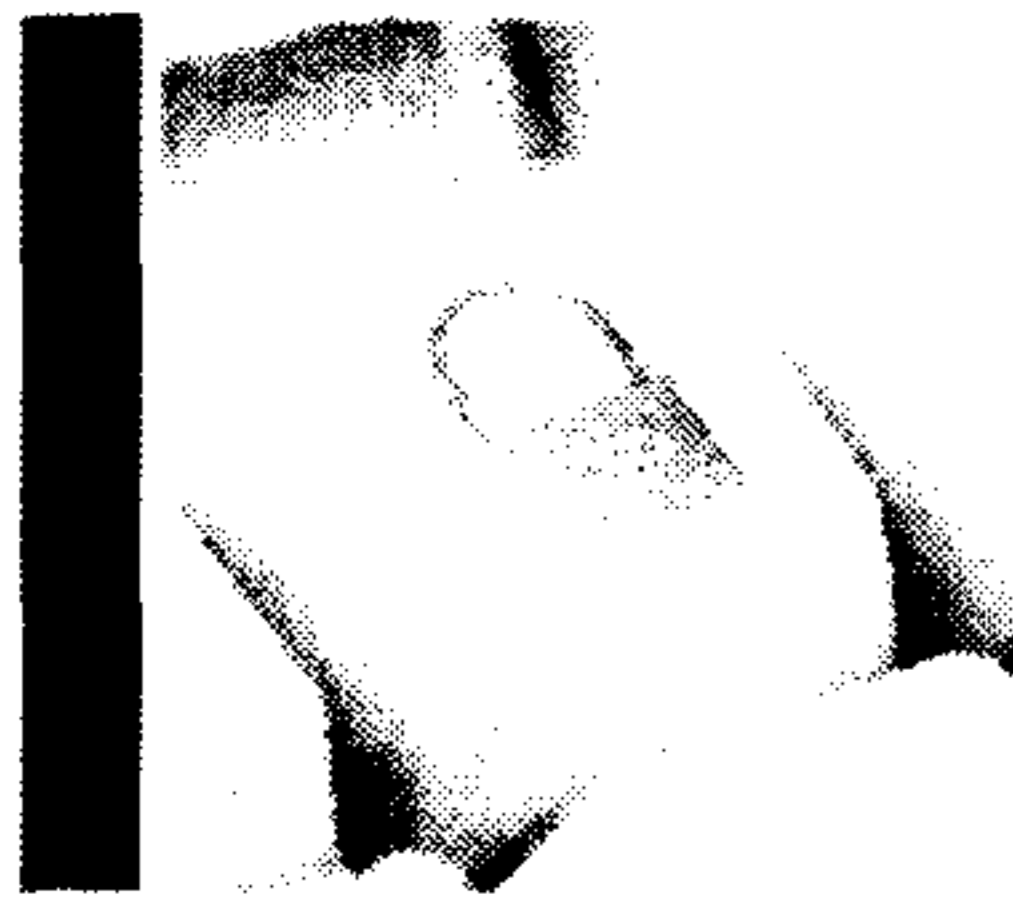
This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. CCIRC is continually working to improve the accuracy of its statistics. As it launches new products, some variations may appear in the presented statistics.

REPORTING CYBER INCIDENTS

Private or public sector partners wishing to report incidents may send an email to cyber-incident@ps-sp.gc.ca using CCIRC's Cyber Duty Officer PGP encryption key, found here: <http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx>.

FEEDBACK

This is a newly developed product. Your feedback is critical to making this product more useful. As such, please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.



CCIRC

Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

TABLE OF CONTENTS

| | |
|---|----|
| Table of Contents | 2 |
| Purpose | 3 |
| Executive Summary..... | 3 |
| Products | 4 |
| Services | 5 |
| Noteworthy Incidents | 6 |
| Trend Analysis | 8 |
| CCIRC Incidents..... | 8 |
| Trends Observed by CCIRC | 9 |
| Emerging Trends..... | 10 |
| Reports Received..... | 10 |
| Published Threat Reports..... | 11 |
| About CCIRC | 12 |
| Annex A – Definitions..... | 13 |
| Annex B – Top 35 Recommended Mitigation Actions | 14 |



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

PURPOSE

This product discusses cyber incidents the Canadian Cyber Incident Response Centre (CCIRC) observed during the July to September 2012 reporting period. Its intent is to convey information to partners in the Canadian public and private sectors about products and services CCIRC provided, noteworthy incidents, and trends.

EXECUTIVE SUMMARY

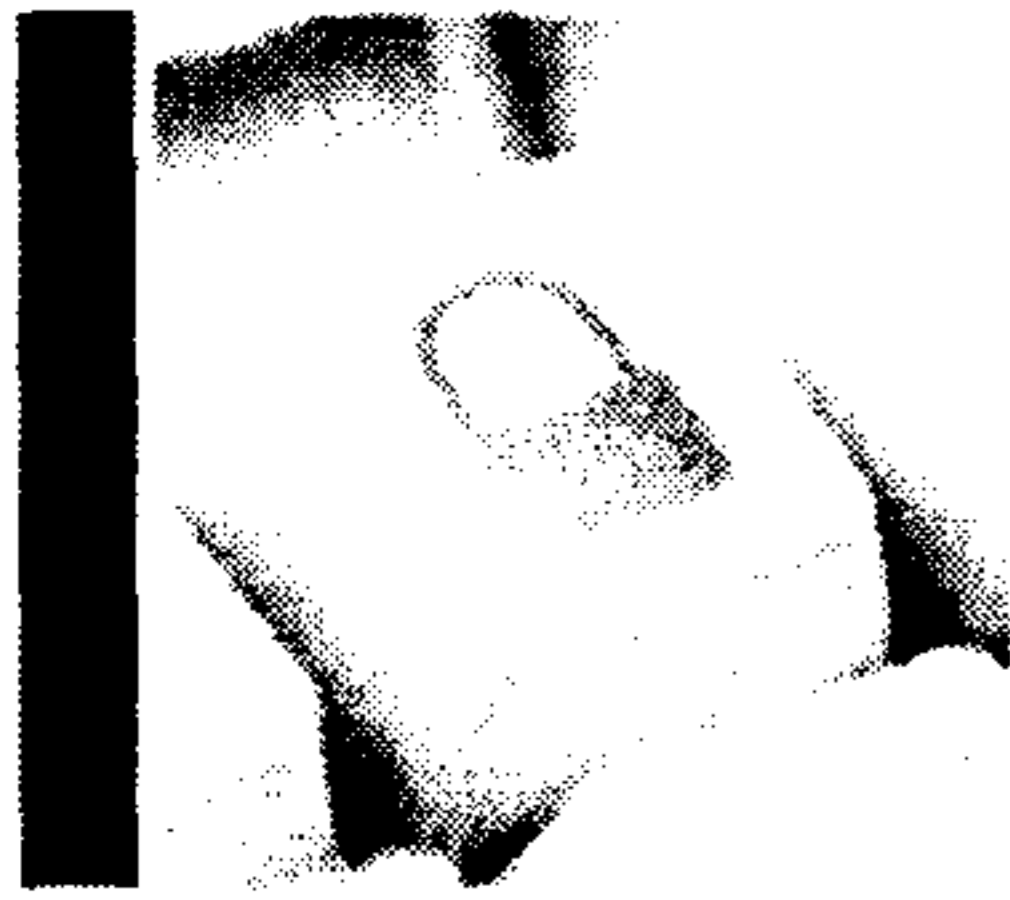
CCIRC handled 251 incidents during the reporting period. An incident is a single or series of unwanted or unexpected information security events that have a significant probability of compromising the business operations and / or the information security of cyber systems within Canadian public and private sector organizations. Malware (e.g. viruses, key loggers, and trojan horses) and phishing attacks were the most common cyber incidents, totalling 63% of the incidents observed by CCIRC. Over the reporting period, a number of significant incidents such as Microsoft Internet Explorer vulnerabilities and a cyber intrusion targeting a Canadian industrial control system manufacturer were observed by CCIRC.

The information and communication technology (ICT), government, and energy and utilities sectors were the largest observed targets of malware attacks, accounting for 66% of incidents. The high numbers associated with the ICT sector throughout this report are not necessarily indicative of the sector itself, but instead likely represent individual Canadians who use the services of these companies.

A clear trend has seen malicious individuals targeting average Canadians by impersonating financial institutions through phishing campaigns. As such, the financial sector accounted for 54% of phishing incidents seen by CCIRC. Phishing is a digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a malicious or forged website that requests information.

CCIRC's code removal requests (CRR) inform Internet service and hosting providers that they are hosting malicious content, website forgeries, and fraudulently collected personal information. Victim notifications advise partners of malware affecting them, and depending on the type, various detection and mitigation methods. The ICT and finance sectors were the most affected by cyber incidents that led to CRRs. The ICT, government, and education sectors were the largest recipients of CCIRC's 3,507 victim notifications.

Advanced persistent threats, crimeware, hacktivism and, increasingly, incidents affecting industrial control systems (ICS) were noteworthy trends observed by CCIRC. Going forward, these types of incidents will likely continue to have an impact on CCIRC's public and private sector partners.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

PRODUCTS

CCIRC issued nine advisories, one alert, seven cyber flashes (CF), and two artifact analysis reports (AAR) over this reporting period. Publically available products can be found on the [CCIRC website](#).

Advisories – CCIRC issued nine advisories to bring attention to significant upgrades and patches of common computer products such as Microsoft, Adobe, and Oracle.

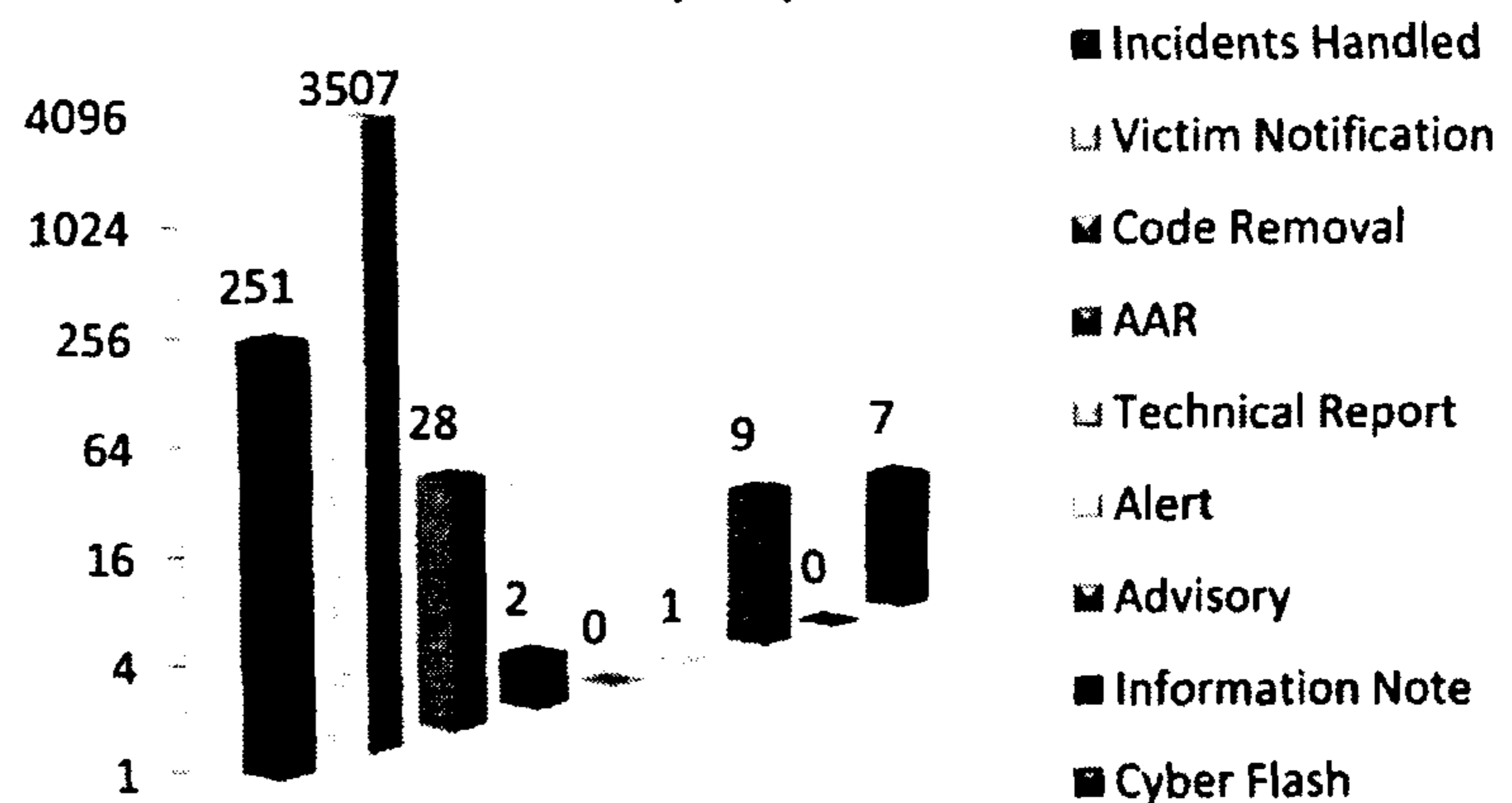
Alert – CCIRC developed one alert related to a Microsoft Internet Explorer security vulnerability.

Cyber flashes – CCIRC released seven cyber flashes providing information and mitigation advice related to: Oracle Java vulnerabilities and exploits; a phishing email campaign targeting multiple organizations; Redkit toolkit affecting critical infrastructure; Shamoon malware targeting international companies in the energy and utilities sector; an Internet Explorer Zero Day vulnerability; and, increased ZeroAccess Botnet activity.

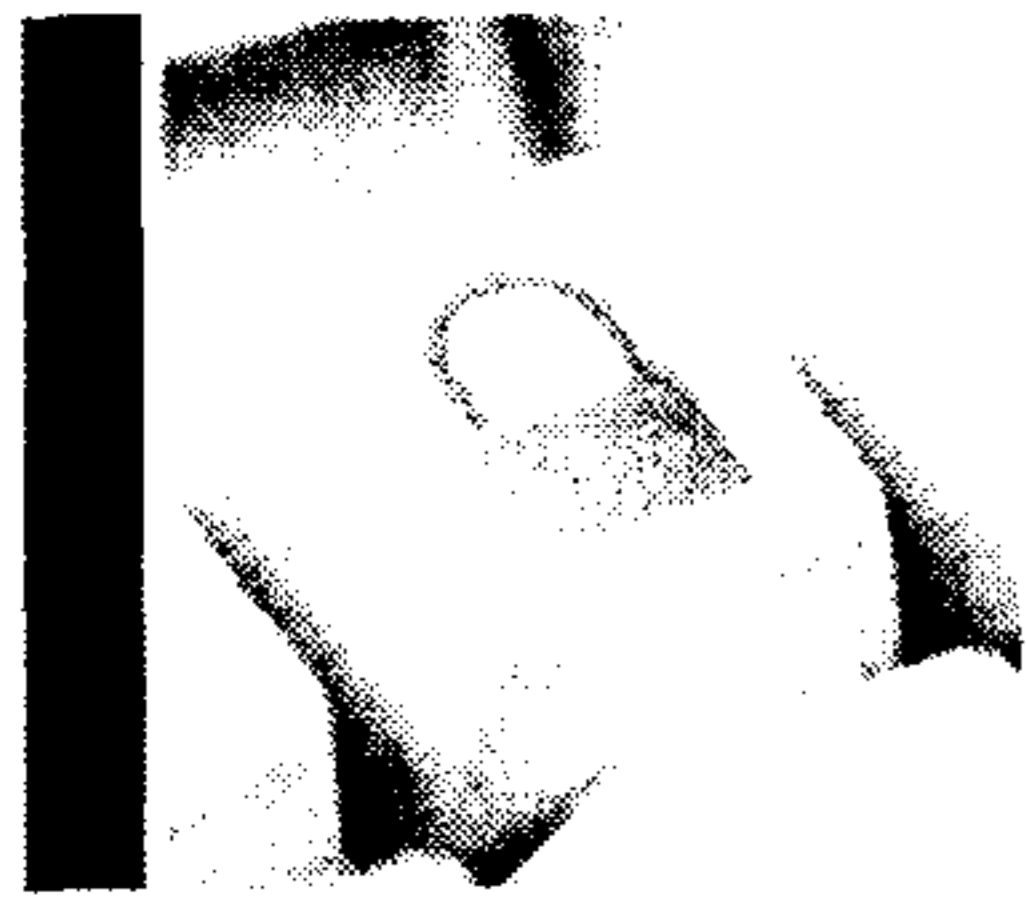
Artifact analysis reports – CCIRC prepared two AARs for suspicious file incidents, including for a website that had been suspected of serving malicious advertisements. AARs are a new CCIRC product that provide partners with in-depth technical analysis and mitigation advice for specific cyber threats.

If you would like to be added to CCIRC's distribution list please contact

CCIRC Products and Services: July - September



| Category | Description |
|---------------------------|--|
| Incidents Handled | Cyber related incidents addressed by CCIRC staff |
| Victim Notification | Informs organizations that have been victimized by cyber security breaches |
| Code Removal Request | Requests that a service provider remove malicious content from a website |
| Artifact Analysis Reports | Provides technical analysis details on a particular malware artifact(s) related to a cyber incident |
| Technical Report | Makes available detailed technical information to trusted partners in order enhance cyber security awareness on a specific topic |
| Alert | Offers critical, time sensitive information and mitigation advice to trusted partners, and normally, the public |
| Advisory | Delivers vulnerability notifications or security fixes for widely utilized information technology products to both trusted partners and the public |
| Information Notes | Provides information to trusted partners and the public in order to enhance cyber security awareness on a specific topic |
| Cyber Flash | Conveys threat detection and mitigation information to trusted partners when no vendor provided solution is available |



BUILDING A SAFE AND RESILIENT CANADA

SERVICES

Victim notifications – CCIRC sent out 3,507 victim notifications for 113,765 affected computing devices during this reporting period. These notifications are a service CCIRC provides to organizations affected by malware and contain detection and mitigation advice depending on the type of malware affecting the partner. The ICT and education sectors were the largest recipients of CCIRC’s victim notifications this quarter, accounting for 112,126 computing devices.

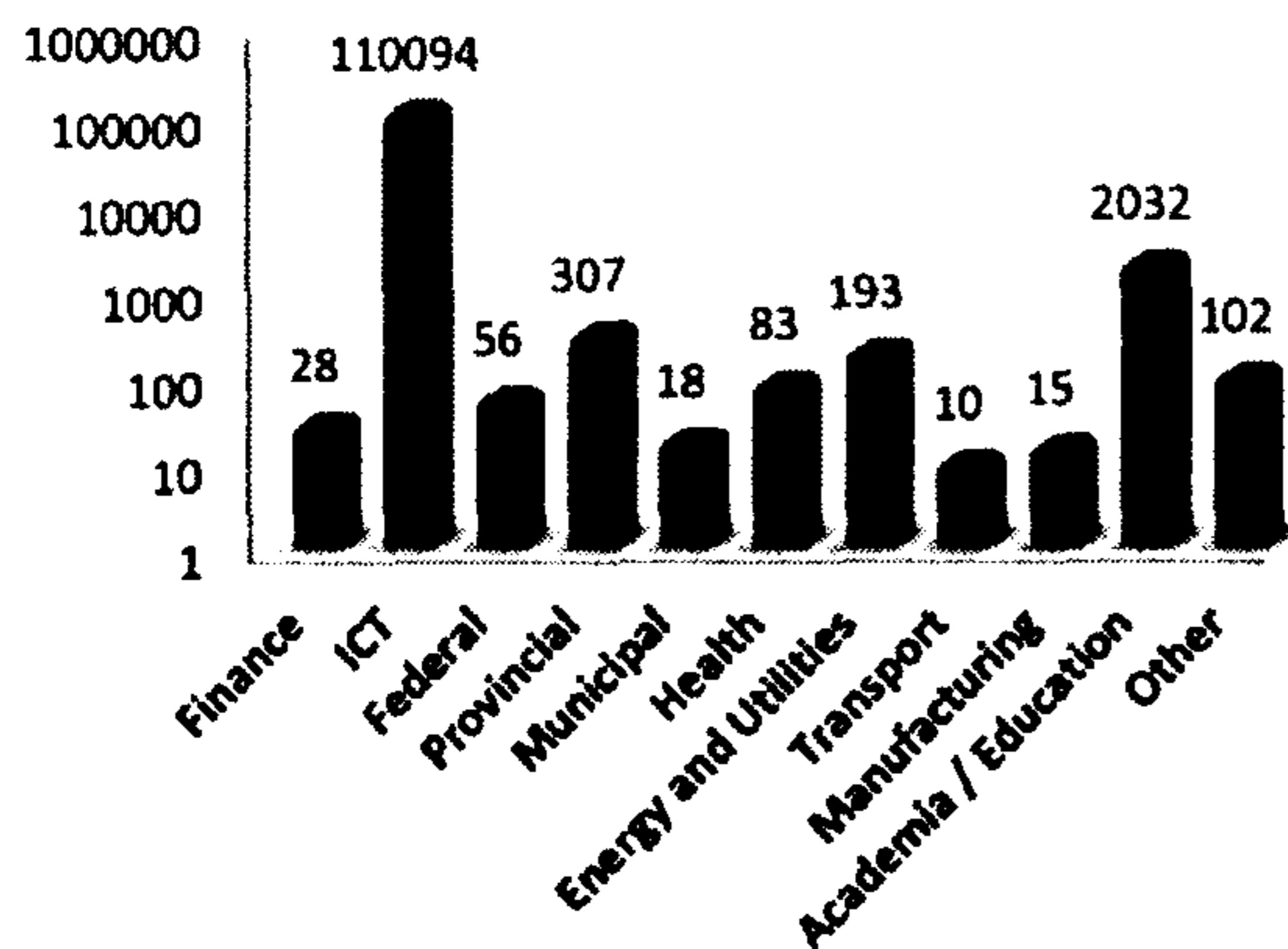
To support this service, CCIRC receives information about potentially infected computing devices from a number of trusted partners. This information is then compared with public and non-public lists to identify the victims and their associated business sectors.

Comment: The high notification rate for the ICT sector is likely due to the fact that most infections represent individual Canadians who are using an ICT company as a service provider. This quarter saw a significant reduction in notifications as replacement DNS servers operated by the Internet Systems Consortium were disconnected. These replacement DNS servers had been set up after the FBI took down an international internet fraud ring that was using DNSChanger malware. In addition, Microsoft shut down a command and control server for malicious software (Nitol).

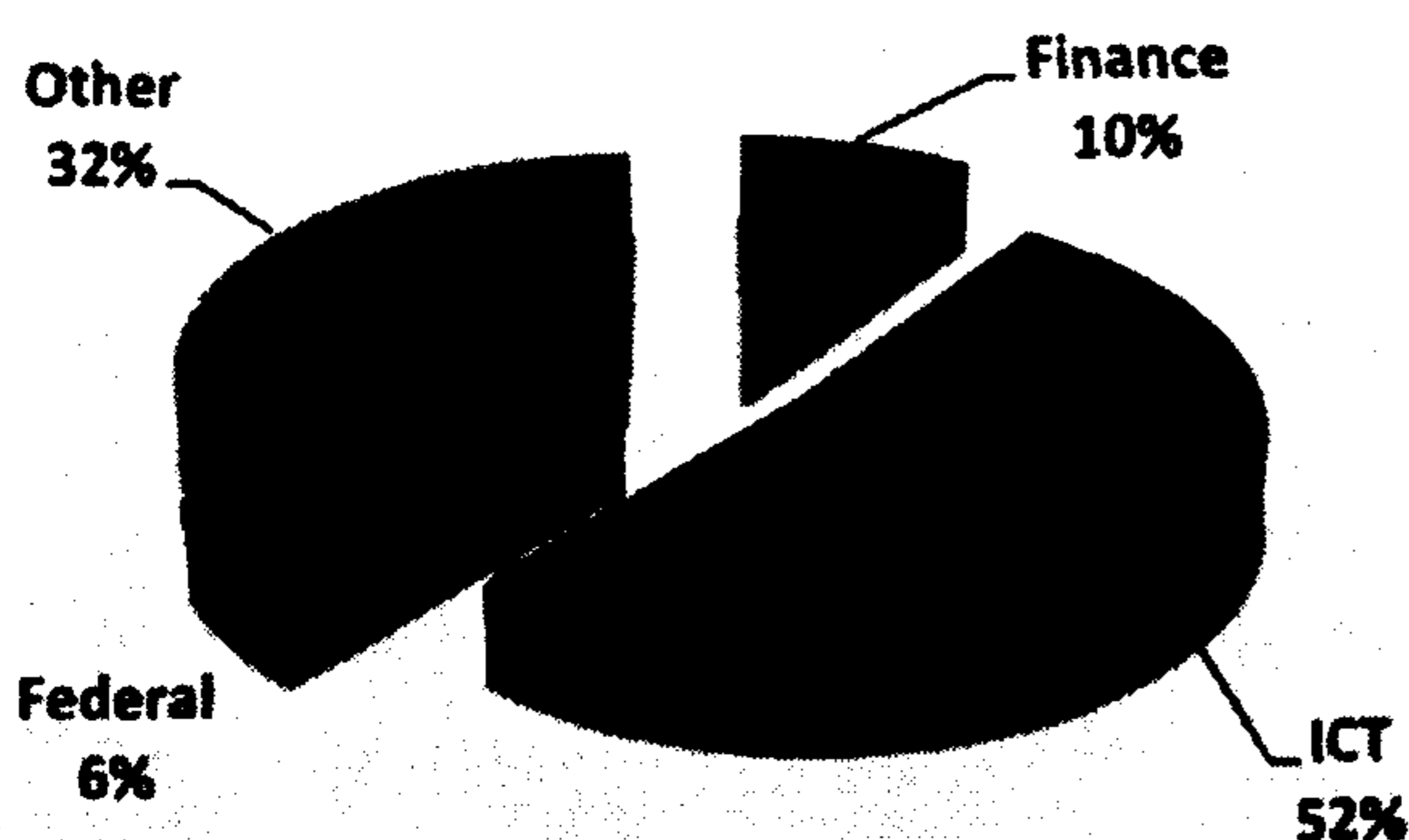
Code removal requests – CCIRC delivered 28 code removal requests (CRR) to Internet service and hosting providers informing them that malicious content was being hosted on their networks. Of these requests, 48% were reported as targeting Canadian critical infrastructure. 52% of the other CRRs, which affected unknown organizations, were proactively identified by CCIRC.

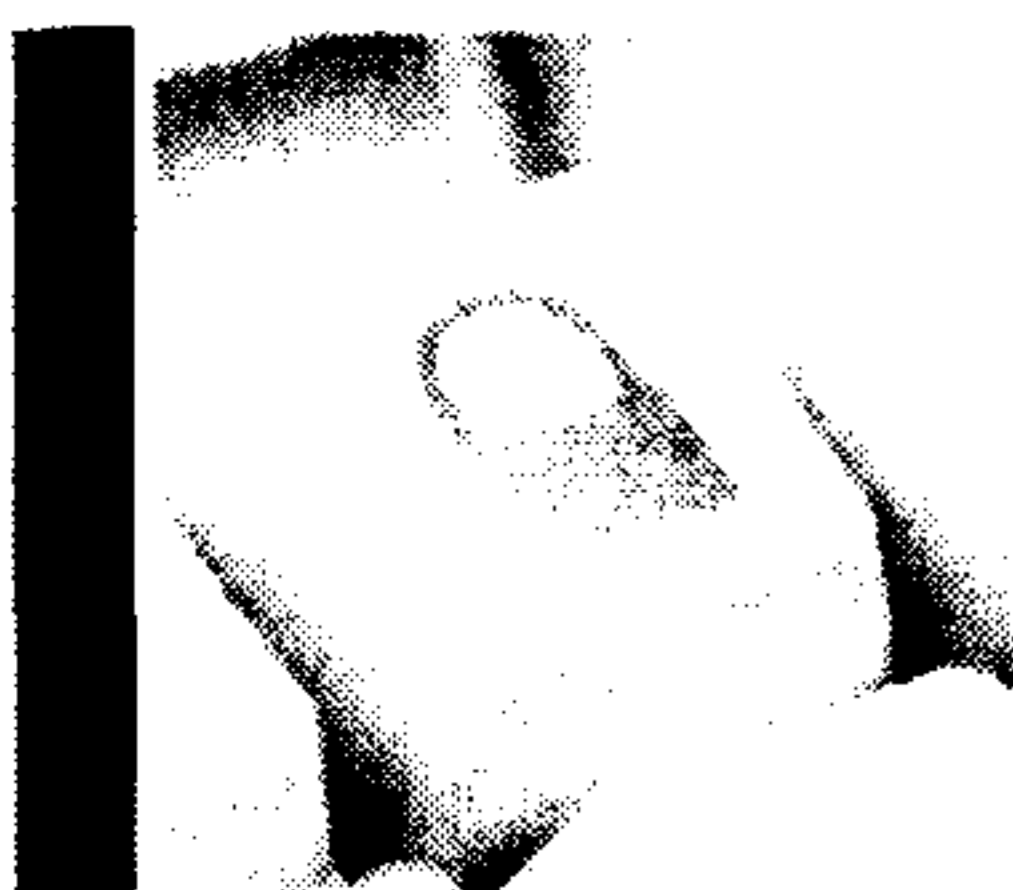
CRRs are a CCIRC service that informs recipients that they are hosting malicious content, website forgeries, and personal information and requests that it be removed. When CCIRC becomes aware of malicious content it sends CRRs to implicated Internet service and hosting providers.

Victim notifications – Computer devices impacted
July - September



Code removal requests – CI sector breakdown
July - September





CCIRC

Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

NOTEWORTHY INCIDENTS

1. Oracle Java vulnerabilities and exploits

CCIRC tracked an Oracle Java exploit targeting Java's HotSpot bytecode verifier. This flaw allows a malicious individual to remotely execute unauthenticated code. CCIRC released both an advisory informing its partners that Oracle had patched this vulnerability and a cyber flash (CF12-010) containing contextual information and mitigation advice. In addition, another Oracle Java vulnerability was exploited through targeted attacks allowing malicious actors to run arbitrary code on a victim's machine. CCIRC released both an advisory and a cyber flash (CF12-012) related to this incident.

2. Ongoing spear phishing campaign

Multiple organizations were targeted by emails sent to specific individuals. These emails contained a hyperlink, that when clicked, downloaded malicious files. CCIRC released a cyber flash (CF12-011) containing contextual information and mitigation advice and also suggested partners consult CCIRC's mitigation guidelines for advanced persistent threats.

3. RedKit exploit kit activity

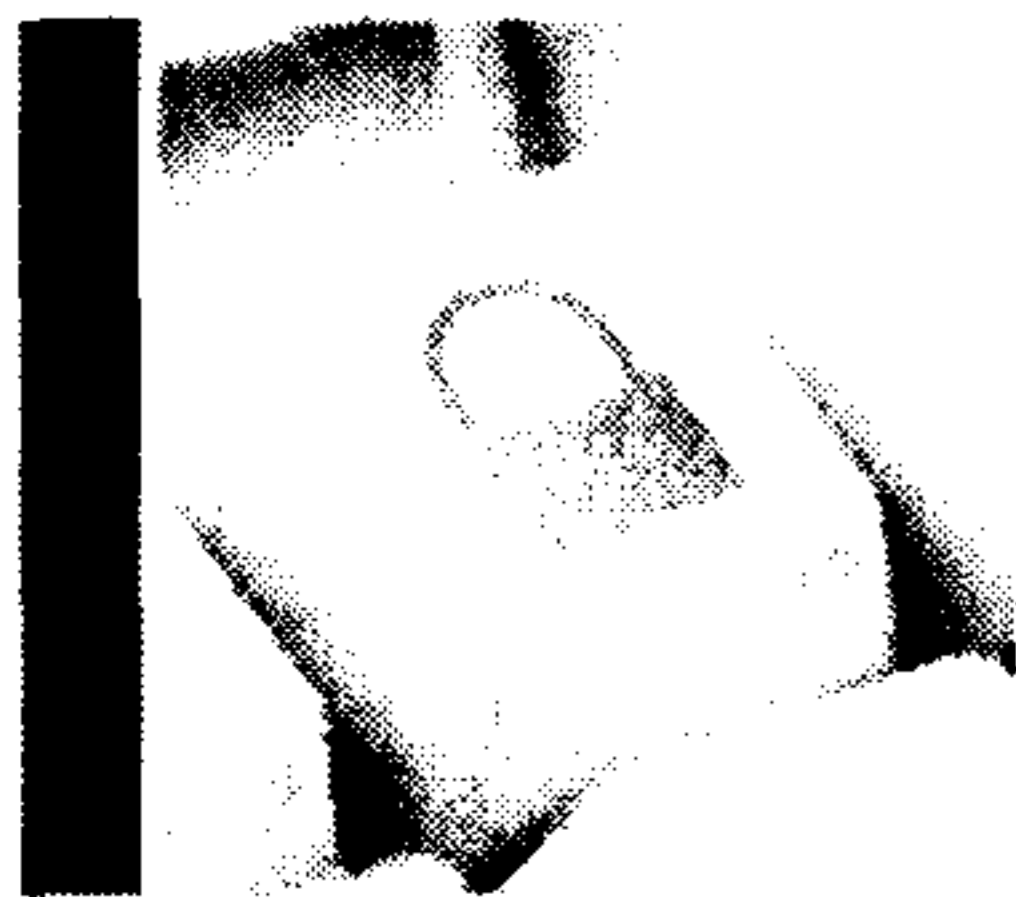
CCIRC became aware that a number of Canadian public and private sector organizations were affected by an exploit toolkit called RedKit. This toolkit inserts hidden malware into legitimate websites to exploit various Adobe and Java vulnerabilities. CCIRC released a cyber flash (CF12-013) related to this incident.

TOP FIVE MITIGATION ACTIONS

Implementing the following recommended actions will help prevent the majority of reported cyber incidents. CCIRC strongly recommends that all organizations use them.

- 1. Patch critical application vulnerabilities as soon as possible (e.g. PDF viewer, Flash Player, Microsoft Office and Java). Use the latest version of applications.**
- 2. Patch critical operating system vulnerabilities as soon as possible. Use the latest operating system version.**
- 3. Minimise the number of users with administrative privileges. Users should use a separate non-administrative account for email and web browsing.**
- 4. Undertake application whitelisting to help prevent malicious software and other unapproved programs from running (e.g. using Microsoft Software Restriction Policies or AppLocker).**
- 5. Utilise a host-based anti-virus and Intrusion Detection / Prevention System to identify anomalous behaviors. Keep systems up to date.**

See Annex B for a complete list of 35 mitigation actions for which there is broad international consensus.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

4. Shamoon / DistTrack malware

CCIRC observed that Shamoon / DistTrack malware was used against international companies in the energy and utilities sector. Shamoon is an information stealing malware that renders infected systems unusable. CCIRC released a cyber flash (CF12-014) and suggested partners consult CCIRC's mitigation guidelines for advanced persistent threats.

5. Internet Explorer zero day vulnerability

CCIRC became aware of an Internet Explorer vulnerability that allows attackers to run arbitrary code in the context of the current user within Internet Explorer. CCIRC released an alert to inform partners of the problem, and a cyber flash (CF12-015) containing contextual information and mitigation advice. CCIRC also released an advisory informing its partners when Microsoft patched this vulnerability.

6. ZeroAccess botnet activity

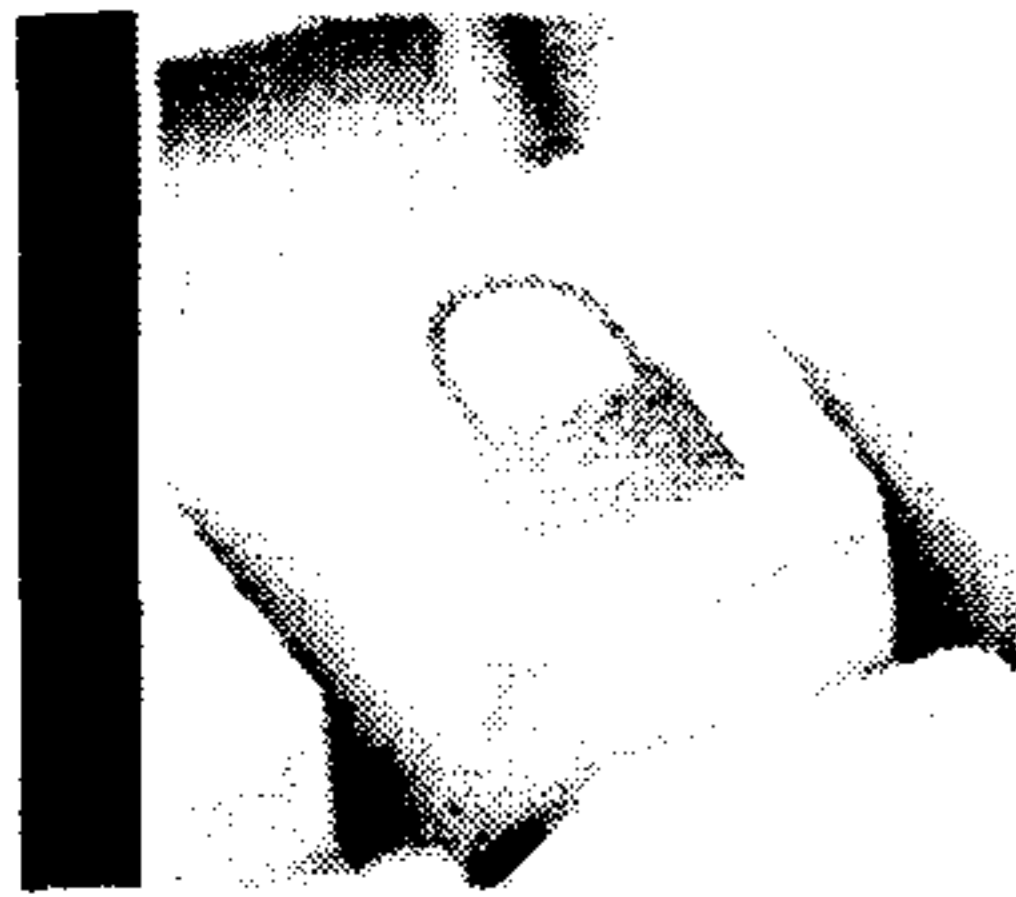
ZeroAccess botnet activity increased significantly over the reporting period. This botnet has infected millions of computers worldwide and is being used for fraudulent money making activities. CCIRC released a cyber flash (CF12-016) for this incident and suggested partners consult CCIRC's advanced persistent threat mitigation guidelines.

7. Cyber intrusion targets Industrial Control Systems (ICS) manufacturer

During this reporting period, a cyber intrusion targeted a Canadian ICS manufacturing company. This incident reportedly affected its operations in Canada and other countries. As of this document's publication date, CCIRC continues to work collaboratively with its domestic and international partners in order to provide mitigation assistance to this manufacturer. CCIRC updated a previous cyber flash (CF12-003) and suggested partners consult CCIRC's mitigation guidelines for advanced persistent threats.

8. Discovery of Gauss malware

Researchers discovered a new malware named Gauss. According to these researchers, Gauss is a cyber-espionage toolkit that can capture information associated with financial transactions, emails, and social network activity. Although Gauss infections were predominantly linked to the Middle East, there were a small number of infections reported in the United States. CCIRC closely monitored this situation, but has not identified any Canadian organizations impacted by this incident.



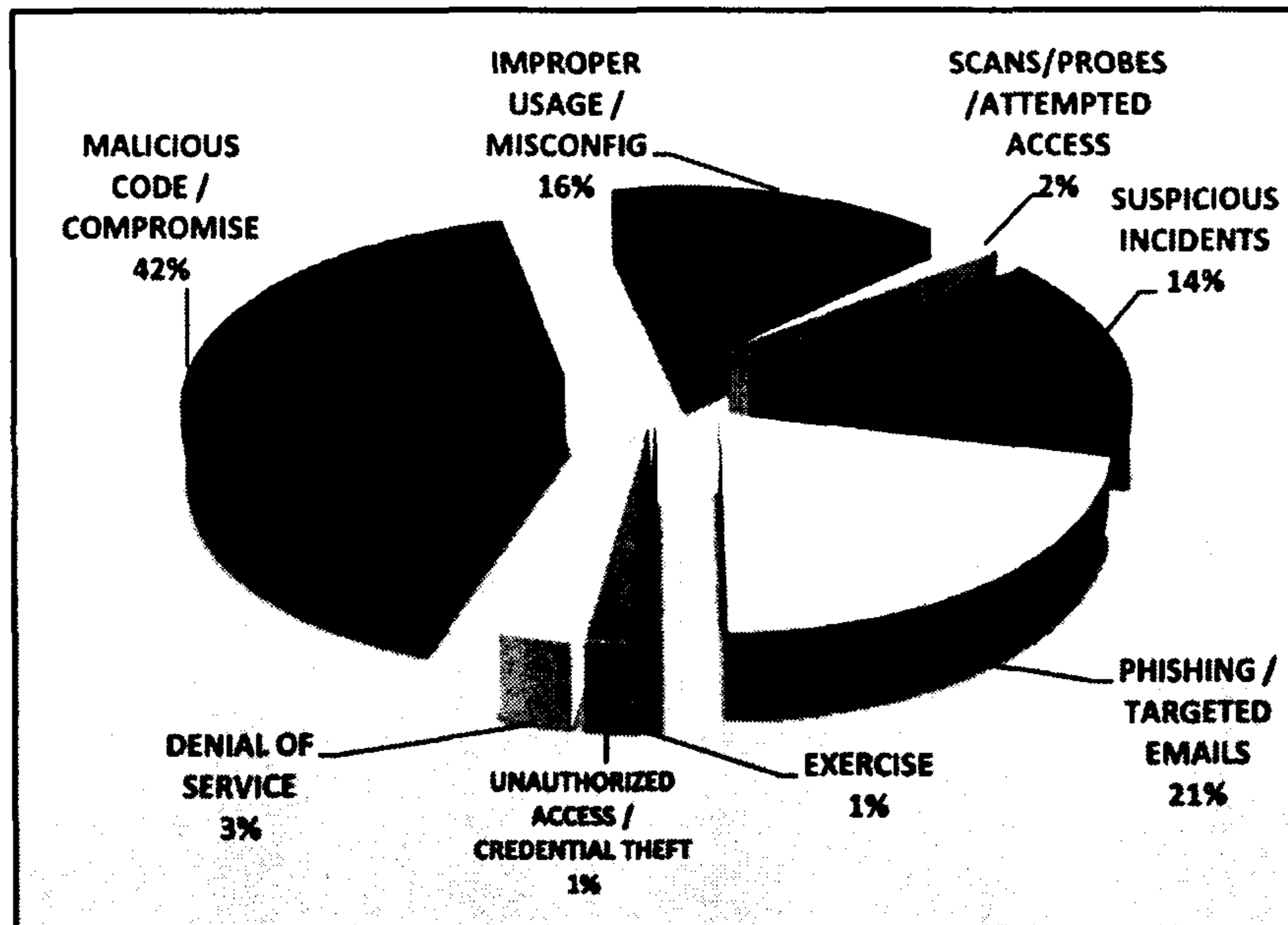
BUILDING A **SAFE AND RESILIENT CANADA**

TREND ANALYSIS

Canadian public and private sector partners with the greatest take-up of CCIRC's products and services have been the financial, ICT, energy and utilities, and government sectors. These enhanced partnerships have provided CCIRC with sector specific data, and therefore, these sectors are the initial focus of analysis. Going forward, this summary will add other sectors as partnerships mature. Definitions of incident categories are provided in Annex A.

There are two important caveats regarding the statistics used in this analysis. First, certain incidents can affect organizations in multiple sectors. To represent this as accurately as possible, these incidents are accounted for in each affected sector rather than in only one. Second, as certain incidents may fall into more than one category, the number of incidents reported may be different than the total of each category and some of the statistics in this report may reflect this discrepancy.

CCIRC INCIDENTS



CCIRC handled 251 incidents during this reporting period, a 6% increase from the previous quarter. Malware attacks (e.g. viruses, key loggers, and trojan horses) and phishing attacks (i.e. attempts to acquire personal or sensitive information by impersonating a trustworthy source) were the most common cyber threats observed by CCIRC – totalling 63% of the incidents handled.

Unauthorized access / credential theft, denial of service, improper usage / misconfiguration, scans / probes / attempted access, and suspicious incidents totalled the other 37% of observed incidents.



BUILDING A SAFE AND RESILIENT CANADA

TRENDS OBSERVED BY CCIRC

| Category | Unauthorized Access | | | Malicious Code | | | Scans / Probes | | | Phishing | | | | | | | | | | | | |
|----------|---------------------|------|---|----------------|-------|---|----------------|-----|------|----------|----|-------|---|---|------|---|----|------|---|----|------|---|
| Apr-Jun | 260 | 1% | ↑ | 26 | -85% | ↓ | 7 | 95 | 15% | ↑ | 9 | 378% | ↑ | 7 | -43% | ↓ | 34 | 9% | ↑ | 82 | -32% | ↓ |
| Jul-Sept | 262 | | | 4 | | | 7 | 109 | | | 43 | | | 4 | | | 37 | | | 56 | | |
| Apr-Jun | 68 | 79% | ↑ | 5 | -40% | ↓ | 4 | 31 | 103% | ↑ | 2 | 1150% | ↑ | 6 | -83% | ↓ | 9 | 44% | ↑ | 11 | 18% | ↑ |
| Jul-Sept | 122 | | | 3 | | | 4 | 63 | | | 25 | | | 1 | | | 13 | | | 13 | | |
| Apr-Jun | 70 | | | 0 | | | 0 | 45 | 13% | ↑ | 1 | | | 1 | | | 7 | | | 16 | -50% | ↓ |
| Jul-Sept | 70 | | | 2 | | | 1 | 51 | | | | | | 1 | | | 7 | | | 8 | | |
| Apr-Jun | 32 | -22% | ↓ | 0 | | | 0 | 19 | | | 1 | | | 0 | | | 6 | -33% | ↓ | 6 | -83% | ↓ |
| Jul-Sept | 25 | | | 0 | | | 0 | 19 | | | 1 | | | 0 | | | 4 | | | 1 | | |
| Apr-Jun | 52 | 12% | ↑ | 4 | -100% | ↓ | 0 | 8 | 75% | ↑ | 0 | | | 1 | | | 4 | 50% | ↑ | 35 | -11% | ↓ |
| Jul-Sept | 58 | | | 0 | | | 3 | 14 | | | 2 | | | 2 | | | 6 | | | 31 | | |

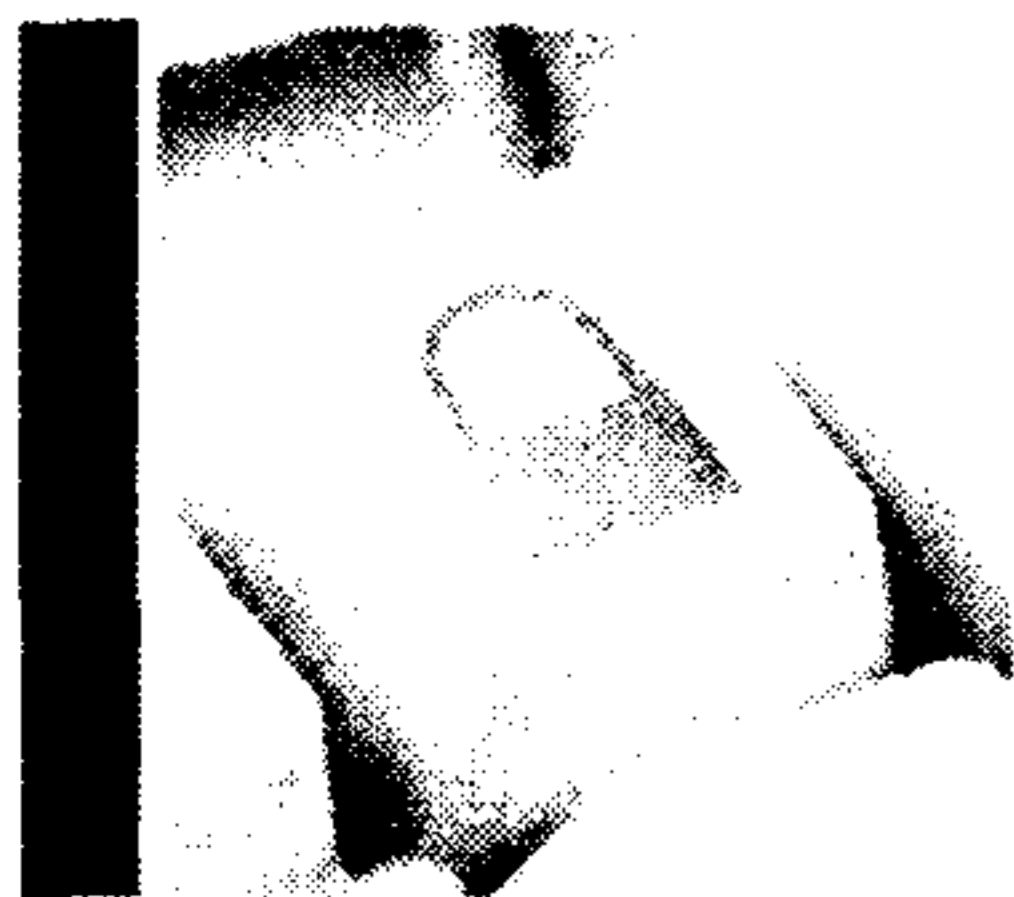
*Some incidents may impact multiple categories, and therefore, be counted more than once. As such, the total incidents in the above chart may be higher than actual totals. For example, this quarter CCIRC dealt with 251 incidents but when accounting for multiple category incidents the total rises to 262.

Malicious code – The government and ICT sectors were the largest targets of malware attacks, accounting for 114 observed cases – a 103% and 13% respective increase from last quarter. This quarter CCIRC observed that most of its partner sectors were affected by increased malware incidents.

Comment: International partners and security companies also observed an increase in malware attacks throughout 2012, with ZeroAccess, Zeus, and Flashback malware playing a significant role. A noteworthy portion of this rise can be attributed to malware specifically targeting mobile devices, as well as the increasingly widespread use of exploit kits, which allow unskilled users to exploit vulnerabilities with relative ease.

Improper usage / Misconfiguration – The government sector was affected by the largest amount of improper use / misconfiguration incidents, accounting for 25 observed cases – an 1150% increase from last quarter. Misconfiguration incidents were the main cause of this observed increase and are defined as a system that is made vulnerable or threatens another system as a result of faulty implementation or inappropriate settings related to the system's software / hardware.

Comment: This quarter, CCIRC received new data related to organizations operating with open DNS resolvers, and this is one of the main reasons for the observed increase in improper usage / misconfiguration incidents. Operating with an open DNS resolver can have a number of



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

consequences, including allowing outsiders to consume resources that do not belong to them, allowing attackers to poison the cache of the open resolver, and leaving the system vulnerable to distributed denial-of-service attacks. As this is specifically Canadian data, international partners may not be witnessing this same trend.

Phishing – This quarter, CCIRC observed 56 phishing incidents – a 32% decrease from last quarter.

Comment: Stable and low levels of phishing have also been observed by international partners and security companies. This could be in part due to the number of botnets which were taken down in 2011, an effort which continued in 2012. In July 2012, security company FireEye took down all of Grum's known command and control servers, which had previously been the world's third largest botnet. However, CCIRC and its partners are observing a noticeable increase in targeted phishing.

EMERGING TRENDS

CCIRC has observed an upward trend in attacks targeting **industrial control systems** (ICS). CCIRC's U.S. counterpart and security companies are also observing this trend, including the Shamoon/DistTrack malware affecting ICS detailed above.

In recognition of this trend and the risks facing ICS, CCIRC has published the *ICS Security Best Practice Guide* on its secure community portal. This guide was written to aid those involved in the design and operation of ICS to understand the critical issues involved in securing these systems. It provides the reader with an overview of the challenges and threats facing ICS owners and operators and presents data from actual ICS security incidents. The current status of the regulatory environment and industry standards is also discussed. The remainder of the document presents a lifecycle approach to managing ICS security, starting with risk assessment and followed by a discussion on best practice approaches to operational and technical security measures. If you would like a copy of this guide please contact [CCIRC](#).

As per last quarter, **advanced persistent threats** (a group with both the capability and the intent to persistently and effectively target a specific entity); **crimeware** (a class of malware designed specifically to automate cybercrime), and **hacktivism threats** (the use of computer networks to protest / promote political ends) remained noteworthy trends. Going forward, these incidents will likely continue to have an impact on CCIRC's public and private sector partners.

REPORTS RECEIVED

CCIRC received 30 cyber incident reports from public and private sector partners directly affected by a cyber incident, which represents a 40% decrease from the last reporting period. CCIRC's effectiveness depends on its partners' reports and if you have incidents of concern please contact CCIRC at [REDACTED]

[REDACTED] Going forward, CCIRC will be focused on enhancing its number of trusted partnerships.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

PUBLISHED THREAT REPORTS

CCIRC encourages its partners to keep up-to-date on the latest in cyber-security, and as such, this section provides a brief outline of a few open source reports.

2012 Norton Cyber Crime Report – Norton highlights that there were 556 million cybercrime victims globally, which amounts to a global price tag for consumer cybercrime of \$110 billion (USD) annually.

Symantec's The Tangled Web: Silent Threats & Invisible Enemies – This white paper aims to help computer users understand the threat posed by spyware, which collects information clandestinely.

Threat Report: EyeStye – This Microsoft Malware Protection Center report provides an overview of the EyeStye Trojan, which can be used to steal sensitive data and other online properties from the websites of financial institutions, using key logging and screenshot capturing techniques.

The Elderwood Project – This Symantec report offers an in depth analysis of high profile attacks that started in 2009 by a group using the Hydraq (Aurora) Trojan. A number of organizations worldwide were targeted by these attacks, mainly in the safety, energy and utilities, and finance sectors.

Smarter Protection for the Smart Grid – This McAfee research paper examines how and why these grids are vulnerable to cyber threats, what is being done to counter them, and what additional measures can be taken to continue to ensure the reliability of the bulk electric power grid.

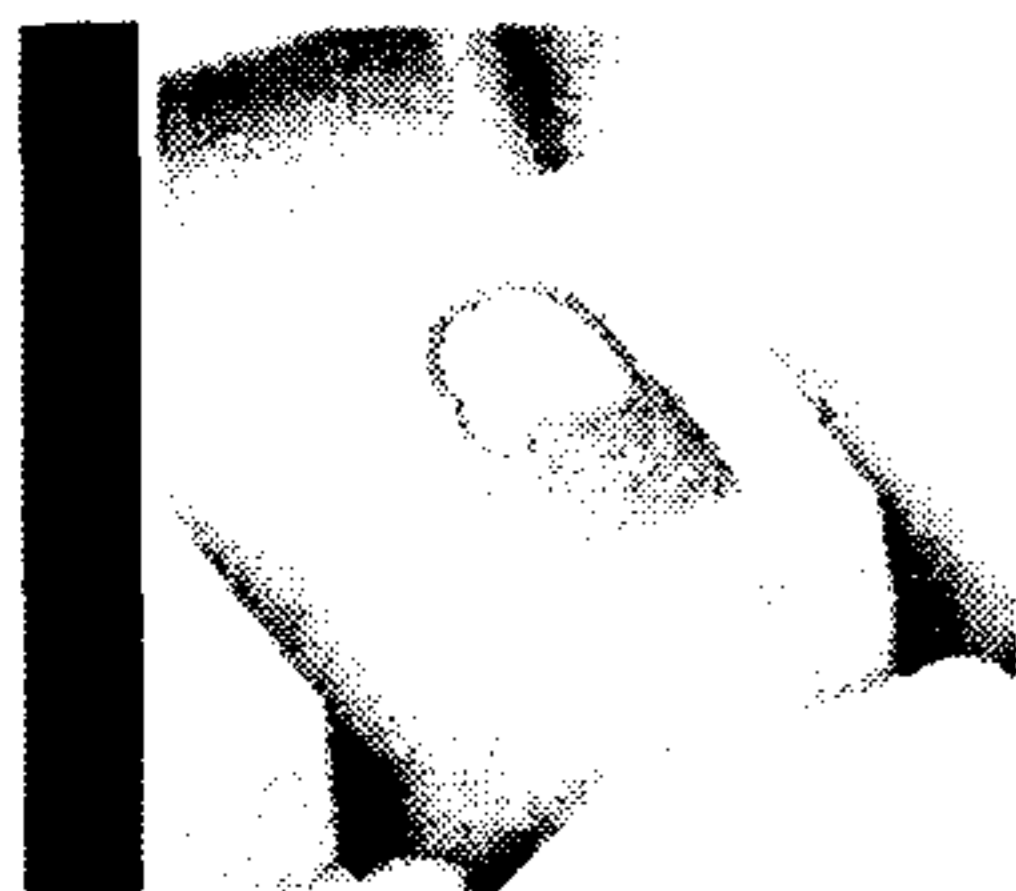
McAfee Threat Report: Second Quarter 2012 – McAfee reports the emergence of mobile “drive-by downloads” as a new attack vector, the use of Twitter to control mobile botnets, and the appearance of mobile ransomware.

F-Secure Threat Report: H1 2012 – Covering the first half of 2012, this report offers an overview of the trends and developments witnessed in the malware threat landscape. A key finding of the report is the increasing number of exploit kits, which allow even unskilled users to easily exploit vulnerabilities.

IBM X-Force: 2012 Mid-year Trend and Risk Report – IBM reported on the threats and emerging trends it saw in the first half of 2012, including the more than 4,400 new vulnerabilities discovered thus far, and that 2012 is on track for breaking the record for the number of new vulnerabilities.

FireEye Advanced Threat Report – Covering the first half of 2012, this report provides an overview of the advanced threat landscape, including information on the nature of advanced malware and tactics used for advanced persistent threats (APT).

- ❖ It is important to note that as these websites are provided for your convenience, the Government is not responsible for the accuracy, currency or the reliability of the content nor does it endorse the sites.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

ABOUT CCIRC

Mandate

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to and recovery from cyber events. It does this by providing authoritative advice and support, and coordinating information sharing and event response.

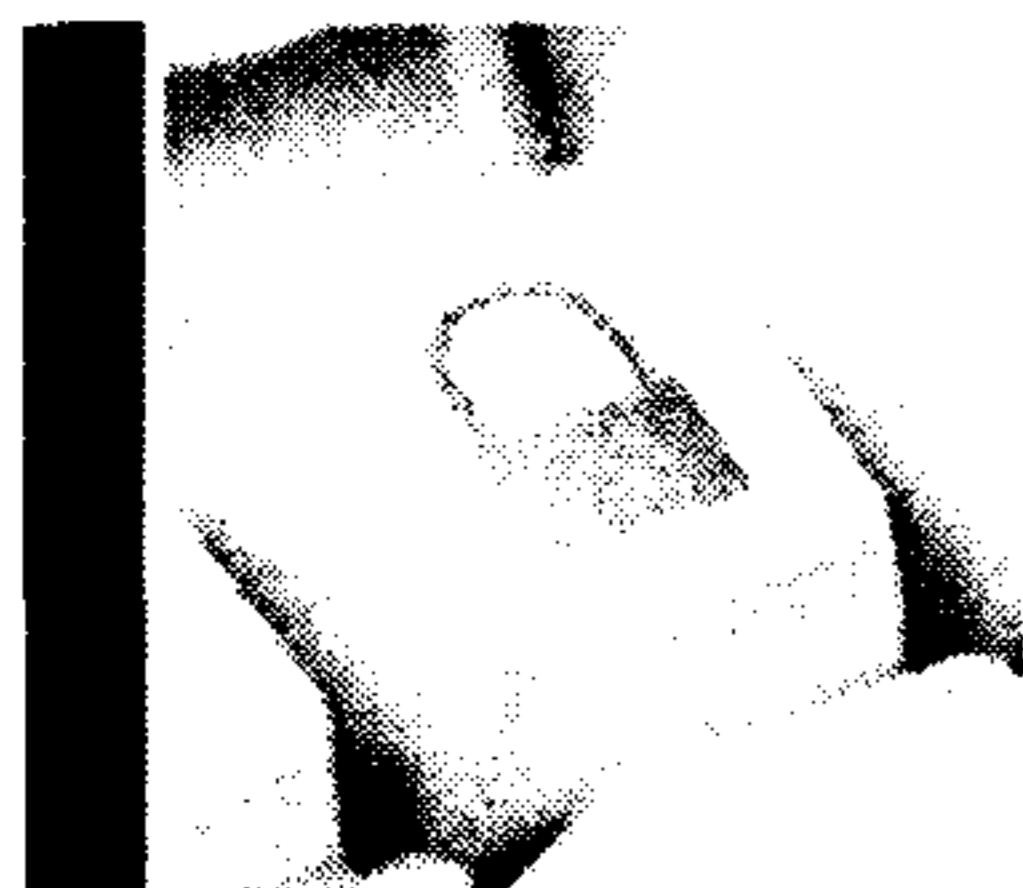
Core functions

To deliver on its mandate, CCIRC:

- Builds and maintains trusted relationships and information sharing mechanisms with partners and clients;
- Disseminates a variety of cyber information products based on data from domestic and international partners and sources;
- Conducts daily cyber operations such as code removal requests related to malicious sites, the notification of compromised systems, and the repatriation of stolen data; and
- Maintains the protocols and mechanisms for coordinating the national cyber incident response in collaboration with law enforcement and intelligence.

Background

Created in 2005 and housed within Public Safety Canada's National Cyber Security Directorate, CCIRC is Canada's national computer emergency readiness team. CCIRC works to reduce Canada's cyber risk by enhancing the cyber security of public and private sector partners and ensuring a coordinated national response to significant cyber events.

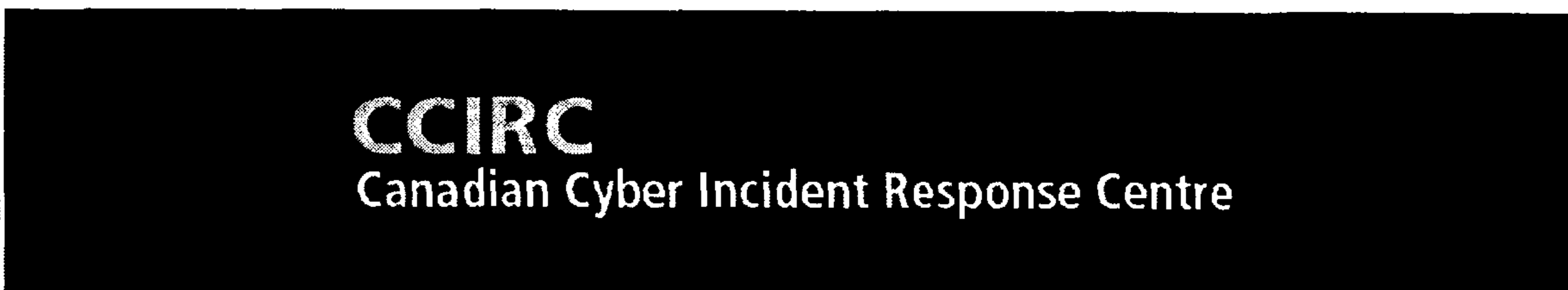
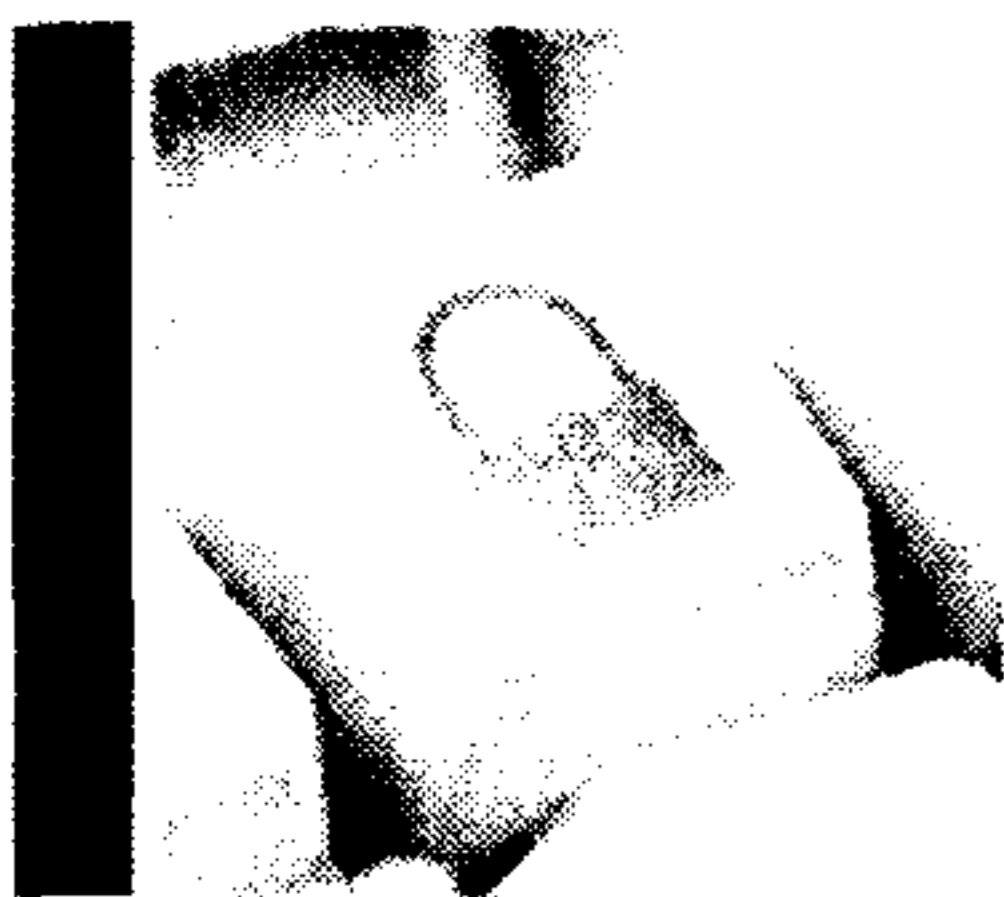


CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

ANNEX A – DEFINITIONS

| Name | Definitions |
|-----------------------------------|---|
| Incident | An incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising the business operations and threatening the information security of system(s) of national significance within the Canadian public and private sectors. |
| Event | An event is an observable change to the normal behavior of a computer, IT system, environment, process, or workflow that may impact or may pose a threat to the system or data integrity, or safety and security. An event can be “upgraded” and become an incident if it becomes apparent that the change observed has a probable negative impact and requires mitigation or advice. |
| Activity | These are “back-of-house” procedures that occur on a daily basis, and that cannot be classified as an event or an incident. In general, they include administrative tasks, or support functions to events or incidents. |
| Unauthorized Access | In this category an individual gains logical or physical access without permission to a network, system, application, data, or other resource |
| Denial of Service (DoS) | An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. |
| Malicious Code | Successful installation of malicious software (e.g. virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. |
| Improper Usage | Any activity that violates acceptable computing use policies. |
| Scans/Probes /Attempted Access | This category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. |
| Investigation | <i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. |
| Phishing / Targeted Emails | A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Criminally-fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. |
| Advanced Persistent Threat (APT): | Adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors. Objectives typically include: establishing and extending footholds within the information technology infrastructure of the targeted organizations for the purpose of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives. The APT pursues its objectives repeatedly over an extended period of time; adapts to defenders’ efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives. |
| Crimeware | Crimeware is malicious software that is covertly installed on computers and has the ability to ‘steal’ confidential information and send it back to cyber criminals. One form of crimeware is ransomware, which is software that denies access to a person’s files until they pay a ransom. |
| Hacktivism | Some groups of computer hackers are not motivated by financial gain and instead are driven by economic, political, or religious interests that generally go beyond their nation’s borders. Their actions are called hacktivism, which is a merger of hacker and political activism. Hacktivists infiltrate networks and put their talents to work for their beliefs by organizing computer attacks, including piracy, hijacking servers, and replacing homepages with ideological messages. |



BUILDING A SAFE AND RESILIENT CANADA

ANNEX B – TOP 35 RECOMMENDED MITIGATION ACTIONS

The following is a list of recommended cyber threat mitigation strategies, listed in order of effectiveness, to which all organizations should adhere. This list has broad international agreement and is being widely distributed following an initial public release by the Australian Government's Defense Signals Directorate.

| Ranking | Mitigation Strategy |
|---------|---|
| 1 | Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications. |
| 2 | Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version. |
| 3 | Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing. |
| 4 | Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker. |
| 5 | Host-based Intrusion Detection/Prevention System to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking. |
| 6 | Whitelisted email content filtering allowing only attachment types required for business functionality. Preferably convert/sanitise PDF and Microsoft Office attachments. |
| 7 | Block spoofed emails using Sender Policy Framework checking of incoming emails, and a 'hard fail' SPF record to help prevent spoofing of your organisation's domain. |
| 8 | User education e.g. Internet threats and spear phishing socially engineered emails. Avoid weak passphrases, passphrase re-use, exposing email addresses, and unapproved USB devices. |
| 9 | Web content filtering of incoming and outgoing traffic, using signatures, reputation ratings and other heuristics, and whitelisting allowed types of web content. |
| 10 | Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. |
| 11 | Web domain whitelisting for HTTPS/SSL domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. |
| 12 | Workstation inspection of Microsoft Office files for abnormalities e.g. using the Microsoft Office File Validation feature. |
| 13 | Application based workstation firewall, configured to deny traffic by default, to protect against malicious or otherwise unauthorised incoming network traffic. |
| 14 | Application based workstation firewall, configured to deny traffic by default, that whitelists which applications are allowed to generate outgoing network traffic. |
| 15 | Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. |
| 16 | Multi-factor authentication especially implemented for when the user is about to perform a privileged action, or access a database or other sensitive information repository. |
| 17 | Randomized local administrator passphrases that are unique and complex for all computers. Use domain group privileges instead of local administrator accounts. |
| 18 | Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words. |
| 19 | Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an email server, or an authenticated web proxy. |
| 20 | Data Execution Prevention using hardware and software mechanisms for all software applications that support DEP. |
| 21 | Antivirus software with up to date signatures, reputation ratings and other heuristic detection capabilities. Use |



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

gateway and desktop antivirus software from different vendors.

- 22 Non-persistent virtualised trusted operating environment with limited access to network file shares, for risky activities such as reading email and web browsing.
- 23 Centralized and time-synchronized logging of allowed and blocked network activity, with regular log analysis, storing logs for at least 18 months.
- 24 Centralized and time-synchronized logging of successful and failed computer events, with regular log analysis, storing logs for at least 18 months.
- 25 Standard Operating Environment with unrequired operating system functionality disabled e.g. IPv6, autorun and Remote Desktop. Harden file and registry permissions.
- 26 Workstation application security configuration hardening e.g. disable unrequired features in PDF viewers, Microsoft Office applications, and web browsers.
- 27 Restrict access to NetBIOS services running on workstations and on servers where possible.
- 28 Server application security configuration hardening e.g. databases, web applications, customer relationship management and other data storage systems.
- 29 Removable and portable media control as part of a data loss prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.
- 30 TLS encryption between email servers to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.
- 31 Disable LanMan password support and cached credentials on workstations and servers, to make it harder for adversaries to crack password hashes.
- 32 Block attempts to access web sites by their IP address instead of by their domain name.
- 33 Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- 34 Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.
- 35 Full network traffic capture to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days.

Created
Sept 17, 2012

2

DATE:

File No.: 390302
RDIMS No.: 688638

MEMORANDUM FOR THE MINISTER

THE CANADIAN CYBER INCIDENT RESPONSE CENTRE'S QUARTERLY CYBER OPERATIONAL SUMMARY

(Information only)

ISSUE

The Canadian Cyber Incident Response Centre (CCIRC) has developed a Quarterly Cyber Operational Summary (QCOS). The QCOS's first iteration, covering the April to June 2012 reporting period, is attached (**Tab A**).

BACKGROUND

As Canada's computer emergency readiness team, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity. CCIRC does this by providing authoritative advice and support, and coordinating information sharing and incident response.

Efforts are underway to strengthen CCIRC's legal, policy, and process foundations and deepen its collaboration with public and private sector partners. As part of this effort, CCIRC is developing a new suite of professional products for its clients.

The QCOS is part of this suite of products and it provides decision makers at the management level with relevant cyber information. It was distributed this August to approximately 100 stakeholders in the private sector, 12 provinces and territories, and was well received.

CONSIDERATIONS

Over time and with greater historical data, the QCOS will offer cyber trend analysis with a Canadian context, and compare Canada's cyber situation to that of other countries. Providing improved situational awareness to partners is a key element of Public Safety's strategy to improve the perceived value of CCIRC's role, and as a consequence to increase partners' information sharing with CCIRC. The feedback questionnaire, which

is attached to this and all new products, will enable CCIRC to ensure its products meet its partners' requirements (**Tab B**).

CURRENT STATUS

New iterations will follow every three months and be available in both official languages. At the request of your office, you will be provided copies. A companion classified quarterly cyber environmental update will be provided under separate cover.

CONCLUSION

Should you require additional information, please do not hesitate to contact me or Lynda Clarimont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.

Graham Flack
Acting Deputy Minister

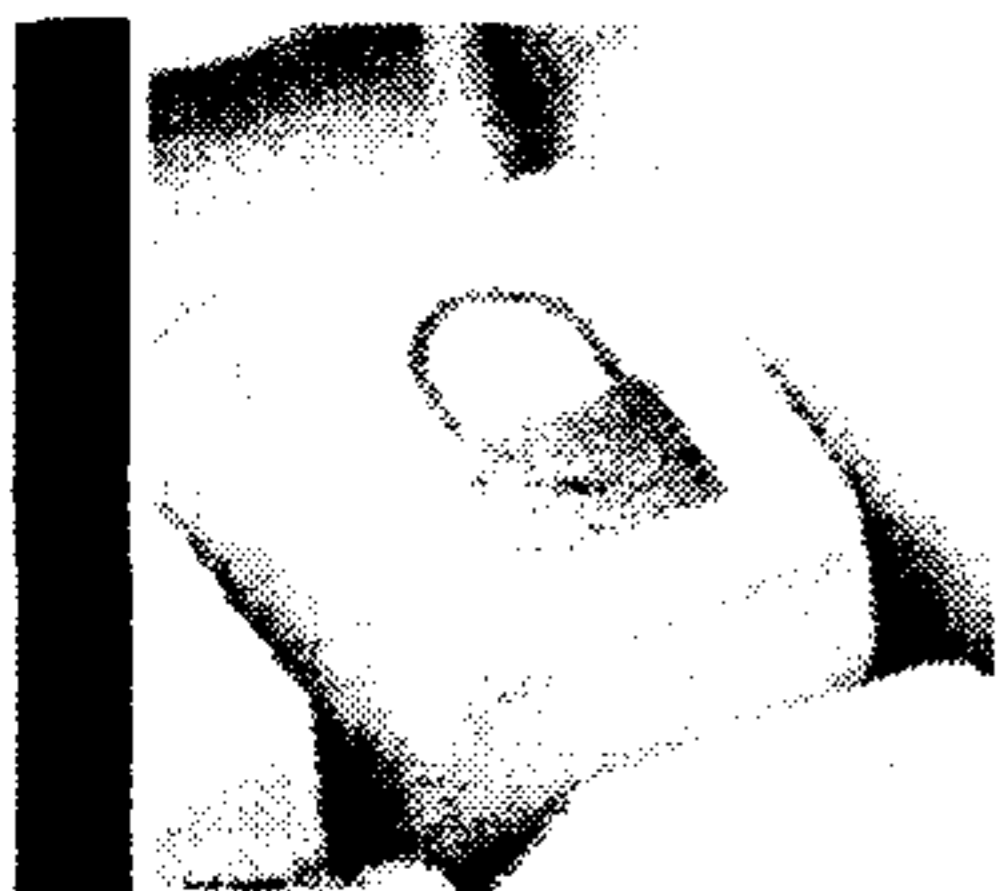
Enclosure: (2)

Prepared by: Nate Klassen



Public Safety
Canada

Sécurité publique
Canada

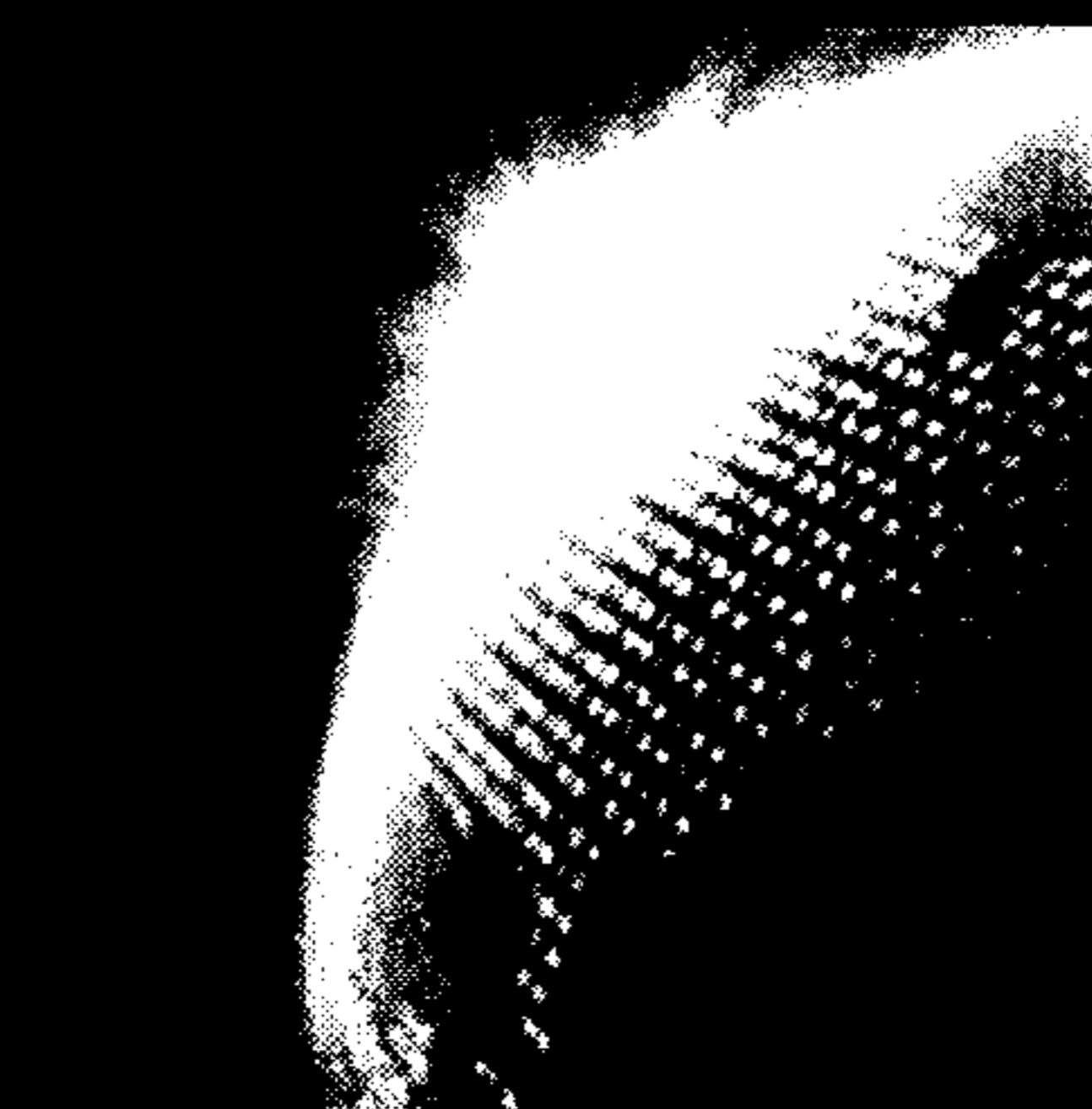


CCIRC

Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

Partnering to Secure Vital Cyber Systems



Quarterly Operational Summary – April to June

Public Safety Canada

This document provides a quarterly summary of the cyber incidents observed by the Canadian Cyber Incident Response Centre (CCIRC).

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. CCIRC is continually working to improve the accuracy of its statistics. As it launches new products, some variations may appear in the presented statistics.

REPORTING CYBER INCIDENTS

Private or public sector partners wishing to report incidents may send an email to cyber-incident@ps-sp.gc.ca using CCIRC's Cyber Duty Officer PGP encryption key, found here: (<http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx>).

FEEDBACK

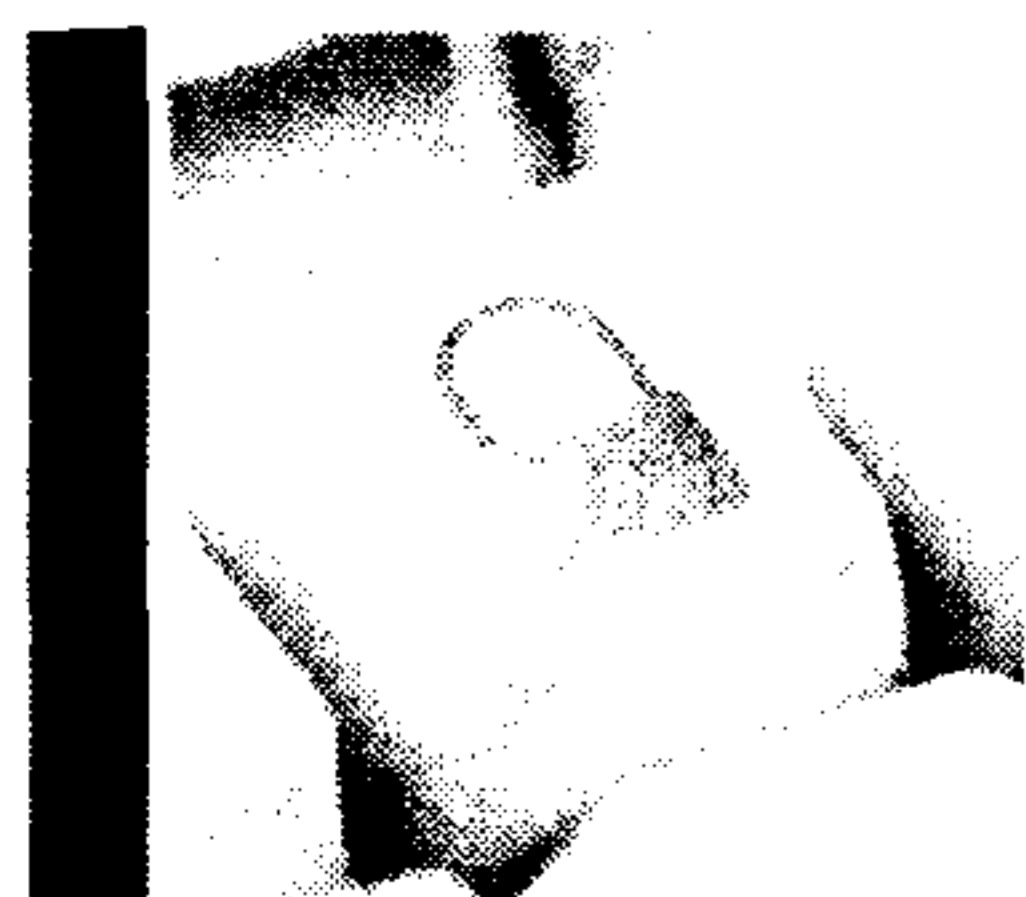
This is a newly developed product. Your feedback is critical to making this product more useful. As such, please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.



BUILDING A **SAFE AND RESILIENT CANADA**

TABLE OF CONTENTS

| | |
|--|----|
| Table of Contents..... | 2 |
| Executive Summary..... | 3 |
| Products | 4 |
| Services | 5 |
| Noteworthy Incidents | 6 |
| Trend Analysis | 8 |
| CCIRC Incidents | 8 |
| Trends Observed by CCIRC..... | 9 |
| Reports Received | 9 |
| Recent Cyber Trends Observed by CCIRC | 9 |
| About CCIRC | 10 |
| Recent Developments..... | 11 |
| Annex A – Definitions..... | 12 |
| Annex B – Top 35 Recommended Mitigation Actions..... | 13 |



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

EXECUTIVE SUMMARY

PURPOSE

This product discusses cyber incidents the Canadian Cyber Incident Response Centre (CCIRC) observed during the April to June 2012 reporting period. Its intent is to convey information to partners in the Canadian private and public sectors about: products and services CCIRC provided; noteworthy incidents; and, trends.

OVERVIEW

CCIRC handled 237 incidents during the reporting period. An incident is a single or series of unwanted or unexpected information security events that have a significant probability of compromising the business operations and information security of systems within the Canadian private and public sectors. Malware (e.g. viruses, key logging, Trojan horses) and phishing attacks were the most common cyber incidents, totalling 68% of the incidents observed by CCIRC.

The information and communication technology (ICT), government, and energy and utilities sectors were the largest targets of malware attacks, accounting for 66% of observed cases. The high numbers associated with the ICT sector throughout this report are not indicative of the sector itself but instead represent individual Canadians who use the services of these companies.

A clear trend has seen malicious individuals target average Canadians by impersonating financial institutions through phishing campaigns. As such, the financial sector accounted for 39% of phishing incidents seen by CCIRC. Phishing is a digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.

CCIRC's code removal requests (CRR) inform Internet Service Providers that they are hosting malicious content, website forgeries, and personal information. The ICT and government sectors were the most affected by cyber incidents that led to CRRs. The ICT, government, and education sectors were the largest recipients of CCIRC's 1,934 victim notifications advising them of malware affecting them, and depending on the type, different detection and mitigation methods.

NOTEWORTHY INCIDENTS

Of the 237 incidents observed during this reporting period, CCIRC identified the following noteworthy incidents: Oracle Java vulnerabilities and exploits; federal government departments being impersonated in an email phishing campaign; discovery of Flame malware; and, increased activity related to ZeuS malware.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

PRODUCTS

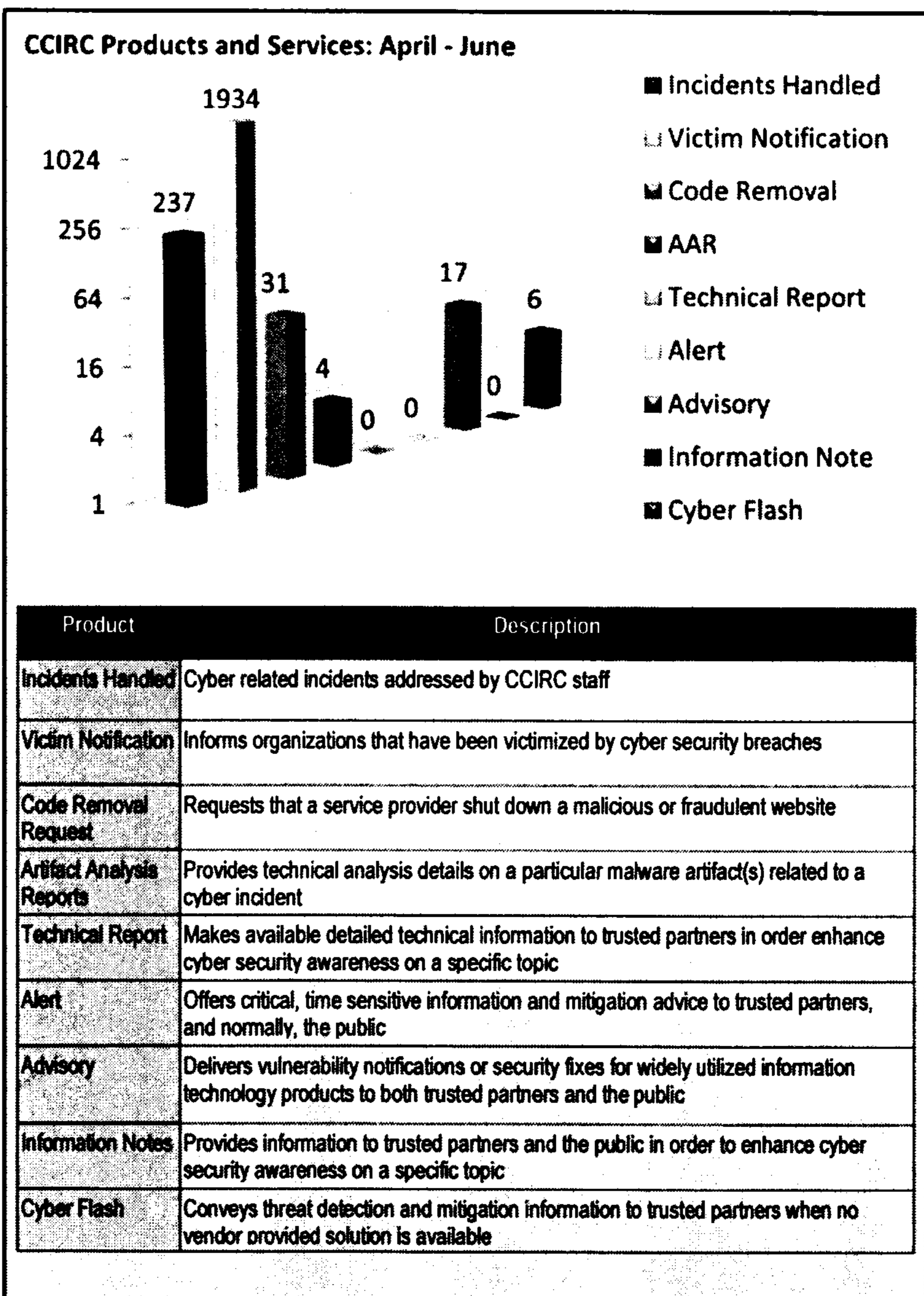
CCIRC issued 17 advisories, six cyber flashes (CF), and four artifact analysis reports (AAR) over this reporting period. Generally, CCIRC posts advisories, information notes, and technical reports on its [website](#).

Cyber flashes – CCIRC released cyber flashes providing information and mitigation advice related to: Oracle Java exploits; phishing email campaigns spoofing the Canada Revenue Agency and Canada Post; Flame malware; and, increased ZeuS malware activity (CF12-004 / CF12-005 / CF12-006 / CF12-007 / CF12-008 / CF12-009).

Artifact analysis reports – In addition, CCIRC prepared four AARs for suspicious file incidents, including ransomware. AARs are a new CCIRC product that provides partners with in-depth technical analysis and mitigation advice for specific cyber threats.

Advisories – CCIRC also issued 17 [advisories](#) to bring attention to significant upgrades and patches of common computer products such as Microsoft, Adobe, and Oracle.

If you would like to be added to CCIRC's distribution list please contact [\[redacted\]](#)





BUILDING A SAFE AND RESILIENT CANADA

SERVICES

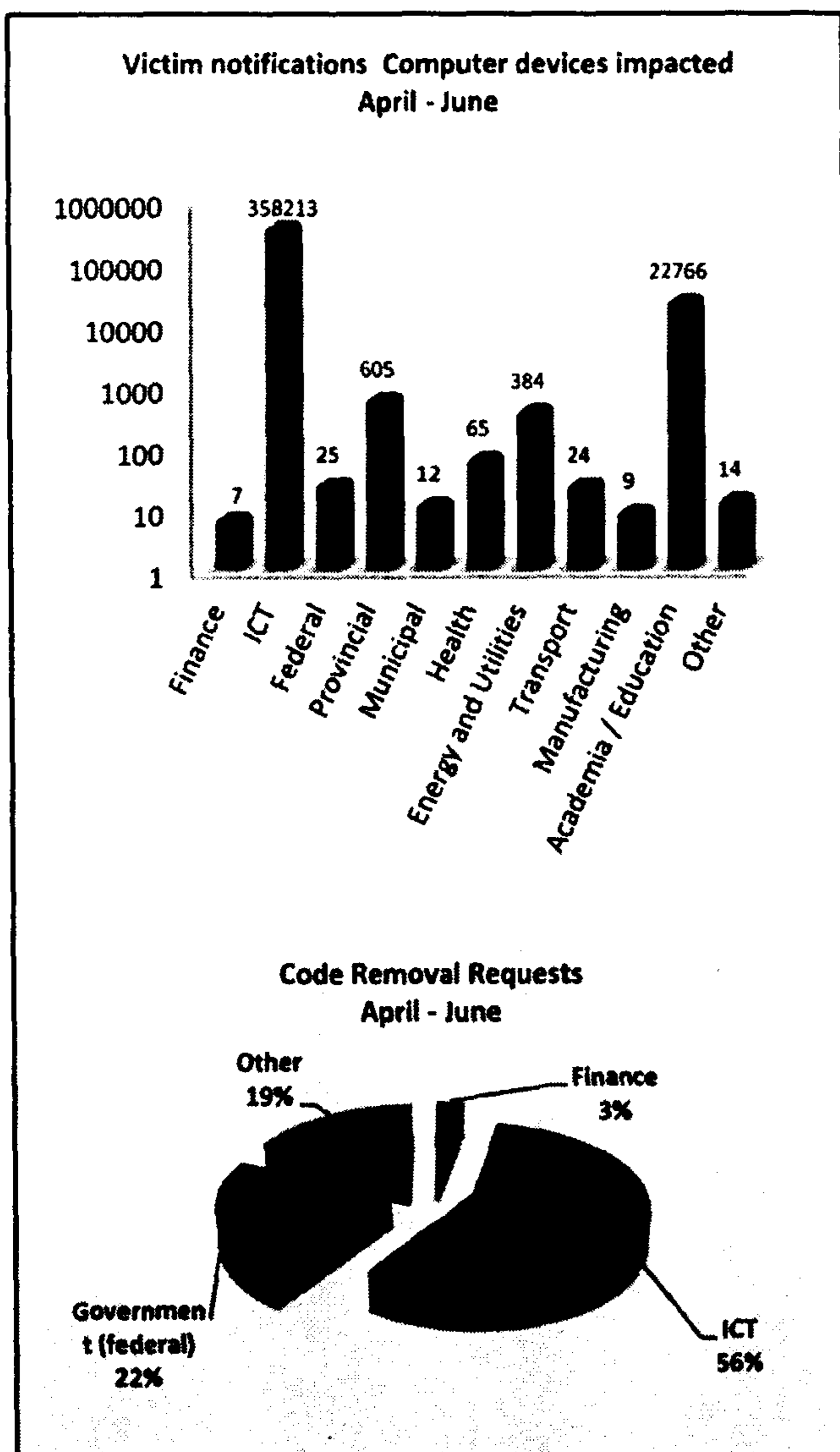
Victim notifications – CCIRC sent out 1,934 victim notifications for 382,124 affected computing device connections during this reporting period. These notifications are a service CCIRC provides to organizations affected by malware and contain detection and mitigation advice depending on the type of malware affecting the client. The ICT and education sectors were the largest recipients of CCIRC's victim notifications this quarter, accounting for 380,979 computing device connections.

To support this service, CCIRC receives information about potentially infected computers from a number of trusted partners. This information is then compared with public and non-public lists to identify the victims and their associated business sectors.

Comment: The high notification rate for the ICT sector is due to the fact that most infections represent individual Canadians who are using an ICT company as a service provider. This quarter, incidents such as DNS Changer and Flashback prompted CCIRC to send out a significant number of notifications.

Code removal requests – CCIRC delivered 31 code removal requests (CRR) to Internet service and hosting providers informing them that malicious content was being hosted on their networks. Of these requests, 44% were reported as affecting organizations in the government, financial, and other sectors. 56% of the other CRRs were proactively identified by CCIRC.

CRRs are a CCIRC service that informs recipients that they are hosting malicious content, website forgeries, and personal information and requests that it be removed. When CCIRC becomes aware of malicious content it sends CRRs to implicated local, national, and international Internet service and hosting providers.





CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

NOTEWORTHY INCIDENTS

1. Oracle Java vulnerabilities and exploits

CCIRC became aware of an Oracle Java vulnerability that was being exploited and allowing malicious actors to break out of the Java Runtime sandbox. Oracle has released a patch to fix this problem and CCIRC provided its partners with a cyber flash containing contextual information and mitigation advice (CF12-004).

2. Phishing emails spoof the Canada Revenue Agency

Malicious emails appearing to originate from the Canada Revenue Agency (CRA) were widely reported by Canadians and businesses. These emails contained an attachment, that when opened, attempted to download a malicious Windows executable file. CCIRC released a cyber flash containing contextual information and mitigation advice (CF12-005).

3. Java exploits lead to data theft

CCIRC became aware of malware that was seeking to steal data from multiple organizations. This malware was downloaded when unsuspecting visitors were redirected to various advertisement sites that downloaded a malicious Java Archive. CCIRC released a cyber flash containing contextual information and mitigation advice (CF12-006).

TOP FIVE MITIGATION ACTIONS

The following five recommended actions will protect your organization from 85% of malicious cyber activity. CCIRC recommends that Canadian organizations implement them.

1. **Patch critical application vulnerabilities as soon as possible (e.g. PDF viewer, Flash Player, Microsoft Office and Java). Use the latest version of applications.**
2. **Patch critical operating system vulnerabilities as soon as possible. Use the latest operating system version.**
3. **Minimise the number of users with administrative privileges. Users should use a separate non-administrative account for email and web browsing.**
4. **Undertake application whitelisting to help prevent malicious software and other unapproved programs from running (e.g. using Microsoft Software Restriction Policies or AppLocker).**
5. **Utilise a host-based anti-virus and Intrusion Detection / Prevention System to identify anomalous behaviors. Keep systems up to date.**

See Annex B for a complete list of 35 mitigation actions for which there is broad international consensus.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

4. Flame / sKyWIper malware

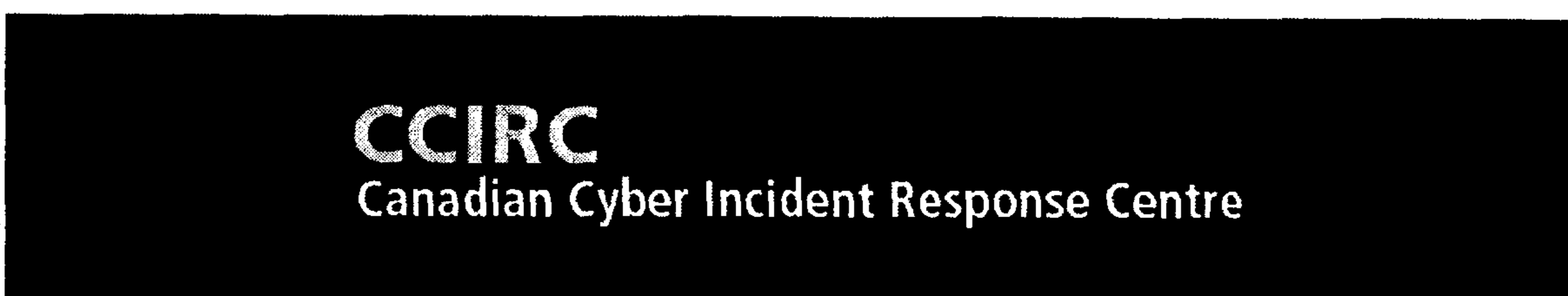
CCIRC tracked activity related to Flame / sKyWIper malware. This malware contained worm-like features allowing it to spread through removable media, malicious links, and email attachments. The malware was used for data exfiltration and had the capability to intercept network traffic, take screenshots, and record audio and keystrokes. At this time, CCIRC is not aware of any Canadian clients affected by this malware. However, it has released a cyber flash containing contextual information and mitigation advice (CF12-007).

5. Ongoing and increased activity linked to the Zeus malware

CCIRC observed suspicious activity indicative of Zeus-based malware infections. Zeus is a malware that is used to steal banking information, credentials, and personal information and is downloaded onto a computer from a drive-by download or phishing scheme. Zeus targets newer Windows Operating Systems, logs keystrokes, and takes screen captures. CCIRC released a cyber flash containing contextual information and mitigation advice (CF12-008).

6. Canada Post email phishing campaign

CCIRC became aware of an email phishing campaign in which malicious actors were falsely representing Canada Post in order to deliver malware to recipients. This event is related to, and used the same infrastructure as the phishing emails that spoofed the CRA. There were multiple variations of the email in circulation instructing the recipient to: print the email and visit their nearest Canada Post outlet; click a link in the email to view the delivery status; or, click a link to download a shipping invoice. Clicking on the link prompted the recipient to open or save a .ZIP file. This file contained malicious software and it has been reported that Zeus variants have been installed. CCIRC released a cyber flash containing contextual information and mitigation advice (CF12-009).



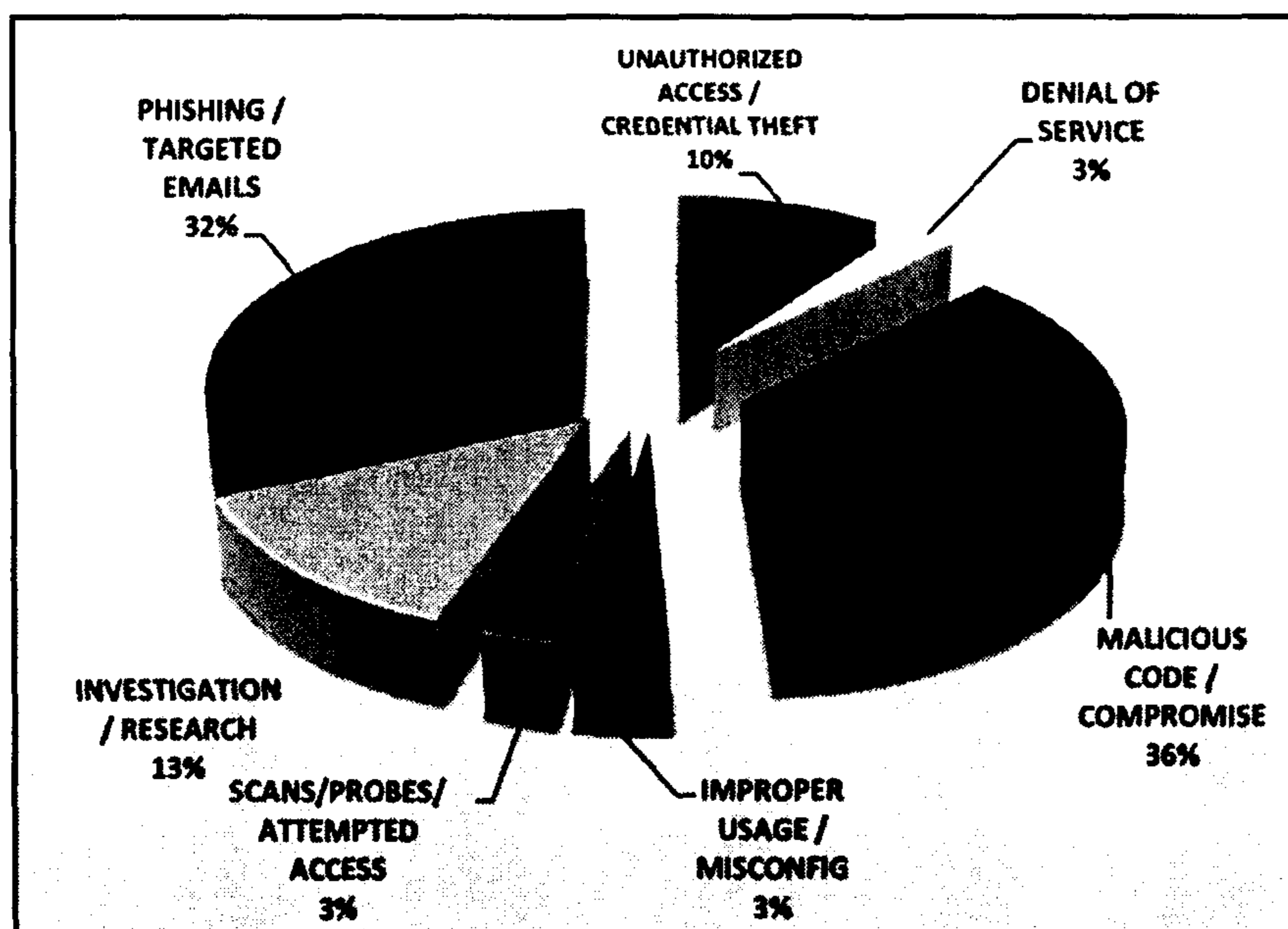
BUILDING A SAFE AND RESILIENT CANADA

TREND ANALYSIS

The Canadian private and public sector partners with the greatest take-up of CCIRC's products and services have been the financial, ICT, energy and utilities, and government sectors. These enhanced partnerships have provided CCIRC with targeted data, and as such, these sectors are the initial focus of analysis. Going forward, this summary will add other sectors as they strengthen their partnership with CCIRC. Definitions of incident categories are provided in Annex A.

There are two important caveats regarding the statistics used in this analysis. First, certain incidents can affect organizations in multiple sectors. To represent this as accurately as possible, these incidents are accounted for in each affected sector rather than in only one. Second, certain incidents fall into more than one incident category and some of the statistics in this report may reflect this discrepancy.

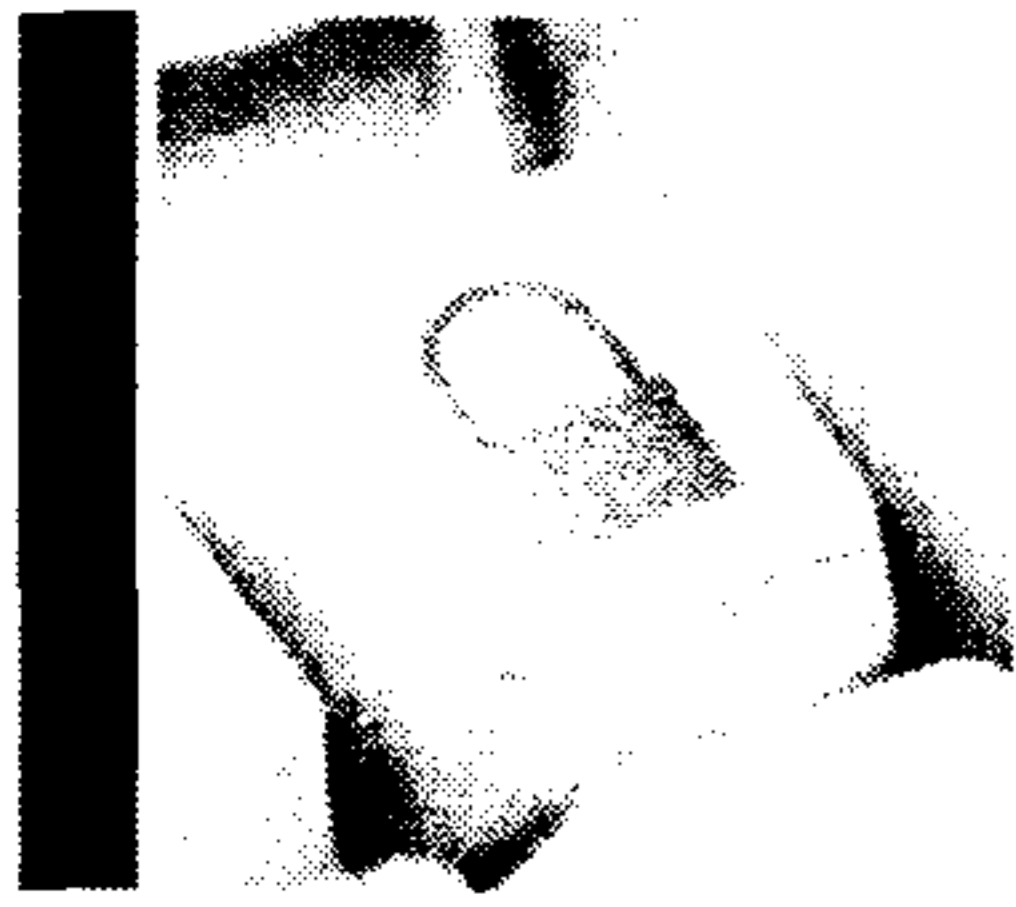
CCIRC INCIDENTS



CCIRC handled 237 incidents during this reporting period, a 45% increase from the previous quarter. Malware attacks (e.g. viruses, key logging, and Trojan horses) and phishing attacks (i.e. attempts to acquire personal or sensitive information by impersonating a trustworthy source) were the most common cyber threats observed by CCIRC – totalling 68% of the incidents handled.

Unauthorized access / credential theft, denial of service, improper usage / misconfiguration, and scans / probes / attempted access totalled 19% of incidents handled.

Comment: This rise in observed incidents may be attributed to a surge in the number of CCIRC staff, the pilot of an information sharing trial with the province of Ontario, and the development of a standard operating procedure to facilitate information sharing with the 33 members of the Canadian Electricity Association.



BUILDING A **SAFE AND RESILIENT CANADA**

TRENDS OBSERVED BY CCIRC

| Category | Unauthorized Access | | | | Malicious Code | | | | Scans / Probes | | | | Phishing | | | | | | | | | | | |
|----------|---------------------|------|---|----|----------------|---|---|------|----------------|----|------|---|----------|------|---|---|-------|---|----|------|---|----|------|---|
| Jan-Mar | 164 | 59% | ↑ | 3 | 767% | ↑ | 1 | 600% | ↑ | 73 | 30% | ↑ | 4 | 125% | ↑ | 2 | 250% | ↑ | 25 | 36% | ↑ | 56 | 46% | ↑ |
| Apr-Jun | 260 | | | 26 | | | 7 | | | 95 | | | 9 | | | 7 | | | 34 | | | 82 | | |
| Jan-Mar | 40 | 70% | ↑ | 1 | 400% | ↑ | 0 | | | 30 | 3% | ↑ | 1 | 100% | ↑ | 1 | 500% | ↑ | 5 | 80% | ↑ | 2 | 450% | ↑ |
| Apr-Jun | 68 | | | 5 | | | 4 | | | 31 | | | 2 | | | 6 | | | 9 | | | 11 | | |
| Jan-Mar | 44 | 59% | ↑ | 1 | -100% | ↓ | 0 | | | 35 | 29% | ↑ | 1 | | | 0 | | | 4 | 75% | ↑ | 3 | 433% | ↑ |
| Apr-Jun | 70 | | | 0 | | | 0 | | | 45 | | | 1 | | | 1 | | | 7 | | | 16 | | |
| Jan-Mar | 27 | 19% | ↑ | 0 | | | 0 | | | 23 | -17% | ↓ | 0 | | | 1 | -100% | ↓ | 2 | 200% | ↑ | 1 | 500% | ↑ |
| Apr-Jun | 32 | | | 0 | | | 0 | | | 19 | | | 1 | | | 0 | | | 6 | | | 6 | | |
| Jan-Mar | 68 | -24% | ↓ | 0 | | | 0 | | | 13 | -38% | ↓ | 0 | | | 0 | | | 6 | -33% | ↓ | 49 | -29% | ↓ |
| Apr-Jun | 52 | | | 4 | | | 0 | | | 8 | | | 0 | | | 1 | | | 4 | | | 35 | | |

The ICT and government sectors were the largest targets of malware attacks, accounting for 76 observed cases – a 29% and 3% respective increase from the first quarter. The financial sector was used by malicious individuals as a lure for 35 phishing incidents – a 27% reduction from the last quarter.

Comment: The government and ICT sectors witnessed various malicious code attacks over this reporting period for a number of different reasons, including hacktivism and state sponsored activity. In the past, CCIRC observed phishing attacks increase around tax time. The decrease in phishing incidents is likely due to the fact that this reporting period only covers one month of the Canadian personal tax season (April).

REPORTS RECEIVED

CCIRC received 50 cyber incident reports from private and public sector partners, which represents a 22% decrease from the last reporting period. CCIRC's effectiveness depends on its partners' reports and if you have incidents of concern please contact CCIRC at [REDACTED] Going forward, CCIRC will be focused on increasing its trusted partnerships.

RECENT CYBER TRENDS OBSERVED BY CCIRC

CCIRC observed that **advanced persistent threats** (a group with both the capability and the intent to persistently and effectively target a specific entity); **crimeware** (a class of malware designed specifically to automate cybercrime), and **hacktivism threats** (the use of computer networks to protest / promote political ends) increased in both number and sophistication. Going forward, these trends will likely have an impact on CCIRC's private and public sector partners.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

ABOUT CCIRC

Mandate

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity. As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events. CCIRC provides authoritative advice and support to, and coordinates information sharing and event response among, all levels of government, the public and private sectors, critical infrastructure sectors, information technology vendors, and international counterparts.

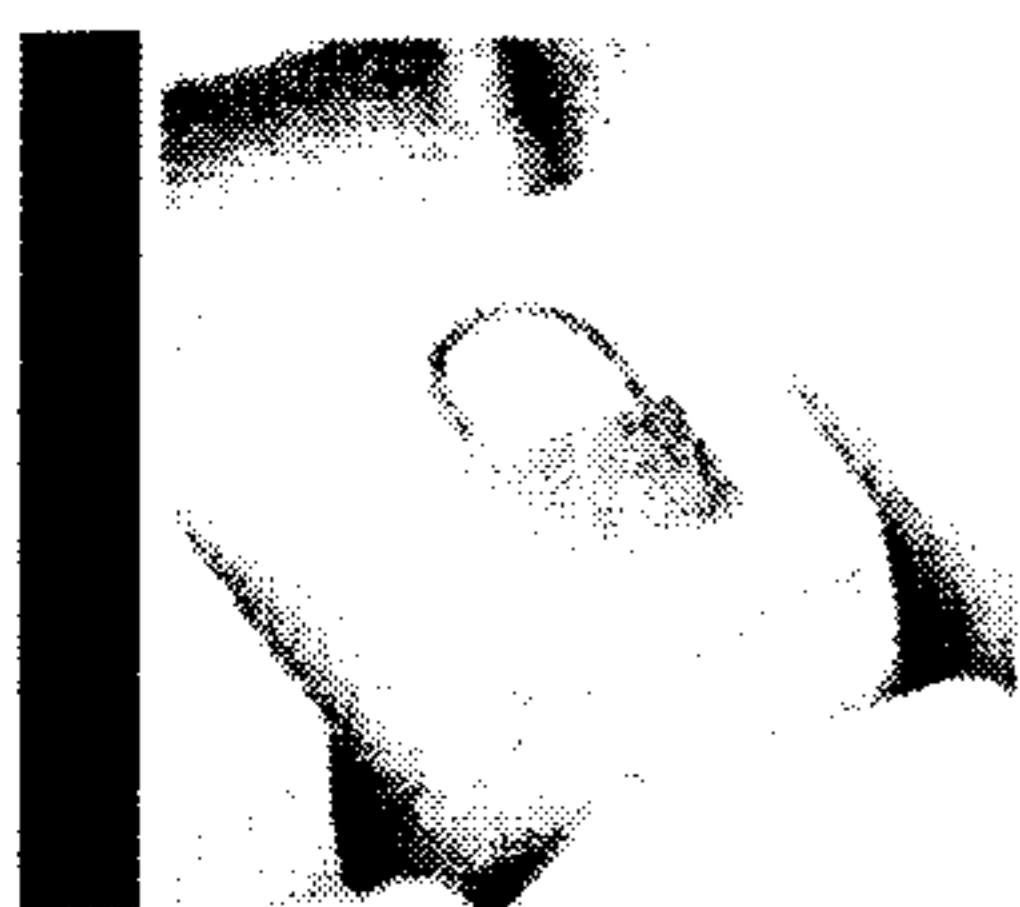
Core functions

To deliver on its mandate, CCIRC:

- Builds and maintains trusted relationships and information sharing mechanisms with partners and clients;
- Disseminates a variety of cyber information products based on data from domestic and international partners and sources;
- Conducts daily cyber operations such as code removal requests related to malicious sites, the notification of compromised systems, and the repatriation of stolen data; and
- Maintains the protocols and mechanisms for coordinating the national cyber incident response in collaboration with law enforcement and intelligence.

Background

Created in 2005 and housed within Public Safety Canada's National Cyber Security Directorate, CCIRC is Canada's national computer emergency readiness team. CCIRC works to reduce Canada's cyber risk by enhancing the cyber security of public and private sector partners and ensuring a coordinated national response to significant cyber events.



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

RECENT DEVELOPMENTS

The last three months have seen CCIRC enhance its capacity and capabilities to contribute to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

STRENGTHENED ANALYTICAL CAPACITY

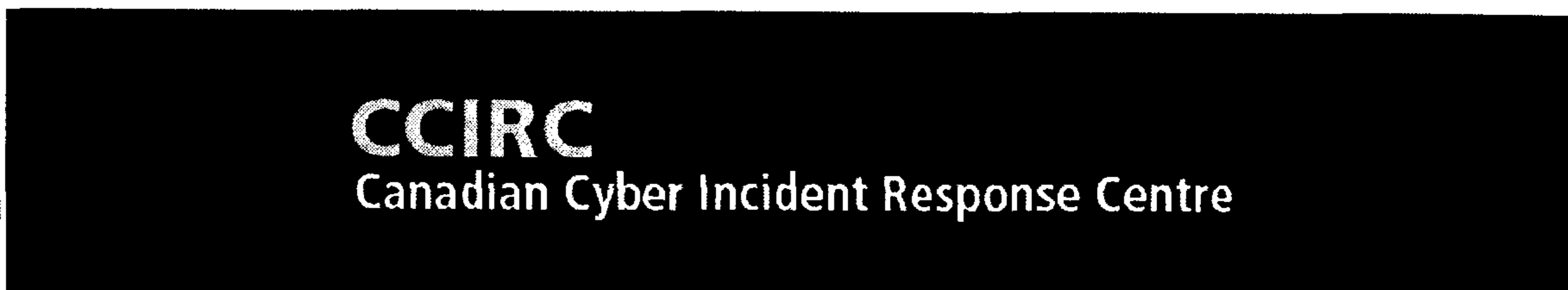
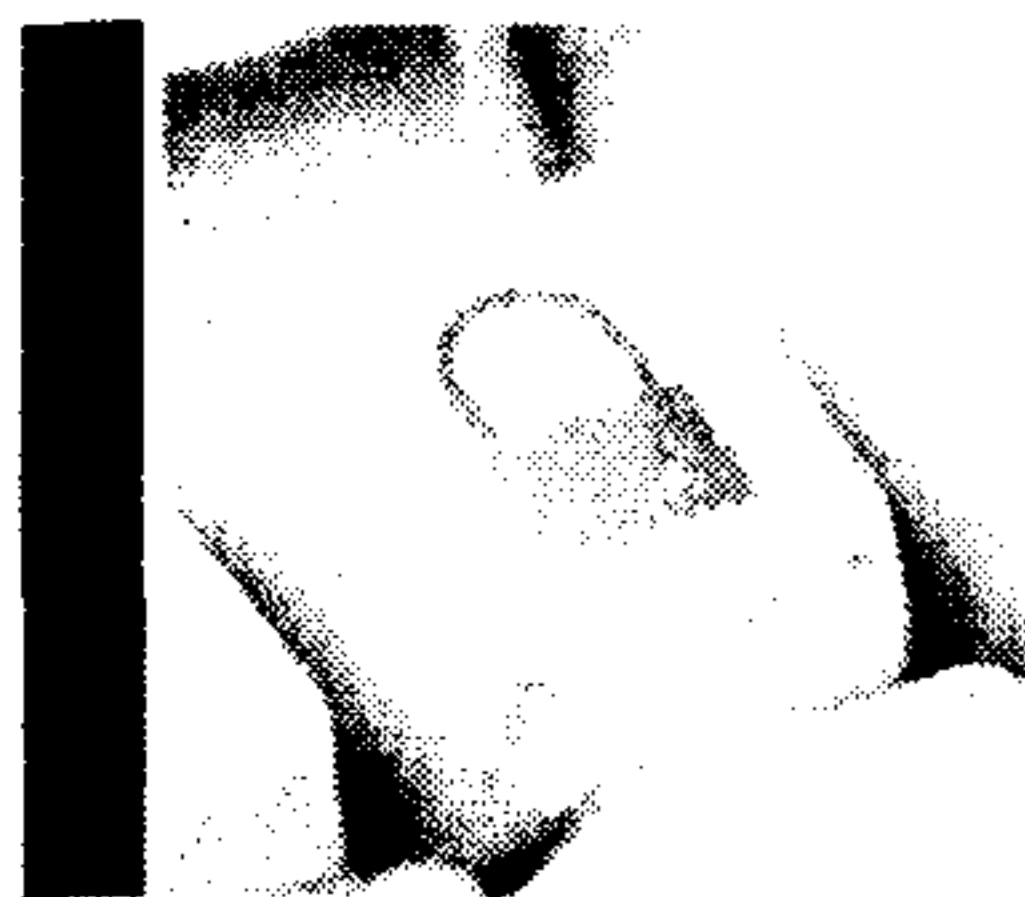
CCIRC has been moving forward to increase its mitigation advice and incident response capacity. A few of these initiatives include:

- **Lab upgrades** – CCIRC has invested in a number of specialized analysis tools that have been integrated into existing systems (e.g. [REDACTED]).
- **Stand-up of an operational support team** – This team's role is to provide senior management and partners with timely reports and information on cyber incidents; and
- **Industrial control systems project** – CCIRC is working on plans to integrate existing industrial control system (ICS) test beds into its lab to better help assess, test, and evaluate ICS network architectures, vulnerabilities, and defense mechanisms. This work is being carried out in collaboration with other federal ICS initiatives undertaken by the Royal Canadian Mounted Police and Natural Resources Canada.

DEEPENING PUBLIC AND PRIVATE SECTOR PARTNER COLLABORATION

CCIRC has been working to enhance incident response and coordination across Canada and to ensure the Government and its partners have increased situational awareness of the cyber environment. A few of these initiatives include:

- **New protocols and tools to enhance information sharing** – In response to specific partner needs, CCIRC has developed non-disclosure agreements and memoranda of understanding to set out expectations for handling of sensitive information. In addition, a CCIRC Community Portal has been soft-launched to offer a secure environment for collaboration and information sharing with partners;
- **Incident response trials** – CCIRC has started an incident response trial with the Province of Ontario. This initiative will soon be expanded to Alberta, Manitoba, and New Brunswick; and
- **Federal level synchronization** – Regular meetings between the federal security and intelligence operational leads is helping to quickly identify and resolve issues.



BUILDING A **SAFE AND RESILIENT CANADA**

ANNEX A – DEFINITIONS

| Name | Definitions |
|----------------------------------|---|
| Incident | An incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising the business operations and threatening the information security of system(s) of national significance within the Canadian private and public sectors. |
| Event | An event is an observable change to the normal behavior of a computer, IT system, environment, process, or workflow that may impact or may pose a threat to the system or data integrity, or safety and security. An event can be “upgraded” and become an incident if it becomes apparent that the change observed has a probable negative impact and requires mitigation or advice. |
| Activity | These are “back-of-house” procedures that occur on a daily basis, and that cannot be classified as an event or an incident. In general, they include administrative tasks, or support functions to events or incidents. |
| Unauthorized Access | In this category an individual gains logical or physical access without permission to a network, system, application, data, or other resource |
| Denial of Service (DoS) | An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. |
| Malicious Code | <i>Successful</i> installation of malicious software (e.g. virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. |
| Improper Usage | Any activity that violates acceptable computing use policies. |
| Scans/Probes /Attempted Access | This category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. |
| Investigation | <i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. |
| Phishing / Targeted Emails | A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Criminally-fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. |
| Advance Persistent Threat (APT): | Adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors. Objectives typically include: establishing and extending footholds within the information technology infrastructure of the targeted organizations for purpose of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives. The APT pursues its objectives repeatedly over an extended period of time; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives. |
| Crimeware | Crimeware is malicious software that is covertly installed on computers and has the ability to 'steal' confidential information and send it back to cyber criminals. One form of crimeware is ransomware, which is software that denies access to a person's files until they pay a ransom. |
| Hacktivism | Some groups of computer hackers are not motivated by financial gain and instead are driven by economic, political, or religious interests that generally go beyond their nation's borders. Their actions are called hacktivism, which is a merger of hacker and political activism. Hacktivists infiltrate networks and put their talents to work for their beliefs by organizing computer attacks, including piracy, hijacking servers, and replacing homepages with ideological messages. |



CCIRC Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

ANNEX B – TOP 35 RECOMMENDED MITIGATION ACTIONS

Australian Government's Defense Signals Directorate (DSD) has produced a valuable list of recommended cyber threat mitigation strategies. Below is the DSD list in order of effectiveness.

| Ranking | Mitigation Strategy |
|---------|---|
| 1 | Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications. |
| 2 | Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version. |
| 3 | Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing. |
| 4 | Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker. |
| 5 | Host-based Intrusion Detection/Prevention System to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking. |
| 6 | Whitelisted email content filtering allowing only attachment types required for business functionality. Preferably convert/sanitise PDF and Microsoft Office attachments. |
| 7 | Block spoofed emails using Sender Policy Framework checking of incoming emails, and a 'hard fail' SPF record to help prevent spoofing of your organisation's domain. |
| 8 | User education e.g. Internet threats and spear phishing socially engineered emails. Avoid weak passphrases, passphrase re-use, exposing email addresses, and unapproved USB devices. |
| 9 | Web content filtering of incoming and outgoing traffic, using signatures, reputation ratings and other heuristics, and whitelisting allowed types of web content. |
| 10 | Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. |
| 11 | Web domain whitelisting for HTTPS/SSL domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. |
| 12 | Workstation inspection of Microsoft Office files for abnormalities e.g. using the Microsoft Office File Validation feature. |
| 13 | Application based workstation firewall, configured to deny traffic by default, to protect against malicious or otherwise unauthorised incoming network traffic. |
| 14 | Application based workstation firewall, configured to deny traffic by default, that whitelists which applications are allowed to generate outgoing network traffic. |
| 15 | Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. |
| 16 | Multi-factor authentication especially implemented for when the user is about to perform a privileged action, or access a database or other sensitive information repository. |
| 17 | Randomized local administrator passphrases that are unique and complex for all computers. Use domain group privileges instead of local administrator accounts. |
| 18 | Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words. |
| 19 | Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an email server, or an authenticated web proxy. |
| 20 | Data Execution Prevention using hardware and software mechanisms for all software applications that support DEP. |
| 21 | Antivirus software with up to date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors. |



CCIRC Canadian Cyber Incident Response Centre

BUILDING A **SAFE AND RESILIENT CANADA**

- 22 Non-persistent virtualised trusted operating environment with limited access to network file shares, for risky activities such as reading email and web browsing.
- 23 Centralized and time-synchronized logging of allowed and blocked network activity, with regular log analysis, storing logs for at least 18 months.
- 24 Centralized and time-synchronized logging of successful and failed computer events, with regular log analysis, storing logs for at least 18 months.
- 25 Standard Operating Environment with unrequired operating system functionality disabled e.g. IPv6, autorun and Remote Desktop. Harden file and registry permissions.
- 26 Workstation application security configuration hardening e.g. disable unrequired features in PDF viewers, Microsoft Office applications, and web browsers.
- 27 Restrict access to NetBIOS services running on workstations and on servers where possible.
- 28 Server application security configuration hardening e.g. databases, web applications, customer relationship management and other data storage systems.
- 29 Removable and portable media control as part of a data loss prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.
- 30 TLS encryption between email servers to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.
- 31 Disable LanMan password support and cached credentials on workstations and servers, to make it harder for adversaries to crack password hashes.
- 32 Block attempts to access web sites by their IP address instead of by their domain name.
- 33 Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- 34 Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.
- 35 Full network traffic capture to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days.



BUILDING A SAFE AND RESILIENT CANADA

CCIRC'S QUARTERLY REPORT – FEEDBACK FORM

1. Please rank the sections in terms of value-added for you *(1 = highest; 6 = lowest)*

- | | |
|--|---|
| <input type="checkbox"/> Products | <input type="checkbox"/> Trend analysis |
| <input type="checkbox"/> Services | <input type="checkbox"/> About CCIRC |
| <input type="checkbox"/> Noteworthy events | <input type="checkbox"/> Annexes |

Comments

Click here to enter text.

2. Which sections do you feel could use additional detail or analysis?

- | | |
|--|---|
| <input type="checkbox"/> Products | <input type="checkbox"/> Trend analysis |
| <input type="checkbox"/> Services | <input type="checkbox"/> About CCIRC |
| <input type="checkbox"/> Noteworthy events | <input type="checkbox"/> Annexes |

Comments

Click here to enter text.

3. The statistics are based primarily on information submitted to CCIRC by its partners. Does your organization submit incident reports to CCIRC? If not, why?

Comments

Click here to enter text.

4. Do you have any suggestions to improve this product?

Comments

Click here to enter text.

5. Overall, would a quarterly product like this be useful to your organization?

Comments

Click here to enter text.



Public Safety Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

CONFIDENTIAL

DATE: **DEC 21 2012**

File No.: 392052

RDIMS No.: 736288

MEMORANDUM FOR THE MINISTER

**INTERNATIONAL TRAVEL AUTHORITY FOR LYNDA CLAIRMONT
AND ROBERT GORDON TO CONDUCT BILATERAL MEETINGS WITH
SOUTH AMERICAN CYBER SECURITY PARTNERS FEBRUARY 3-17, 2013**

(Signature required)

ISSUE

Your approval is sought for Lynda Clairmont, Senior Assistant Deputy Minister, and Robert Gordon, Special Advisor, National Cyber Security, to travel to South America (Brazil, Argentina, Colombia, Chile and Uruguay) from February 3 to 17, 2013. This visit is part of Canada's initiative to support global efforts on cyber security, including supporting capacity building in the Americas.

BACKGROUND

Under *Canada's Cyber Security Strategy*, Canada has made a commitment to working internationally to promote an open, secure and trusted cyber community. Engagement and capacity building in Latin America have been emphasized given the importance of the Americas as one of Canada's foreign policy priorities.

the Beyond the Border Action Plan commits Canada to strengthening cooperation on international cyber security and internet governance issues.

In this regard, Canadian objectives are to support cyber capacity building to enhance hemispheric security, particularly for critical infrastructure protection, as well as to help encourage the development of cyber security policies.

As a part of Canada's leadership efforts, Public Safety Canada (PS) recently hosted a policy roundtable on cyber security with the Organization of American States (OAS), on

Canada

.../2

s.13(1)(a)

s.15(1) - Int'l

000066

CONSIDERATIONS

The proposed bilateral meetings would be an opportunity to build on the key regional relationships established at the September 2012 OAS Roundtable and would further advance Canadian objectives in the area of cyber security. The itinerary would also include briefings at Canadian embassies in each country to brief them on Canada's cyber security activities, regional cooperation and country specific objectives.

The meetings will focus on cyber security policy issues, as well as enhanced operational cooperation among national Computer Emergency Response Teams (CERTs), which is essential for protecting critical infrastructure from cyber attacks. Country specific objectives are outlined below.

Brazil

Argentina

Argentina has invested significant resources to address cyber security issues, with the Presidential Cabinet creating a new Program for Critical Infrastructures and Cyber Security. Additionally, Argentina is increasing its profile internationally and playing a larger regional role, notably in hosting the 2013 Meridian Conference on Critical Information Infrastructure Protection. This is an international forum supported by both PS and the U.S. During the November 2012 Meridian Conference, Mr. Gordon and a representative from the U.S. Department of Homeland Security (DHS), provided a joint presentation highlighting the collaboration between the two countries. Meetings with officials will give Canada the opportunity to encourage Argentina's continued regional leadership in this area, and to build on discussions from the Meridian Conference.

Colombia

Colombia is focused on increasing collaboration between the public and private sectors, including training programs, awareness campaigns and establishing metrics to track the success of cyber security efforts. Meetings with key officials will be an opportunity to share best practices on engaging the private sector.

Chile

Chile's cyber security policies are aligned with Canadian and American approaches, and as a regional leader, Chile is in a key position to influence other countries in South America to adopt similar policies, as well as to help promote hemispheric capacity building. Discussions with officials will allow Canada to express support for these objectives.

.../3

s.13(1)(b)

s.15(1) - Int'l

Uruguay

While smaller than its regional neighbours,

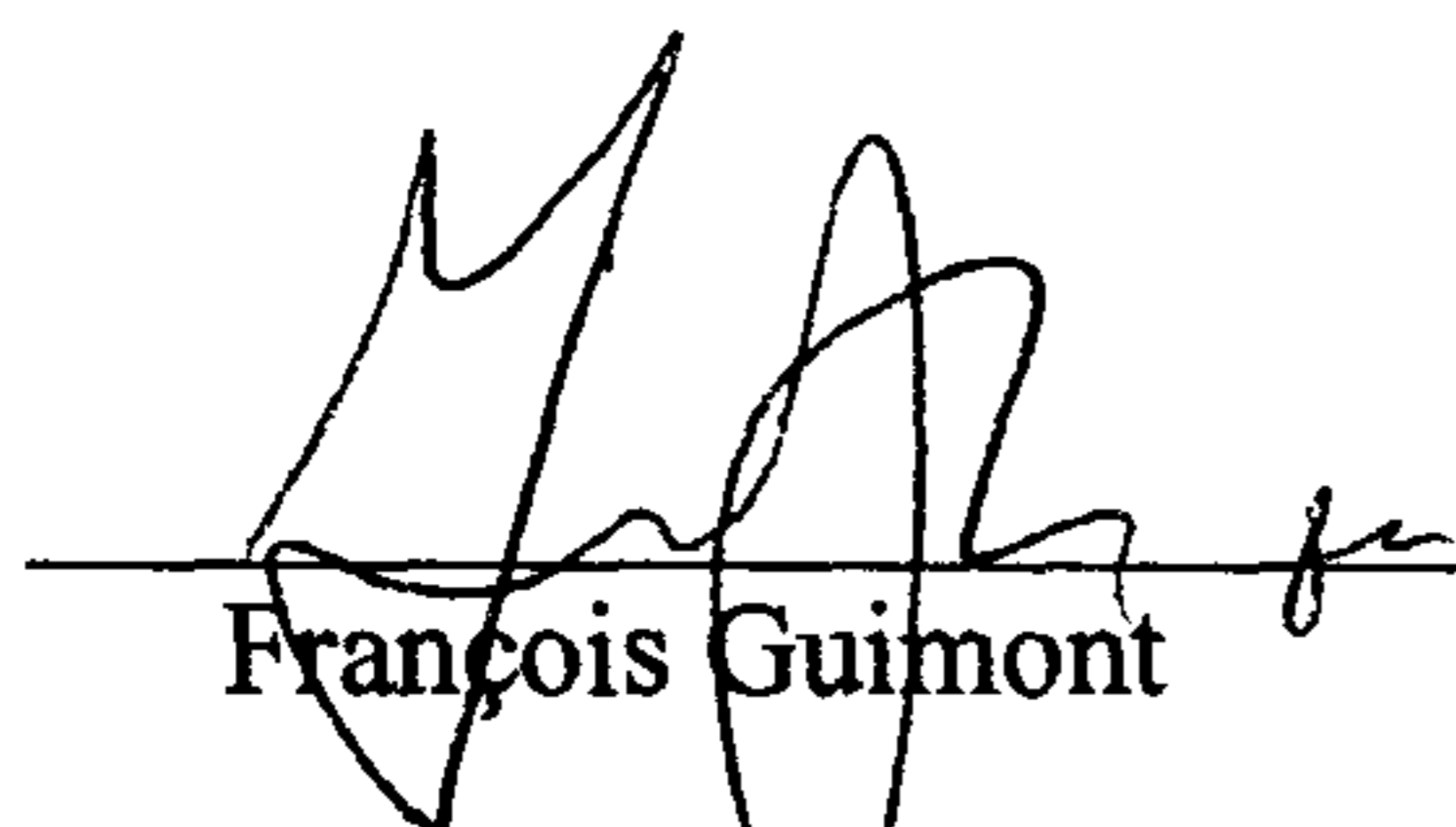
Additional bilateral meetings will be arranged in all countries with key senior cyber security interlocutors. PS is working closely with Canadian embassy officials, as well as directly with government departments each country, to develop a detailed itinerary for the trip. It is expected that the details for each meeting will be finalized over the coming weeks.

The estimated cost for the two travellers is \$36,075.47. All costs related to this request fall within the Department's Travel, Hospitality and Conference cap for this fiscal year.

RECOMMENDATION

It is recommended that you approve this travel authorization request by signing the Travel Authority and Advance forms (**TAB A**). The International Travel Request is included for your information (**TAB B**).

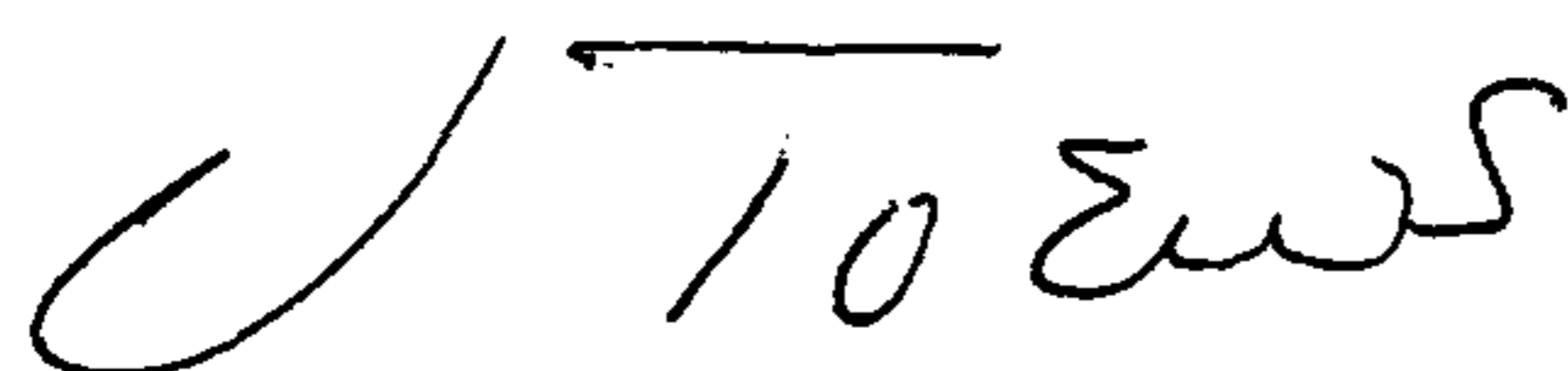
Should you require additional information, please do not hesitate to contact me or Ms. Lynda Clairmont, Senior Assistant Deputy Minister, National Security at 613-990-4976.


François Guimont

Enclosures: (3)

I approve:

I do not approve:



JAN 10 2013

Vic Toews, P.C., Q.C., M.P.

Vic Toews, P.C., Q.C., M.P.

Prepared by: Adriana Lopez-Ramirez

Original / Prem. demande

Amended (Same levels of approval as original dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

| | | |
|---|--|---|
| Department - Ministère Public Safety Canada | 14A Travel Authority No. (TAN) N°. d'aut de voyager (NAV) LNW9 | 736909 |
| Address - Adresse 340 Laurier Ave W. | Type 2 Name of traveller - Nom du voyageur Robert Gordon | Classification EX-05 |
| Branch Contact - Personne ressource a la direction Jane Hayward | Branch / Division / Group - Direction / Division / Groupe NS-NCSD-DG | |
| Purpose of travel - Objet du voyage Meetings with South American counterparts | Telephone No. - No. de téléphone 949-7380 | If different address, send cheque to: Si adresse différente, envoyer chèque à |
| | Telephone No. - No. de téléphone 613-991-1982 | |
| | No. of days Nbre de jours 17 | Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage (CV)? <input checked="" type="checkbox"/> Yes / Oui <input type="checkbox"/> No / Non |
| | | If no, would you like to request one? Les cas échéant, aimerez-vous en avoir une? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> 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 | | No. of meals prepaid Nbre de repas prépayés | Accommodation Hébergement | File locator number N°. de repérage du dossier |
|-------------------|------------------|--------------------|---|-----------------------------|----------|--|------------------------------|--|
| | | | | Mode | Class | | | |
| 3-Feb-13 | Ottawa YOW | Bogota BGO | 07:00- 21:01 | Air | Business | 2 | | |
| 6-Feb-13 | Bogota BGO | Rio de Jan (GIG) | 21:53 - 07:23 | Air | Business | 1 | | |
| 10-Feb-13 | Rio de Jan (GIG) | Uruguay (MVD) | 07:44-10:50 | Air | Business | 1 | | |
| 12-Feb-13 | Uruguay (MVD) | Buenos Aires (AEP) | 13:00 - 12:45 | Air | Business | 2 | | |
| 14-Feb-13 | Buenos Aires | Santiago | 12:45 - 15:10 | Air | Economy | 0 | | |
| 16-Feb-13 | Santiago | Cancun | 09:20 - 14:40 | Air | Business | 1 | | |
| 16-Feb-13 | Cancun | Ottawa | 22:40 - 03:40 (+1) | Air | Business | | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel |
|--|----------------------------------|---|----------------------------------|---|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif | |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$2,691.00 | Accommodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | Assistant Deputy Minister level Part D - Partie D Estimated Cost - Coût estimatif Prepaid - Prépayé \$11,000.00 Other - Autre \$5,111.33 Trip Total - Coût total du voyage \$16,111.33 Funding - Financement A) Travellers cheques / Cheques 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 |
| 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: <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$74.80 | Other (Specify) - Autre (préciser) Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | \$0.00 | |
| Transportation Transport | \$600.00 | <input checked="" type="checkbox"/> First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) <input type="checkbox"/> Business class / Other-Upgraded (other than article 3.1.9) 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) | | |
| Meals and incidentals Repas et frais accessoires | \$1,375.53 | | | |
| Other (Specify) - Autre (préciser) Breakfast | \$370.00 | | | |
| | | Approval - Approbation | | |

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] 2012/2/07

Signature Date

| | | | |
|---|------|--|-------------|
| Recommended by (signature) - Recommandé par (signature) | Date | Approved by (signature) - Approuvé par (signature) | Date |
| | | <i>[Signature]</i> | 09 Feb 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 |
|-----------|--------------------------------|-------------------|------------------|-----------------------------|---|-----------------------------|

Accounting Information / Renseignement comptables

| | | | | |
|-----------------------|-------------------------------|---|---|------------------|
| Sub-type Sous-type | Vendor Code Code du fourm. | Departmental Ref. No. No. de réf. Du ministère THC NCSD T61 | Coding - Cidification 475 - PSABASE - 2001 500102565 | Amount - Montant |
|-----------------------|-------------------------------|---|---|------------------|

| | |
|---|---|
| Description | Financial encumbrance No. No. de consignation de fonds |
| Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature) | Cheque No. - N° du cheque |
| Verified correct (PWGSC) (signature) Vérifié conform (TPSGC) (signature) | Date |
| Services officer (PWGSC) (signature) Agent responsable (TPSGC) (signature) | Signature |

WORKSHEET - FEUILLE DE TRAVAIL

| Estimated Cost - Coût estimatif: Prepaid - Prépayé | | | Amount/Montant |
|---|----------------------------|------------|-----------------|
| Airfare / Frais d'avion | | | \$11,000.00 |
| Train / Train | | | \$0.00 |
| Other / Autres | | | \$0.00 |
| | | | \$11,000.00 |
| Estimated Cost - Coût estimatif: Other - Autre | | | Amount/Montant |
| | Rate / Tarif | No. / Nbre | |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du rép | \$277.00 | 3 | \$831.00 |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du rép | \$200.00 | 3 | \$600.00 |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du rép | \$264.00 | 2 | \$528.00 |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du rép | \$196.00 | 2 | \$392.00 |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du rép | \$170.00 | 2 | \$340.00 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du réperto | \$0.00 | 0 | \$0.00 |
| | | | \$340.00 |
| 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 | |
| Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé | 0.550 | 136.0 | \$74.80 |
| | | | \$0.00 |
| | Rate / Tarif | No. / Nbre | |
| Parking & Tolls / stationnement et frais de péage | | \$0.00 | \$0.00 |
| Taxi/Limo | Home to Airport | | \$0.00 |
| | Airport - Hotel / Meetings | | \$200.00 |
| | Hotel - Airport | | \$200.00 |
| | Airport to Home | | \$0.00 |
| | Meeting - Meetings | | \$200.00 |
| | | | \$600.00 |
| Transportation / Transportation (No receipt) | \$10.00 | | \$0.00 |
| Ferry & Miscellaneous | | \$0.00 | \$0.00 |
| | | | \$600.00 |
| Canadian | | | Amount/Montant |
| | Rate / Tarif | No. / Nbre | |
| Breakfast / Petits déjeuners | \$15.50 | | \$0.00 |
| Lunch / Déjeuners | \$15.00 | 1 | \$15.00 |
| Dinner / Diners | \$41.30 | | \$0.00 |
| Incidentals /Frais divers | \$17.30 | 1 | \$17.30 |
| Total Canadian | | | \$32.30 |
| Columbia | | | Amount/Montant |
| | Rate / Tarif | No. / Nbre | |
| Breakfast / Petits déjeuners | \$0.00 | | \$0.00 |
| Lunch / Déjeuners | \$28.55 | 3 | \$85.65 |
| Dinner / Diners | \$36.87 | 3 | \$110.61 |
| Incidentals /Frais divers | \$26.17 | 3 | \$78.51 |
| Total Columbia | | | \$274.77 |
| Brazil | | | Amount/Montant |
| | Rate / Tarif | No. / Nbre | |
| Breakfast / Petits déjeuners | \$12.79 | 3 | \$38.37 |
| Lunch / Déjeuners | \$30.19 | 3 | \$90.57 |
| Dinner / Diners | \$40.99 | 3 | \$122.97 |
| Incidentals /Frais divers | \$26.87 | 3 | \$80.61 |
| Total Brazil | | | \$332.52 |
| Uruguay | | | Amount/Montant |
| | Rate / Tarif | No. / Nbre | |
| Breakfast / Petits déjeuners | \$0.00 | | \$0.00 |
| Lunch / Déjeuners | \$38.00 | 3 | \$114.00 |
| Dinner / Diners | \$48.60 | 2 | \$97.20 |
| Incidentals /Frais divers | \$34.64 | 2 | \$69.28 |
| Total Uruguay | | | \$280.48 |
| Argentina | | | Amount/Montant |
| | Rate / Tarif | No. / Nbre | |
| Breakfast / Petits déjeuners | \$0.00 | | \$0.00 |
| Lunch / Déjeuners | \$25.43 | 2 | \$50.86 |
| Dinner / Diners | \$34.46 | 2 | \$68.92 |
| Incidentals /Frais divers | \$23.96 | 2 | \$47.92 |
| Total Argentina | | | \$167.70 |
| Chile | | | Amount/Montant |
| | Rate / Tarif | No. / Nbre | |
| Breakfast / Petits déjeuners | \$25.08 | 2 | \$50.16 |
| Lunch / Déjeuners | \$35.05 | 1 | \$35.05 |
| Dinner / Diners | \$44.95 | 3 | \$134.85 |
| Incidentals /Frais divers | \$33.85 | 2 | \$67.70 |
| Total Chile | | | \$287.76 |
| GRAND TOTAL | | | \$652.58 |
| Business Phone / Téléphone d'affaires | | | \$50.00 |
| Airport Improvement Fee / Frais de l'Aéroport | | | \$0.00 |
| Cash Advance Fee / Frais d'avances | | | \$20.00 |
| Misc. Business Services / Diverses charges d'affaires | | | \$0.00 |
| Miscellaneous / Diverses | | | \$300.00 |
| | | | \$370.00 |

**International Travel Request
Demande de voyage international**

| | | | |
|---|---|--|---|
| Event title - <i>Titre de l'événement</i> BILATERAL MEETINGS WITH SOUTH AMERICAN CYBER SECURITY PARTNERS | | Date of event - <i>Date de l'événement</i> | |
| | | From - <i>Du</i> : February 3 | To - <i>Au</i> : February 17 2013 |
| Location (City, Country) - <i>Lieu (Ville, Pays)</i> Region: South America Countries: Argentina, Brazil, Chile, Colombia, and Uruguay | | Estimated total cost - <i>Coût total prévu</i> \$ 36,075.47 | |
| Description of meeting (provide agenda) <i>Description de l'événement (joindre l'ordre du jour)</i> Ms. Clairmont and Mr. Gordon will meet with cyber security senior officials from each listed country to follow up on specific issues on cyber security. The final itinerary would include briefings at Canadian embassies in each country to apprise them of Canada's cyber security activities and country specific objectives. The meeting agendas are still in development. The names of the individuals with whom they will be meetings are included in the covereing memo. Brazil Discussions will be arranged with: [REDACTED] [REDACTED] Argentina Discussions will be arranged with: [REDACTED] [REDACTED] Uruguay Discussions will be arranged with: [REDACTED] [REDACTED] Colombia Discussions will be arranged with: [REDACTED] [REDACTED] Chile Discussions will be arranged with: [REDACTED] [REDACTED] | | Pre-approved under Branch travel plans? <i>Pré-approuvé selon les directives sur les voyages de la direction générale?</i> <input checked="" type="checkbox"/> Yes/Oui <input type="checkbox"/> No/Non | |
| Participant(s) | | | |
| Name (s) <i>Nom (s)</i> | Directorate/Branch <i>Direction générale/Secteur</i> | Work address <i>Adresse au travail</i> | Telephone No. <i>N° de telephone</i> |
| Lynda Clairmont Robert Gordon | National Security NS-NCSD | 269 Laurier Avenue West 340 Laurier Avenue West | 613-990-4976 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.) <i>Objectif du voyage et rôle du voyageur (p. ex. conférence annuelle, conférencier principal, visite d'études/d'apprentissage, membre d'une délégation canadienne, etc.)</i> Canadian delegation. | | | |
| Description of how event advances Department's priorities and expected outcomes <i>Comment l'événement permet t'il l'avancement des priorités du Ministère et des résultats attendus</i> This is an opportunity to build on the relationships established at the Organization of American States (OAS) Roundtable hosted by Public Safety Canada in Ottawa, September 2012 and further Canadian objectives in the region. The meetings will focus both on cyber security policy issues as well as operational cooperation among Computer Emergency Response Teams (CERTs) involved in protecting critical infrastructure from cyber attacks. Under Canada's Cyber Security Strategy, Canada has made a commitment to working internationally to promote an open, secure and trusted cyber community. Engagement and capacity building in Latin America have been a focus given the importance of the Americas in Canada's foreign policy priorities [REDACTED] [REDACTED] | | | |

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement

N/A

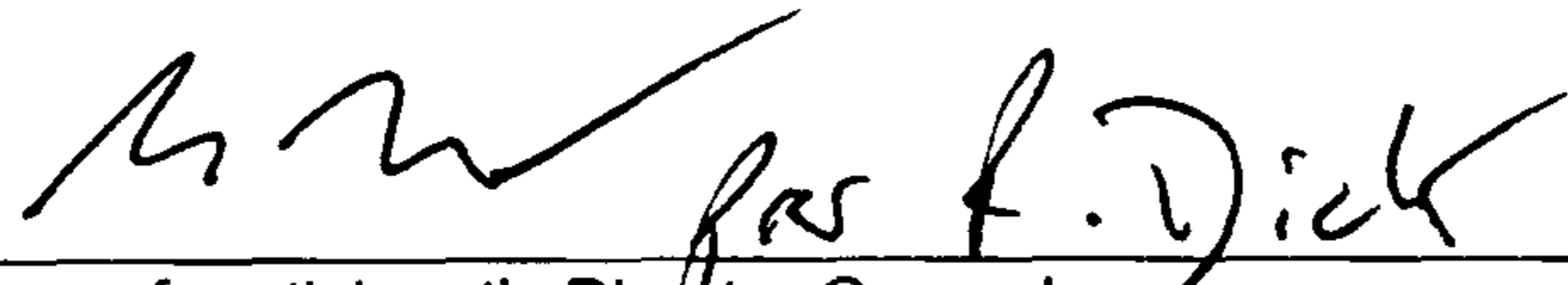
Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

N/A

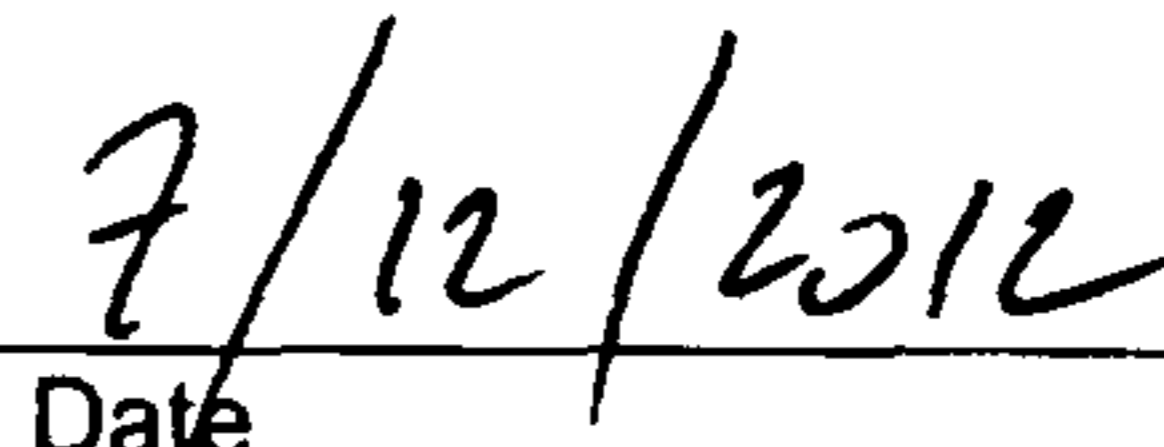
It is understood that a brief (2-3 page) post-travel report will be submitted (to include synopsis, follow-up, and advancement of Department's priorities) no later than 10 business days upon return. Travellers should notify appropriate Canadian Embassy officials in advance of travel and include DFAIT 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

Reviewed by/
Examiné par :

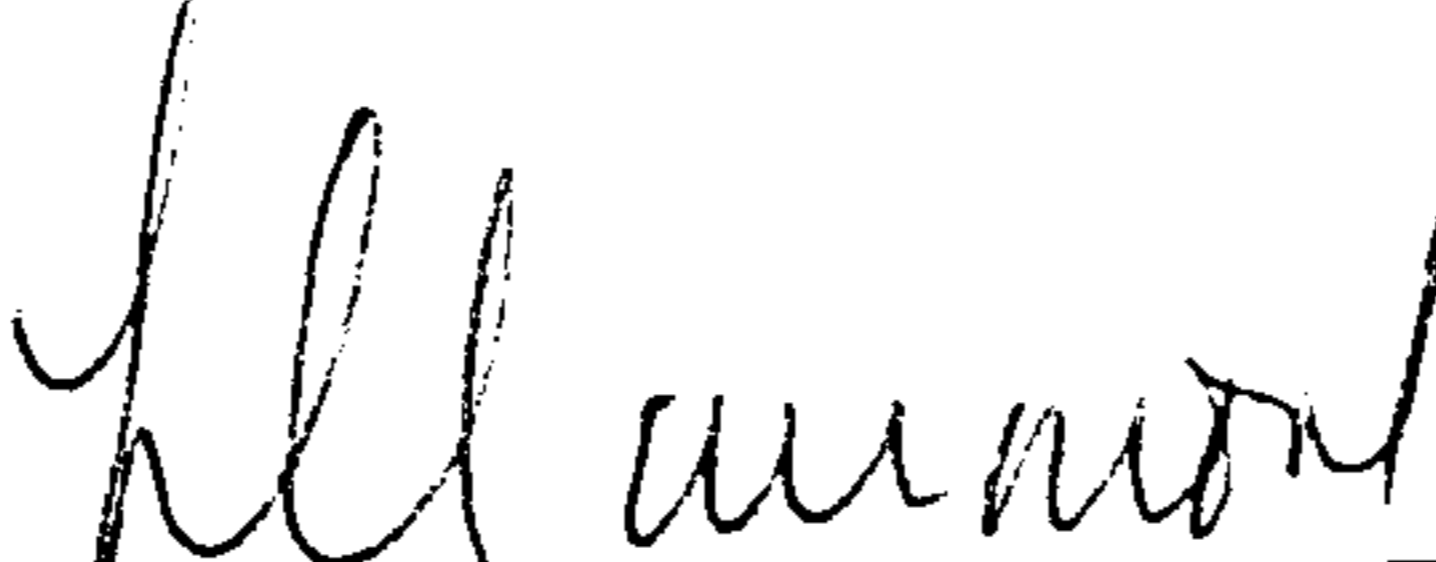


Director General, International Affairs Directorate
Directeur Générale, Direction générale des affaires internationales

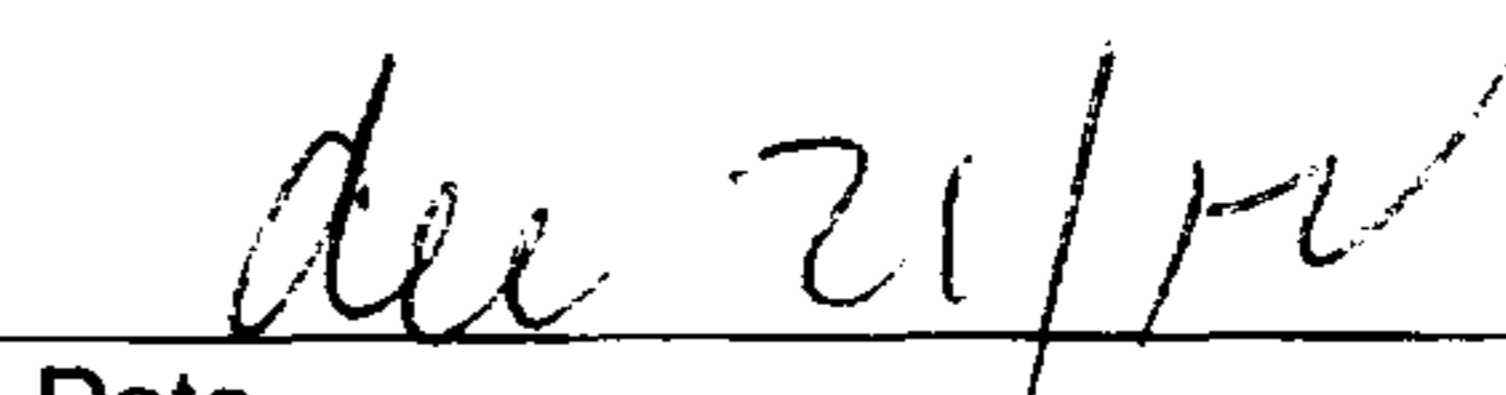


Date

Approved by/
Approuvé par :



Name of participant's Assistant Deputy Minister
Nom du sous-ministre adjoint du voyageur



Date



Public Safety Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: DEC 21 2012

File No.: 391919

RDIMS No.: 734053

MEMORANDUM FOR THE MINISTER

**INTERNATIONAL TRAVEL AUTHORITY FOR
LYNDA CLAIRMONT, ROBERT GORDON,
STEPHANIE DURAND, WINDY ANDERSON AND CHRISTINE
BINNE TO ATTEND THE RSA CONFERENCE AND BILATERAL
MEETINGS IN SAN FRANCISCO, FEBRUARY 23 - MARCH 2, 2013**

(Decision sought)

ISSUE

Your approval is being sought for Ms. Lynda Clairmont, Senior Assistant Deputy Minister, National Security, to lead a small delegation to participate in a series of bilateral and technical meetings on cyber security, and attend the RSA Conference, in San Francisco, United States (U.S.), from February 25 - March 1, 2013.

BACKGROUND

The RSA Conference is one of the largest international information security conferences with annual industry events in the U.S., Europe and Asia. RSA is the security division of the EMC Corporation, which is a global leader among technology companies. A copy of the conference schedule is attached for your information (TAB A).

The 2013 Conference will cover more than 275 sessions across 22 themes, including Cloud and Virtualization Security, Data Security and Privacy, Hackers and Threats, Policy and Government, and Security Trends and Innovation.

.../2

Canada

CONSIDERATIONS

On the margins of the Conference, Ms. Clairmont will be leading a small delegation, including Mr. Gordon, to several "by invitation only" sessions that will explore potential solutions and actions to address the evolving cyber threat environment and the growing dependence of critical infrastructure sectors on cyber systems. These special sessions continue to offer a valuable opportunity to meet with senior level global leaders in the private and public sector, including the U.S. administration and representatives from technology companies (e.g. Microsoft and Google), to discuss strategic issues at the policy and technical levels.

Bilateral meetings will also be scheduled with senior officials from the U.S. Department of Homeland Security (DHS) [REDACTED]

[REDACTED] In this context, the RSA is an ideal forum for addressing sensitive policy issues and threats to cyberspace through public-private sector collaboration.

Stéphanie Durand from Communications will also be joining the delegation given the opportunities to advance the *Get Cyber Safe* public awareness campaign. Bilateral meetings will also be set up to share communications best practices across governments and industry, and build new partnerships on cyber security public awareness. The U.S. based *Stop.Think.Connect* campaign leaders will be in attendance and discussions will be taking place during the margins of the Conference.

Ms. Anderson and Ms. Binne will accompany Ms. Clairmont, Mr. Gordon, and Ms. Durand at the RSA Conference 2013 to provide technical assistance and advice on cyber security. Attending this Conference will also provide Ms. Binne and Ms. Anderson with an opportunity to exchange experiences with public-private sector partners in the areas of cyber incident response, handling, and other information technology best practices.

The estimated total cost for five PS participants is \$27,648.67. The conference registration fees will \$8,975.00 (U.S. dollars) and travel expenses have been estimated to be \$18,673.67. All costs related to this request fall within the Department's Travel, Hospitality and Conference cap for this fiscal year. The International Travel Request is included for your information (**TAB B**).

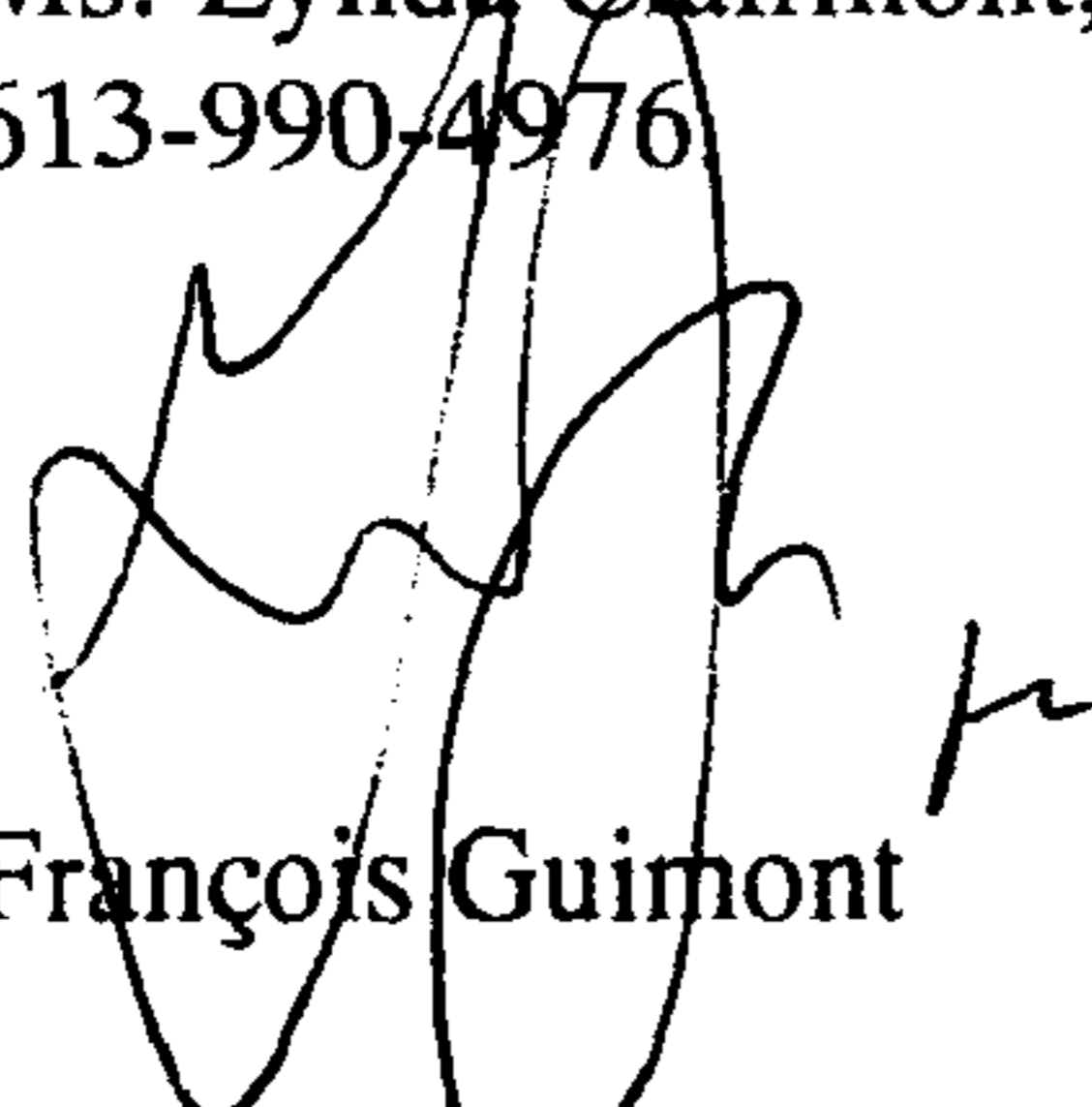
s.15(1) - Int'l

.../3

RECOMMENDATION

It is recommended that you approve this travel request. Should you agree, your signature is sought on the attached Travel Authority and Advance Forms (TAB C) and Training Application and Authority Forms (TAB D).

Should you require additional information, please do not hesitate to contact me or Ms. Lynda Clairmont, Senior Assistant Deputy Minister, National Security at 613-990-4976



François Guimont

Enclosures: (4)

I approve :

I do not approve:

Vic Toews, P.C., Q.C., M.P.

Vic Toews, P.C., Q.C., M.P.

Prepared by: Christine Binne

Please see attached approval



(/events/2013/usa/index.htm)

Agenda at-a-Glance

Below is a snapshot of the Conference schedule and different events taking place at RSA Conference 2013. Please check back often as we will be adding times and more detailed information soon.

| Monday, February 25, 2013 | | | |
|------------------------------|---|--|-----------------------------------|
| All Day | Morning | Afternoon | Evening |
| Security Basics Seminar | Information Security Leadership Development Seminar | Advancing Information Risk Practices Seminar | Orientation |
| Social Engineering Seminar | CSA Summit | Innovation Sandbox | Welcome Reception |
| SANS Tutorials | TCG Seminar | Professional Development Track | |
| Tuesday, February 26, 2013 | | | |
| All Day | Morning | Afternoon | Evening |
| Bookstore | Keynotes | Track Sessions | Expo Hall Pub Crawl |
| Expo | | Peer2Peer Sessions | Encore Sessions |
| | | | Dinner for 6 |
| Wednesday, February 27, 2013 | | | |
| All Day | Morning | Afternoon | Evening |
| Bookstore | Track Sessions | Track Sessions | Encore Sessions |
| Expo | Peer2Peer Sessions | Peer2Peer Sessions | Dinner for 6 |
| | | Keynotes | |
| Thursday, February 28, 2013 | | | |
| All Day | Morning | Afternoon | Evening |
| Bookstore | Track Sessions | Track Sessions | Encore Sessions |
| | Peer2Peer Sessions | Peer2Peer Sessions | Flash Talks Powered by PechaKucha |
| | Expo | Keynotes | RSA® Conference Codebreakers Bash |
| | | Expo | |
| Friday, March 1, 2013 | | | |
| All Day | Morning | Afternoon | Evening |
| | Track Sessions | Bookstore | |
| | Bookstore | Keynotes | |



International Travel Request Demande de voyage international

| | | |
|--|---|---------------------------|
| Event title - Titre de l'événement RSA Conference 2013 | Date of event - Date de l'événement | |
| | From - Du : February 25 - 2012 | To - Au : March 1 2012 |
| Location (City, Country) - Lieu (Ville, Pays) San Francisco, United States of America (U.S.) | Estimated total cost - Coût total prévu \$26,648.67 (all costs) | |
| Description of meeting (provide agenda) <i>Description de l'événement (joindre l'ordre du jour)</i> RSA Conference is one of the largest information security conferences in the world, consistently attracting the world's best and brightest in the field. The Conference plays an integral role in keeping security professionals across the globe connected and educated and creating opportunities for conference attendees to learn about information security's most important issues through first-hand interactions with peers, and industry leaders. The 2013 conference will cover more than two-hundred and seventy-five sessions across 22 tracks, including Cloud & Virtualization Security, Data Security & Privacy, Hackers & Threats, Policy & Government, and Security Trends & Innovation. | Pre-approved under Branch travel plans? <i>Pré-approuvé selon les directives sur les voyages de la direction générale?</i> <input checked="" type="checkbox"/> Yes/Oui <input type="checkbox"/> No/Non | |

Participant(s)

| Name (s) <i>Nom (s)</i> | Directorate/Branch <i>Direction générale/Secteur</i> | Work address <i>Adresse au travail</i> | Telephone No. <i>N° de telephone</i> |
|--|---|---|--|
| Lynda Clairmont Bob Gordon Windy Anderson Christine Binne | NCSD / National Security | 269 Laurier Avenue West 340 Laurier Avenue West, Ottawa, ON, K1A 0P8 | 990-4976 949-7380 991-7055 990-9379 |
| Stéphanie Durand | Communications | | 991-2799 |

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.)

Learning Event/

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 RSA conference sessions provide the latest thinking on topics related to cyber security which will inform our working priorities. The large participation by government and private sector representatives provides excellent opportunity for learning and networking with individuals who can be of assistance in furthering Departmental objectives.

Stéphanie Durand from Communications will also be joining my delegation given the learning opportunities to advance the Get Cyber Safe public awareness campaign. Bilateral meetings will also be set up to share communications best practices across governments and industry, and build new partnerships on cyber security public awareness. The US-based Stop.Think.Connect campaign leaders will be in attendance and discussions will be taking place during the margins of the Conference.

Other Department, Portfolio or Government representatives attending event
Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement


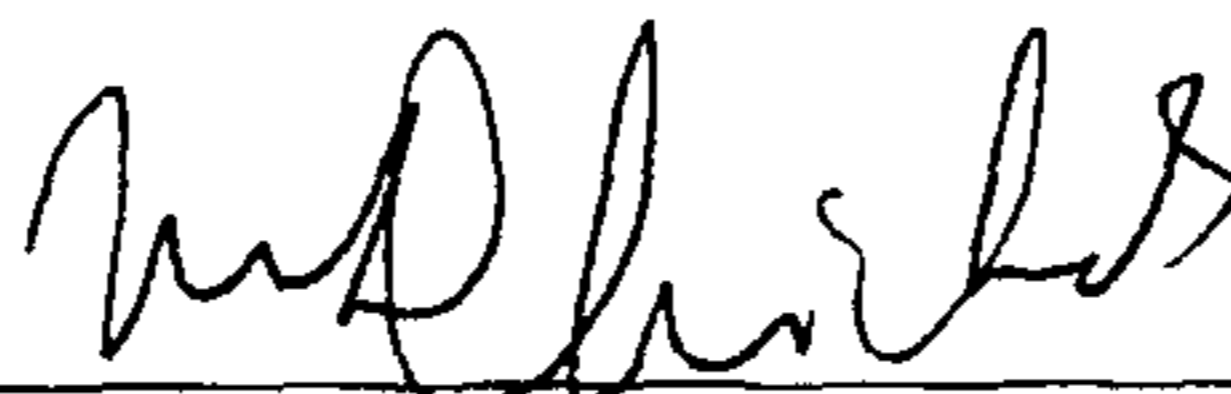

We are not aware of any other government employees or representatives that will be attending this event other than those who are listed above.

Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

There has not been outside consultations.

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 <i>Nom du Directeur Générale du voyageur</i> | <u>Dec 4/12</u> Date |
| Reviewed by/ Examiné par : |  Director General, International Affairs Directorate <i>Directeur Générale, Direction générale des affaires internationales</i> | <u>Dec 5/12</u> Date |
| Approved by/ Approuvé par : |  Name of participant's Assistant Deputy Minister <i>Nom du sous-ministre adjoint du voyageur</i> | <u>DEC 11 2012</u> Date |

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 original 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)
LNW9 80671

Document No. RDIMS - N° du document SGGDI

RDIMS 754283

Type 2 Name of traveller - Nom du voyageur
Windy Anderson

Classification
EX-01

Part A - Partie A

Department - Ministère
Public Safety Canada

Branch / Division / Group - Direction / Division / Groupe
NS-NCSD- Canadian Cyber Institute Response Centre

Address - Adresse
340 Laurier Ave W.

Telephone No. - No. de téléphone
613-990-9379

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 training- RSA Conference 2013

No. of days / Nbre de jours
 Yes / Oui No / Non

Do you have a Govt. Ind. Travel Card (ITC)? / Avez-vous une carte de voyage (CV)
 Yes / Oui No / Non

Part B - Travel Itinerary / Partie B - Itinéraire

| Date M/D-J | From - De | To - A | Time - Heure Departure - Arrivée | Transportation / Transport | | No. of meals prepaid / Nbre de repas prépayés | Accommodation / Hébergement | File locator number / N° de repérage du dossier |
|------------|---------------|---------------|-------------------------------------|----------------------------|---------|---|-----------------------------|---|
| | | | | Mode | Class | | | |
| 23-Feb-13 | Ottawa YOW | San Francisco | 09:00 - 14:36 | Air | Economy | 0 | Parc 55 | 326L2XJD |
| 23-Feb-12 | Personal Day | | | | | | | |
| 2-Mar-13 | San Francisco | Ottawa | 08:00 - 19:10 | Air | Economy | 0 | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel |
|---|---------------------------------|--|---------------------------------|--|
| Item / Type de dépenses | Estimated cost / Coût estimatif | Item / Type de dépenses | Estimated cost / Coût estimatif | |
| Accommodation (white page hotel) / Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$1,067.58 | Accommodation (green page hotel) / Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | <p>Part D - Partie D Estimated Cost - Coût estimatif Prépayé - Prépayé \$1,137.85 Other - Autre \$2,025.34 Trip Total - Coût total du voyage \$3,163.19 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 Ticket pick-up date and location / Date et lieu de la collecte des billets</p> |
| 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) | \$0.00 | |
| Private vehicle requested by: / Voiture particulière demandée par: <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$33.00 | Upgrade transportation (specify in "Class" above) / Transport à tarif supérieur (préciser la "classe" ci-dessus) | \$0.00 | |
| Public Liability and Property Damage min \$1 million. Deductibles NOT reimbursable / Responsabilité civile et dommages matériels (mbr. 1 000 000\$). Les franchises NO SONT PAS remboursables | | First class (Deputy Head or equivalent approval) / Prem. Classe (approuvée par le sou-chef ou l'équiv.) | | |
| Transportation / Transport | \$200.00 | Business class / Other Upgraded (other than article 1) / Classe d'affaires - ou autre classe à tarif supérieur (approuvée par le sou-chef ou l'équiv., s'il s'agit d'une autre classe) | | |
| Meals and incidentals / Repas et frais accessoires | \$819.78 | 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 autre classe) | | |
| Other (Specify) - Autre (préciser) | \$105.80 | | | |
| Baggage fees & Business phone | | Approval - Approbation | | |

Part E - Traveller / Partie E - Voyageur

I have accepted the Treasury Board Travel Policy (normal policy for separate employers) and accept the terms and conditions of travel that are in accordance with current policy.
 J'ai accepté la politique du Conseil du Trésor sur les voyages (Politique interne pour les employeurs distincts) et on accepte les conditions.

W. Anderson Signature Date **Dec 6/12**

Recommended by (signature) - Recommandé par (signature) **Leumont** Date **DEC 11 2012**

Part F - Request for Advance / Partie F - Demande d'avance

Type 3 Particulars (sub information) - Détails (sujets) 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 |
|--------|----------------------|-------------------|------------------|-----------------------------|--|----------------------------|
| | B O | | | | | |

Accounting Information / Renseignements comptables

| Sub-type / Sous-type | Voucher Code / Code du form. | Departmental Ref. No. / No. de réf. Du ministère | Coding - Classification | Amount - Montant |
|----------------------|------------------------------|--|----------------------------|------------------|
| | | T24 | 223-PSABASE-2001-500102384 | |

Description: Financial encumbrance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent n°1 chargé de la vér. Préalable des comptes (signature)
 Verified correct (PWGSC) (signature) / Vérifié conform (TRSGC) (signature)
 Services officer (PWGSC) (signature) / Agent responsable (TRSGC) (signature)

WORKSHEET - FEUILLE DE TRAVAIL

| Estimated Cost - Coût estimatif: Prepaid - Prépayé | | | Amount/Montant |
|--|----------------------------|------------|-----------------|
| Airfare / Frais d'avion | | | \$1,137.85 |
| Train / Train | | | \$0.00 |
| Other / Autres | | | \$0.00 |
| | | | \$1,137.85 |
| Estimated Cost - Coût estimatif: Other - Autre | | | Amount/Montant |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du r | Rate / Tarif | No. / Nbre | Amount/Montant |
| | \$177.93 | 6 | \$1,067.58 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du réper | | | \$0.00 |
| | | | \$1,067.58 |
| 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 | 60.0 | \$33.00 |
| | | | \$0.00 |
| | Rate / Tarif | No. / Nbre | Amount/Montant |
| Parking & Tolls / stationnement et frais de péage | | \$0.00 | \$0.00 |
| Taxi/Limo | Home to Airport | \$0.00 | \$200.00 |
| | Airport - Hotel / Meetings | \$50.00 | |
| | Hotel - Airport | \$50.00 | |
| | Airport to Home | \$0.00 | |
| | Meeting - Meetings | \$100.00 | |
| Transportation / Transportation (No receipt) | \$10.00 | | \$0.00 |
| Ferry & Miscellaneous | | \$0.00 | \$0.00 |
| | | | \$200.00 |
| Canadian | | | Amount/Montant |
| Breakfast / Petits déjeuners | \$15.50 | 1 | \$15.50 |
| Lunch / Déjeuners | \$15.00 | 1 | \$15.00 |
| Dinner / Dîners | \$41.30 | | \$0.00 |
| Incidentals /Frais divers | \$17.30 | 1 | \$17.30 |
| Total Canadian | | | \$47.80 |
| Country # 1 | | | Amount/Montant |
| Breakfast / Petits déjeuners | \$15.39 | 6 | \$92.34 |
| Lunch / Déjeuners | \$14.90 | 6 | \$89.40 |
| Dinner / Dîners | \$41.02 | 7 | \$287.14 |
| Incidentals /Frais divers | \$17.18 | 6 | \$103.08 |
| Total Country # 1 | | | \$571.96 |
| Country #2 | | | 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 | | | \$619.76 |
| Business Phone / Téléphone d'affaires | | | \$50.00 |
| Airport Improvement Fee / Frais de l'Aéroport | | | \$0.00 |
| Cash Advance Fee / Frais d'avances | | | \$0.00 |
| Misc. Business Services / Diverses charges d'affaires | | | \$0.00 |
| Miscellaneous / Diverses - Conference Fees | | | \$55.00 |
| | | | \$105.00 |

Original / Prem. demande
 Amended (Same levels of approval as original dated)

| | | |
|--------|---|--|
| 14A | Travel Authority No. (TAN) N°. d'aut de voyager (NAV) LNW9 | Document No. RDIMS - N° du document SGGDI 734368 |
| Type 2 | Name of traveller - Nom du voyageur Christine Binne | Classification EC-07 |

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)
Part A - Partie A

| | | |
|--|--|--|
| Department - Ministère Public Safety Canada | Branch / Division / Group - Direction / Division / Groupe NS-NCSD-Policy and Issues Division | |
| Address - Adresse 340 Laurier Ave W. | Telephone No. - No. de téléphone 613-990-9379 | 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 training- RSA Conference 2013 (Training) | No. of days Nbre de jours | Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage (CV)? <input checked="" type="checkbox"/> Yes / Oui <input type="checkbox"/> No / Non |
| | | If no, would you like to request one? Les cas échéant, aimeriez-vous en avoir une? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> No / Non |

Part B - Travel Itinerary / Partie B - Itinéraire

| Date M / D - J | From - De | To - A | Time - Heure Departure - Arrivée Départ - Arrivée | Transportation Transport | | No. of meals prepaid Nbre de repas prépayés | Accommodation Hébergement | File locator number N°. de repérage du dossier |
|-------------------|---------------|---------------|---|-----------------------------|---------|--|------------------------------|--|
| | | | | Mode | Class | | | |
| 23-Feb-13 | Ottawa YOW | San Francisco | 09:00- 14:36 | Air | Economy | 0 | Parc 55 | 326L2XJF |
| 24-Feb-13 | Personal Day | | | | | | | |
| 2-Mar-13 | San Francisco | Ottawa | 08:00 - 19:10 | Air | Economy | 0 | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | |
|--|----------------------------------|---|----------------------------------|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$1,067.58 | Accommodation (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) | \$0.00 |
| Private vehicle requested by: Voiture particulière demandée par: <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$22.55 | Other (Specify) - Autre (préciser) Business Class | \$0.00 |
| 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 | | Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | \$0.00 |
| Transportation Transport | \$245.00 | <input type="checkbox"/> First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) Business class / Other-Upgraded (other than article) | |
| Meals and incidentals Repas et frais accessoires | \$619.78 | <input type="checkbox"/> 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 | |
| Other (Specify) - Autre (préciser) | \$55.00 | | |
| Baggage Fee Service | | 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
\$1,137.85
Other - Autre
\$2,009.91
Trip Total - Coût total du voyage
\$3,147.76

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]
Signature

Dec 5/12
Date

| | | | |
|---|----------------------------|--|------|
| Recommended by (signature) - Recommandé par (signature) <i>[Signature]</i> | Date DEC 11 2012 | 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 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 |
|--------|--------------------------------|-------------------|------------------|-----------------------------|---|-----------------------------|

Accounting Information / Renseignement comptables

| | | | | |
|-----------------------|-------------------------------|--|---|------------------|
| Sub-type Sous-type | Vendor Code Code du fourn. | Departmental Ref. No. No. de réf. Du ministère T24 | Coding - Cidification 496-PSABASE-2001-500102386 | Amount - Montant |
|-----------------------|-------------------------------|--|---|------------------|

| | |
|---|---|
| Description | Financial encumbrance No. No. de consignation de fonds |
| Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature) | Cheque No. - N° du chèque |
| Verified correct (PWGSC) (signature) Vérifié conform (TPSGC) (signature) | Date |
| Services officer (PWGSC) (signature) Agent responsable (TPSGC) (signature) | Signature |

WORKSHEET - FEUILLE DE TRAVAIL

| Estimated Cost - Coût estimatif: Prepaid - Prépayé | | | | Amount/Montant |
|--|----------------------------|--------------|------------|-----------------|
| Airfare / Frais d'avion | | | | \$1,137.85 |
| Train / Train | | | | \$0.00 |
| Other / Autres | | | | \$0.00 |
| | | | | \$1,137.85 |
| Estimated Cost - Coût estimatif: Other - Autre | | | | Amount/Montant |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du r | | \$177.93 | 6 | \$1,067.58 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du repe | | | | \$0.00 |
| | | | | \$1,067.58 |
| 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 | 41.0 | \$22.55 |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Parking & Tolls / stationnement et frais de péage | | | \$0.00 | \$0.00 |
| Taxi/Limo | Home to Airport | | \$45.00 | \$245.00 |
| | Airport - hotel / Meetings | | \$50.00 | |
| | Hotel - Airport | | \$50.00 | |
| | Airport to Home | | \$0.00 | |
| | Meeting - Meetings | | \$100.00 | |
| Transportation / Transportation (No receipt) | | \$10.00 | | \$0.00 |
| Ferry & Miscellaneous | | | \$0.00 | \$0.00 |
| | | | | \$245.00 |
| Canadian | | | | Amount/Montant |
| Breakfast / Petits déjeuners | | \$15.50 | 1 | \$15.50 |
| Lunch / Déjeuners | | \$15.00 | 1 | \$15.00 |
| Dinner / Diners | | \$41.30 | | \$0.00 |
| Incidentals /Frais divers | | \$17.30 | 1 | \$17.30 |
| Total Canadian | | | | \$47.80 |
| U.S.A. | | | | Amount/Montant |
| Breakfast / Petits dejeuner | | \$15.39 | 6 | \$92.34 |
| Lunch / Déjeuners | | \$14.90 | 6 | \$89.40 |
| Dinner / Diners | | \$41.02 | 7 | \$287.14 |
| Incidentals /Frais divers | | \$17.18 | 6 | \$103.10 |
| Total U.S.A. | | | | \$571.98 |
| Country #2 | | | | Amount/Montant |
| Breakfast / Petits dejeuner | | \$0.00 | | \$0.00 |
| Lunch / Dejeuners | | \$0.00 | | \$0.00 |
| Dinner / Diners | | \$0.00 | | \$0.00 |
| Incidentals /Frais divers | | \$0.00 | | \$0.00 |
| Total Country #2 | | | | \$0.00 |
| GRAND TOTAL | | | | \$619.78 |
| Business Phone / Téléphone d'affaires | | | | \$0.00 |
| Airport Improvement Fee / Frais de l'Aéroport | | | | \$0.00 |
| Cash Advance Fee / Frais d'avances | | | | \$0.00 |
| Misc. Business Services / Diverses charges d'affaires | | | | \$0.00 |
| Miscellaneous / Diverses - Conference Fees | | | | \$55.00 |
| | | | | \$55.00 |

Original / Prem. demande

Amended (Same levels of approval as original dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

| | | | |
|--|--|--|--|
| Department - Ministère Public Safety Canada | 14A | Travel Authority No. (TAN) N° d'aut de voyager (NAV) LNW9 | 734182 |
| Address - Adresse 340 Laurier Ave W. | Type 2 | Name of traveller - Nom du voyageur Robert Gordon | Classification EX-05 |
| Branch Contact - Personne ressource à la direction Jane Hayward | Branch / Division / Group - Direction / Division / Groupe NS-NCSD-Advisor to the Senor ADM | | |
| Purpose of travel - Objet du voyage To attend training- RSA Conference 2013 (Training) | Telephone No. - No. de téléphone 613-949-7380 | Telephone No. - No. de téléphone 613-991-1982 | If different address, send cheque to: Si adresse différente, envoyer cheque a |
| No. of days Nbre de jours 7 | Do you have a Govt Ind Travel Card (ITC)? Avez-vous une carte de voyage (CV) <input checked="" type="checkbox"/> Yes / Oui <input type="checkbox"/> No / Non | If no, would you like to request one? Les cas échéant, aimeriez-vous en avoir une? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> 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 | | No. of meals prepaid Nbre de repas prépayés | Accommodation Hébergement | File locator number N° de repérage du dossier |
|-------------------|---------------|---------------|---|-----------------------------|---------|--|------------------------------|---|
| | | | | Mode | Class | | | |
| 23-Feb-13 | Ottawa YOW | San Francisco | 09:00- 14:36 | Air | Economy | 0 | Grand Hyatt | 326L2XHZ |
| 24-Feb-12 | Personal Day | | | | | | | |
| 2-Mar-13 | San Francisco | Ottawa | 08:00 -19:10 | Air | Economy | 0 | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel |
|--|----------------------------------|---|----------------------------------|--|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif | |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$1,067.58 | Accommodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | <p>Part D - Partie D</p> <p>Estimated Cost - Coût estimatif</p> <p>Prepaid - Prépayé</p> <p>\$1,137.85</p> <p>Other - Autre</p> <p>\$2,064.94</p> <p>Trip Total - Coût total du voyage</p> <p>\$3,202.79</p> <p>Funding - Financement</p> <p>A) Travellers cheques / Chèques de voyage</p> <p>Cdn / Can \$0.00</p> <p>US / É.U. \$0.00</p> <p>Other / Autre \$0.00</p> <p>B) Other advance / Autre avance</p> <p>Cheque / Chèque \$0.00</p> <p>Cash / Comptant \$0.00</p> <p>Total funding requested (A + B)</p> <p>Financement total demandé (A + B)</p> <p>\$0.00</p> <p>Ticket pick-up date and location</p> <p>Date et lieu de la collecte des billets</p> |
| 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) | \$0.00 | |
| Private vehicle requested by: Voiture particulière demandée par: | \$72.60 | Other (Specify) - Autre (préciser) | \$0.00 | |
| <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | | Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | \$0.00 | |
| Transportation Transport | \$200.00 | <input type="checkbox"/> First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) Business class / Other-Upgraded (other than article 9) | | |
| Meals and incidentals Repas et frais accessoires | \$619.76 | <input type="checkbox"/> 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 | | |
| Other (Specify) - Autre (préciser) | \$105.00 | | | |
| Baggage Fees & Business Phone | | Approval - Approbation | | |

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]* **2012/2/05**

Signature Date

| | | | |
|---|------|--|------|
| 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 cheque | 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 |
|--------|--------------------------------|-------------------|------------------|-----------------------------|---|-----------------------------|

Accounting Information / Renseignement comptables

| | | | | |
|---|-------------------------------|--|---|---|
| Sub-type Sous-type | Vendor Code Code du fourn. | Departmental Ref. No. No. de réf. Du ministère T24 | Coding - Cidification 475-PSABASE-2001-500102367 | Amount - Montant |
| Description | | | | Financial encumbrance No. No. de consignation de fonds |
| Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature) | | | | Cheque No. - N° du cheque |
| Verified correct (PWGSC) (signature) Vérifié conform (TPSGC) (signature) | | | | Date |
| Services officer (PWGSC) (signature) Agent responsable (TPSGC) (signature) | | | | Signature |

WORKSHEET - FEUILLE DE TRAVAIL

| Estimated Cost - Coût estimatif: Prepaid - Prépayé | | | | Amount/Montant |
|--|----------------------------|--------------|------------|-----------------|
| Airfare / Frais d'avion | | | | \$1,137.85 |
| Train / Train | | | | \$0.00 |
| Other / Autres | | | | \$0.00 |
| | | | | \$1,137.85 |
| Estimated Cost - Coût estimatif: Other - Autre | | | | Amount/Montant |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du r | | Rate / Tarif | No. / Nbre | Amount/Montant |
| | | \$177.93 | 6 | \$1,067.58 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du repe | | | | \$0.00 |
| | | | | \$1,067.58 |
| 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 |
| Private vehicle / Voiture particulière: Mileage (km) Employer Rate / Taux parcours (km) pour employé | | Rate / Tarif | No. / Nbre | Amount/Montant |
| | | 0.550 | 132.0 | \$72.60 |
| | | | | \$0.00 |
| Parking & Tolls / stationnement et frais de péage | | Rate / Tarif | No. / Nbre | Amount/Montant |
| | | | \$0.00 | \$0.00 |
| Taxi/Limo | Home to Airport | | \$0.00 | \$200.00 |
| | Airport - Hotel / Meetings | | \$50.00 | |
| | Hotel - Airport | | \$50.00 | |
| | Airport to home | | \$0.00 | |
| | Meeting - Meetings | | \$100.00 | |
| Transportation / Transportation (No receipt) | | \$10.00 | | \$0.00 |
| Ferry & Miscellaneous | | | \$0.00 | \$0.00 |
| | | | | \$200.00 |
| Canadian | | | | Amount/Montant |
| Breakfast / Petits déjeuners | | Rate / Tarif | No. / Nbre | Amount/Montant |
| | | \$15.50 | 1 | \$15.50 |
| Lunch / Déjeuners | | \$15.00 | 1 | \$15.00 |
| Dinner / Diners | | \$41.30 | | \$0.00 |
| Incidentals /Frais divers | | \$17.30 | 1 | \$17.30 |
| Total Canadian | | | | \$47.80 |
| U.S.A. | | | | Amount/Montant |
| Breakfast / Petits déjeuners | | Rate / Tarif | No. / Nbre | Amount/Montant |
| | | \$15.39 | 6 | \$92.34 |
| Lunch / Déjeuners | | \$14.90 | 6 | \$89.40 |
| Dinner / Diners | | \$41.02 | 7 | \$287.14 |
| Incidentals /Frais divers | | \$17.18 | 6 | \$103.08 |
| Total U.S.A. | | | | \$571.96 |
| Country #2 | | | | Amount/Montant |
| Breakfast / Petits déjeuners | | Rate / Tarif | No. / Nbre | Amount/Montant |
| | | \$0.00 | | \$0.00 |
| Lunch / Dejeuners | | \$0.00 | | \$0.00 |
| Dinner / Diners | | \$0.00 | | \$0.00 |
| Incidentals /Frais divers | | \$0.00 | | \$0.00 |
| Total Country #2 | | | | \$0.00 |
| GRAND TOTAL | | | | \$619.76 |
| Business Phone / Téléphone d'affaires | | | | \$50.00 |
| Airport Improvement Fee / Frais de l'Aéroport | | | | \$0.00 |
| Cash Advance Fee / Frais d'avances | | | | \$0.00 |
| Misc. Business Services / Diverses charges d'affaires | | | | \$0.00 |
| Miscellaneous / Diverses - Conference Fees | | | | \$55.00 |
| | | | | \$105.00 |

**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 Anderson | | Given name and initials – Prénom et initiales Windy G | | | |
| 4. PRI – CIDP [REDACTED] | 5. Sex – Sexe <input type="checkbox"/> Male / Homme <input checked="" type="checkbox"/> Female / Femme | 6. Classification Gr. S.-gr. Lev. Niv. EX 01 | | 7. First official language – Première langue officielle <input checked="" type="checkbox"/> (1) English / Anglais <input type="checkbox"/> (2) French / Français | |
| 8. Position title – Titre du poste Director, Canadian Cyber Incident Response Centre | | | | | |
| 9. Employee's office telephone number – N° de téléphone de l'employé au bureau 613-991-7055 | | | Facsimile – Télécopieur | | E-Mail – Courrier électronique windy.anderson@ps-sp.gc.ca |
| 10. Department name – Nom du ministère Public Safety Canada | | 11. Dept. Code – Code min. 0880 | | 12. Branch/Division – Direction/Division National Security | |
| 13. Office, Workstation, mailing address – Adresse postale, bureau, poste de travail 257 Slater Street, Ottawa, Ontario, 4th Floor Room 453 | | | | City/Postal code – Ville/Code postal K1A 0P8 | |
| 14. Supervisor's name and title – Nom du surveillant et titre Robert Dick | | | | Telephone No. – N° de téléphone 613-990-2661 | |
| 15. Supervisor's Office, Workstation, mailing address – Adresse postale, bureau, poste de travail du superviseur 340 Laurier Avenue West, Ottawa, Ontario, 11th Floor | | | | City/Postal code – Ville/Code postal K1A 0P8 | |
| 16. Objective of training * - Objective de la formation * The RSA conference sessions provide the latest thinking on topics related to cyber security which will inform our working priorities. The large participation by government and private sector representatives provides an excellent opportunity for learning and networking with individuals who can be of assistance in furthering Departmental objectives. | | | | | |
| Expenditure Initiation Approval - L'engagement des dépenses | | Date | Print Name- Imprimer Nom | Signature - (Authorized Signing Officer) / (Un dirigeant autorisé) | |
| Employee Name and Signature - Nom de l'employé et signature | | Date | Print Name- Imprimer Nom | Employee's - Signature - Employé(e) | |
| | | | DEC 4/12 WINDY ANDERSON | <i>W. Anderson</i> | |

TRAINING INFORMATION – RENSEIGNEMENTS SUR LA FORMATION

| | | | | | | | | |
|---|--|--|---|--|--------------|--|-------------------------|-----|
| 17. Course code * - Code du cours * | | 18. Course title – Titre du cours RSA Conference 2013 | | | | | | |
| 19. Location of training * - Lieu de formation * San Francisco, CA, USA | | | 20. Date of course - Date du cours | | | 21. Departmental training program code * Code min. du programme de formation * 009 | | |
| | | | From – Du | | To – Au | | | |
| | | | Y-A | M | D-J | Y-A | M | D-J |
| | | | 13 | 02 | 23 | 13 | 03 | 03 |
| 22. Time of training - Période retenue pour la formation <input type="checkbox"/> (1) Outside working hours / En dehors des heures de travail <input checked="" type="checkbox"/> (2) During working hours / Pendant les heures de travail | | 23. Duration of training * (nearest half-day) / Durée de la formation * (plus proche demi-journée) 5 | | 24. Language of course - Langue de cours <input checked="" type="checkbox"/> English / Anglais <input type="checkbox"/> French / Français <input type="checkbox"/> Bilingual / Bilingue <input type="checkbox"/> Other / Autre | | | | |
| 25. Source of training - Source de la formation <input type="checkbox"/> (1) TPB/PSC / DGPF/CFP <input type="checkbox"/> (2) Dept'l / Min. <input type="checkbox"/> (3) Interdept'l / Intermin. <input type="checkbox"/> (4) University/College / Université/Collège <input checked="" type="checkbox"/> (5) Other / Autre | | | 26. Transit time (person-days) * / Durée des déplacements (jours-personnes) 2 | | 27. Province | | 28. Location * / Lieu * | |

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 * <input type="checkbox"/> 0% <input type="checkbox"/> 50% <input checked="" type="checkbox"/> 100% | 500102384 Line 3 | \$1795.00 | a) * |
| Travel / Living / Déplacement / Subsistance | 500102384 Line 1+2 | \$3341.14 | b) |
| Other * / Autres * | | | c) * |
| 30. Responsibility centre (collator) code / Code du centre de responsabilité (destinataire) 223 | | TOTAL | \$5136.14 |
| Recipient organization code / Code d'organisation du/de la récipiendaire 088 | | 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) * | | 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 |



**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 Binne | | Given name and initials - Prénom et initiales Christine | |
| 4. PRI - CIDP [REDACTED] | 5. Sex - Sexe <input type="checkbox"/> Male / Homme <input checked="" type="checkbox"/> Female / Femme | 6. Classification Gr. S-gr. Lev. Niv. EC 07 | 7. First official language - Première langue officielle <input checked="" type="checkbox"/> (1) English / Anglais <input type="checkbox"/> (2) French / Français |
| 8. Position title - Titre du poste Senior Strategist | | | |
| 9. Employee's office telephone number - N° de téléphone de l'employé au bureau 613-990-9379 | | Facsimile - Télécopieur 613-990-3287 | E-Mail - Courrier électronique Christine.Binne@ps-sp.gc.ca |
| 10. Department name - Nom du ministère Public Safety Canada | | 11. Dept. Code - Code min. 0880 | 12. Branch/Division - Direction/Division National Security |
| 13. Office, Workstation, mailing address - Adresse postale, bureau, poste de travail 340 Laurier Avenue West, Ottawa, ON, Room 11D102 | | | City/Postal code - Ville/Code postal K1A 0P8 |
| 14. Supervisor's name and title - Nom du surveillant et titre Mark Matz, Director, Policy and Issues Management | | | Telephone No. - N° de téléphone (613) 993-9635 |
| 15. Supervisor's Office, Workstation, mailing address - Adresse postale, bureau, poste de travail du superviseur 340 Laurier Avenue West, Ottawa, ON, Room 11C093, | | | City/Postal code - Ville/Code postal K1A 0P8 |
| 16. Objective of training - Objectif de la formation * The RSA conference sessions provide the latest thinking on topics related to cyber security which will inform our working priorities. The large participation by government and private sector representatives provides an excellent opportunity for learning and networking with individuals who can be of assistance in furthering Departmental objectives. | | | |
| Expenditure Initiation Approval - L'engagement des dépenses | | Date | Print Name - Imprimer Nom |
| Employee Name and Signature - Nom de l'employé et signature Christine Binne | | Date DEC 4/12 | Print Name - Imprimer Nom |
| | | Signature - (Authorized Signing Officer) / (Un dirigeant autorisé) | |
| | | Employee's - Signature - Employé(e) <i>[Signature]</i> | |

TRAINING INFORMATION - RENSEIGNEMENTS SUR LA FORMATION

| | | | | | |
|---|---|--|---|--|--|
| 17. Course code * Code du cours * | 18. Course title - Titre du cours RSA Conference 2013 | | | | |
| 19. Location of training * - Lieu de formation * San Francisco, CA, USA | | | 20. Date of course - Date du cours | | 21. Departmental training program code * Code min. du programme de formation * 009 |
| | | | From - Du | | To - Au |
| | | | Y-A | M | D-J |
| | | | 13 | 02 | 23 |
| | | | Y-A | M | D-J |
| | | | 13 | 03 | 03 |
| 22. Time of training - Période retenue pour la formation <input type="checkbox"/> (1) Outside working hours / En dehors des heures de travail <input checked="" type="checkbox"/> (2) During working hours / Pendant les heures de travail | | 23. Duration of training * (nearest half-day) / Durée de la formation * (plus proche demi-journée) 5 | | 24. Language of course - Langue de cours <input checked="" type="checkbox"/> English / Anglais <input type="checkbox"/> French / Français <input type="checkbox"/> Bilingual / Bilingue <input type="checkbox"/> Other / Autre | |
| 25. Source of training - Source de la formation <input type="checkbox"/> (1) TPB/PSC / DGPF/CFP <input type="checkbox"/> (2) Dept / Min. <input type="checkbox"/> (3) Interdept / Intermin. <input type="checkbox"/> (4) University/College / Université/Collège <input checked="" type="checkbox"/> (5) Other / Autre | | | 26. Transit time (person-days) * / Durée des déplacements (jours-personnes) 2 | | 27. Province |
| | | | | | 28. Location * / Lieu * |

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 * <input type="checkbox"/> 0% <input type="checkbox"/> 50% <input checked="" type="checkbox"/> 100% | 500102386 line 3 | \$ 1,795.00 | a) * |
| Travel / Living / Déplacement / Subsistance | 500102386 line 1 and 2 | \$ 3314.67 | b) * |
| Other * / Autres * | | | c) * |
| 30. Responsibility centre (collator) code / Code du centre de responsabilité (destinataire) 496 | TOTAL | \$ 5109.67 | d) * |
| Recipient organization code / Code d'organisation du/de la récipiendaire 098 | | Récipient reference 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) * | | 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 _____ |



**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 Gordon | | | Given name and initials – Prénom et initiales Robert | | |
| 4. PRI – CIDP [REDACTED] | 5. Sex – Sexe <input checked="" type="checkbox"/> Male / Homme <input type="checkbox"/> Female / Femme | 6. Classification Gr. S.-gr. Lev. Niv. EX 05 | | 7. First official language – Première langue officielle <input checked="" type="checkbox"/> (1) English / Anglais <input type="checkbox"/> (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 613-949-7380 | | | Facsimile – Télécopieur 613-990-3287 | | E-Mail – Courrier électronique Robert.Gordon@ps-sp.gc.ca |
| 10. Department name – Nom du ministère Public Safety Canada | | 11. Dept. Code – Code min. 0880 | | 12. Branch/Division – Direction/Division National Security | |
| 13. Office, Workstation, mailing address – Adresse postale, bureau, poste de travail 340 Laurier Avenue West, Ottawa, ON, Room 11D111 | | | | City/Postal code – Ville/Code postal K1A 0P8 | |
| 14. Supervisor's name and title – Nom du surveillant et titre Robert Dick, Director General, National Cyber Security Directorate | | | | Telephone No. – N° de téléphone (613) 990-2661 | |
| 15. Supervisor's Office, Workstation, mailing address – Adresse postale, bureau, poste de travail du superviseur 340 Laurier Avenue West, Ottawa, ON, Room 11D127 | | | | City/Postal code – Ville/Code postal K1A 0P8 | |
| 16. Objective of training * - Objectif de la formation * The RSA conference sessions provide the latest thinking on topics related to cyber security which will inform our working priorities. The large participation by government and private sector representatives provides excellent opportunity for learning and networking with individuals who can be of assistance in furthering Departmental objectives. | | | | | |
| Expenditure Initiation Approval - L'engagement des dépenses | | Date | Print Name - Imprimer Nom | Signature - (Authorized Signing Officer) / (Un dirigeant autorisé) | |
| Employee Name and Signature - Nom de l'employé et signature | | Date 04/12/2012 | Print Name - Imprimer Nom Robert Gordon | Employee's Signature - Employé(e) <i>Robert Gordon</i> | |

TRAINING INFORMATION – RENSEIGNEMENTS SUR LA FORMATION

| | | | | | | | | |
|---|--|---|------------------------------------|--|-----|---|--------------------------|-----|
| 17. Course code * Code du cours * | | 18. Course title – Titre du cours RSA Conference 2013 | | | | | | |
| 19. Location of training * - Lieu de formation * San Francisco, CA, USA | | | 20. Date of course - Date du cours | | | 21. Departmental training program code * Code min. du programme de formation * 009 | | |
| | | | From - Du | | | To - Au | | |
| | | | Y-A | M | D-J | Y-A | M | D-J |
| | | | 13 | 02 | 23 | 13 | 03 | 03 |
| 22. Time of training - Période retenue pour la formation <input type="checkbox"/> (1) Outside working hours En dehors des heures de travail <input checked="" type="checkbox"/> (2) During working hours Pendant les heures de travail | | 23. Duration of training * (nearest half-day) Durée de la formation * (plus proche demi-journée) 5 | | 24. Language of course - Langue de cours <input checked="" type="checkbox"/> English / Anglais <input type="checkbox"/> French / Français <input type="checkbox"/> Bilingual / Bilingue <input type="checkbox"/> Other / Autre | | | | |
| 25. Source of training - Source de la formation <input type="checkbox"/> (1) TPB/PSC / DGPF/CFP <input type="checkbox"/> (2) Dept'l / Min. <input type="checkbox"/> (3) Interdept'l / Intermin. <input type="checkbox"/> (4) University/College / Université/Collège <input checked="" type="checkbox"/> (5) Other / Autre | | | | 26. Transit time (person-days) * Durée des déplacements (journées-personnes) 2 | | 27. Province | 28. Location * Lieu * | |

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 * <input type="checkbox"/> 0% <input type="checkbox"/> 50% <input type="checkbox"/> 100% | 500102367 Line 3 | 1795.00 | a) * |
| Travel / Living Déplacement / Subsistance | 500102367 Line 1 and 2 | 3380.72 | b) |
| Other * Autres * | | | c) * |
| 30. Responsibility centre (collator) code Code du centre de responsabilité (destinataire) 475 | | TOTAL \$5175.72 | |
| Recipient organization code Code d'organisation du/de la récipiendaire 088 | | 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) * | | 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 |



Public Safety / Sécurité publique
Canada / Canada

Deputy Minister / Sous-ministre

Ottawa, Canada
K1A 0P8

*To MO
Jan 4, 2013*

UNCLASSIFIED

DATE:

File No. 391482
RDIMS No.: 738229

MEMORANDUM FOR THE MINISTER

ADVANCED AUTHORIZATION TO EXTEND HOSPITALITY:

[Redacted]

(Decision sought)

ISSUE

Your approval is sought to authorize the proposed hospitality to host a senior level delegation of cyber security officials [Redacted]

[Redacted]

BACKGROUND

[Redacted]

The meeting will take place over a two day period and will provide an opportunity for the Government of Canada to engage with [Redacted] counterparts on several cyber related issues of mutual interest.

CURRENT STATUS

The enclosed hospitality request seeks approval to provide food and refreshments for approximately 45 senior officials and their associates. [Redacted]

[Redacted]

[Redacted] We are currently waiting the list of participants for the January 2013 meeting.

.../2

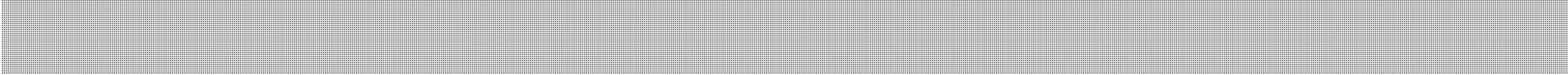
Hospitality

As indicated in the proposed agenda (**TAB A**), the meetings will be held at DFAIT headquarters over a two-day period. Working lunches are planned to maximize the time available and heavy agenda. The estimated cost for the working lunches and breaks over the two-day period would be \$3,348.48.



The total cost of extending hospitality, including catering and the host dinner, is \$ 6,977.52.

Translation and Interpretation Services

 We were advised by Public Works and Government Services Canada (PWGSC), that seven interpreters would be required to provide simultaneous interpretation services during the course of the event and that this service would be provided at no charge to PS.

The Department would be responsible for all travel, accommodation and associated expenses for the interpreters. Six of the interpreters are available locally, but an additional interpreter will travel from Toronto at an estimated cost of \$1,777.33.

PWGSC will pay for the interpreters' professional fees of \$13,020.00. However, if the event is cancelled after the contract for services has been signed, PS would be responsible and charged a cancellation fee of \$7,486.50.

Translation services will be provided by the Canadian Security Intelligence Service.

.../3

Audio Visual

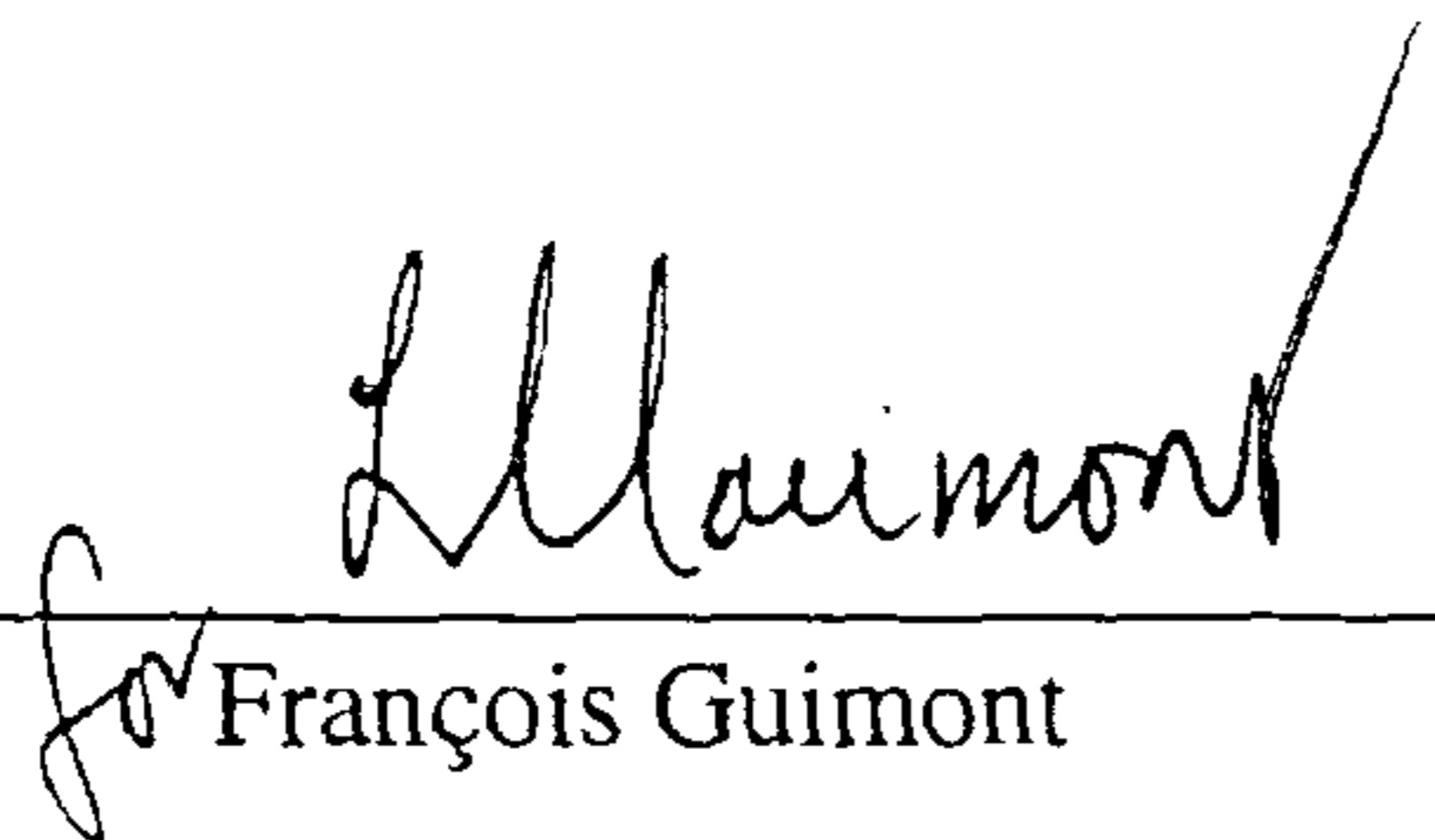
No cost will be incurred for the technical equipment required by the interpreters as the room is already equipped for simultaneous interpretation of up to nine languages.

RECOMMENDATION

It is recommended that you approve the *Advanced Authorization to Extend Hospitality* for [REDACTED] which is estimated to be \$6,977.42, by signing the enclosed form (**TAB B**).

The total estimated cost [REDACTED] is \$8,754.85.

Should you require additional information, please do not hesitate to contact me or Ms. Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.


for François Guimont

Enclosures: (3)

I approve:

I do not approve:

Vic Toews, P.C., Q.C., M.P.

Vic Toews, P.C., Q.C., M.P.

Prepared by: Ian Anderson and Melanie Mohammed

Pages 91 to / à 95
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



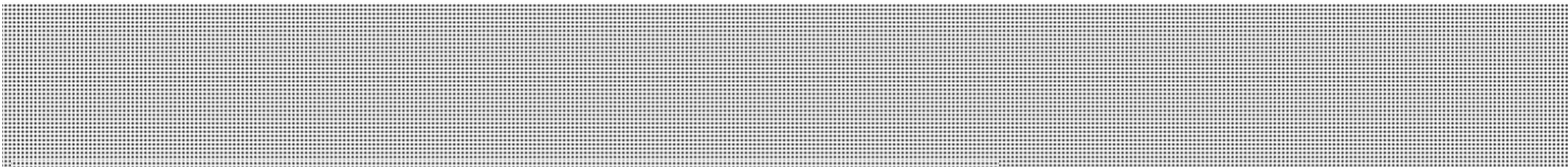
ADVANCED AUTHORIZATION TO EXTEND HOSPITALITY DEMANDE D'AUTORISATION POUR OFFRIR UNE RÉCEPTION OFFICIELLE

NOTE: To be used by employees to whom authority has not been delegated but who may be required to extend hospitality in **exceptional circumstances**.

REMARQUE: Doit être remplie par les employés à qui l'autorisation n'a pas été déléguée, mais qui peuvent être appelés à offrir des réceptions officielles dans **des circonstances exceptionnelles**.

| Employee's Name - <i>Nom de l'employé</i> | | Branch - <i>Direction</i> | | |
|---|--|--|-------|---|
| Robert Dick | | NCSD, National Security Branch | | |
| Type of Function - <i>Nature de l'événement</i> | | Place of Function - <i>Lieu de l'événement</i> | | |
| Health Breaks (3) Breakfast, Lunch (3) and Dinner | | 125 Sussex Drive, Ottawa, ON | | |
| Function Date <i>Date de l'événement</i> | Number In Attendance - <i>Nombre de participants</i> | | | Total Estimated Cost <i>Coût total prévu</i> |
| | Gov't of Canada - <i>Gouv. du Canada</i> | Other - <i>Autres</i> | Total | |
| January 29-30, 2013 | 15 | 30 | 45 | \$ 6,977.52 |

Purpose of Hospitality - *Objet de la dépense*




The meeting will take place over a two-day period and will provide an opportunity for the Government of Canada to engage with counterparts on several cyber related issues of mutual interest.

This hospitality request includes two breakfasts, three health breaks, two lunches, and a working lunch with Senior Officials. A dinner/reception on the evening of January 29, 2013 is also planned at which time alcohol will be served. The Working Lunch with Senior Officials (wine will be available) exceeds the TBS Standard Costs but does not exceed the Maximum Costs.

The list of participants has not yet been finalized, however, based on the planning for the previous meeting, we expect that [redacted] would consist of 22 attendees.

I hereby request authorization to extend hospitality as stated above, in accordance with Treasury Board Policy and Guidelines on Hospitality.

Je demande par la présente l'autorisation d'offrir la réception officielle susmentionnée, conformément aux politiques et lignes directrices concernant les réceptions officielles publiées par le Conseil du Trésor.


Employee's Signature - *de l'employé*
Robert Dick

Date

Authorizing Officer's - Signature - *de l'agent responsable*

Date

Lajeunesse, Elizabeth

From: Dick, Robert
Sent: December-21-12 4:38 PM
To: Lajeunesse, Elizabeth
Subject: [REDACTED]

Beth - as I'm out of the office, would you please sign the hospitality request on my behalf as discussed.

Thanks.

Robert

s.15(1) - Int'l



Public Safety Canada / Sécurité publique Canada

Senior Assistant Deputy Minister

Sous-ministre adjoint principal

Ottawa, Canada K1A 0P8

COPY

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA

2012 OCT 29 P 3:44

2012 OCT 29 A 11:10

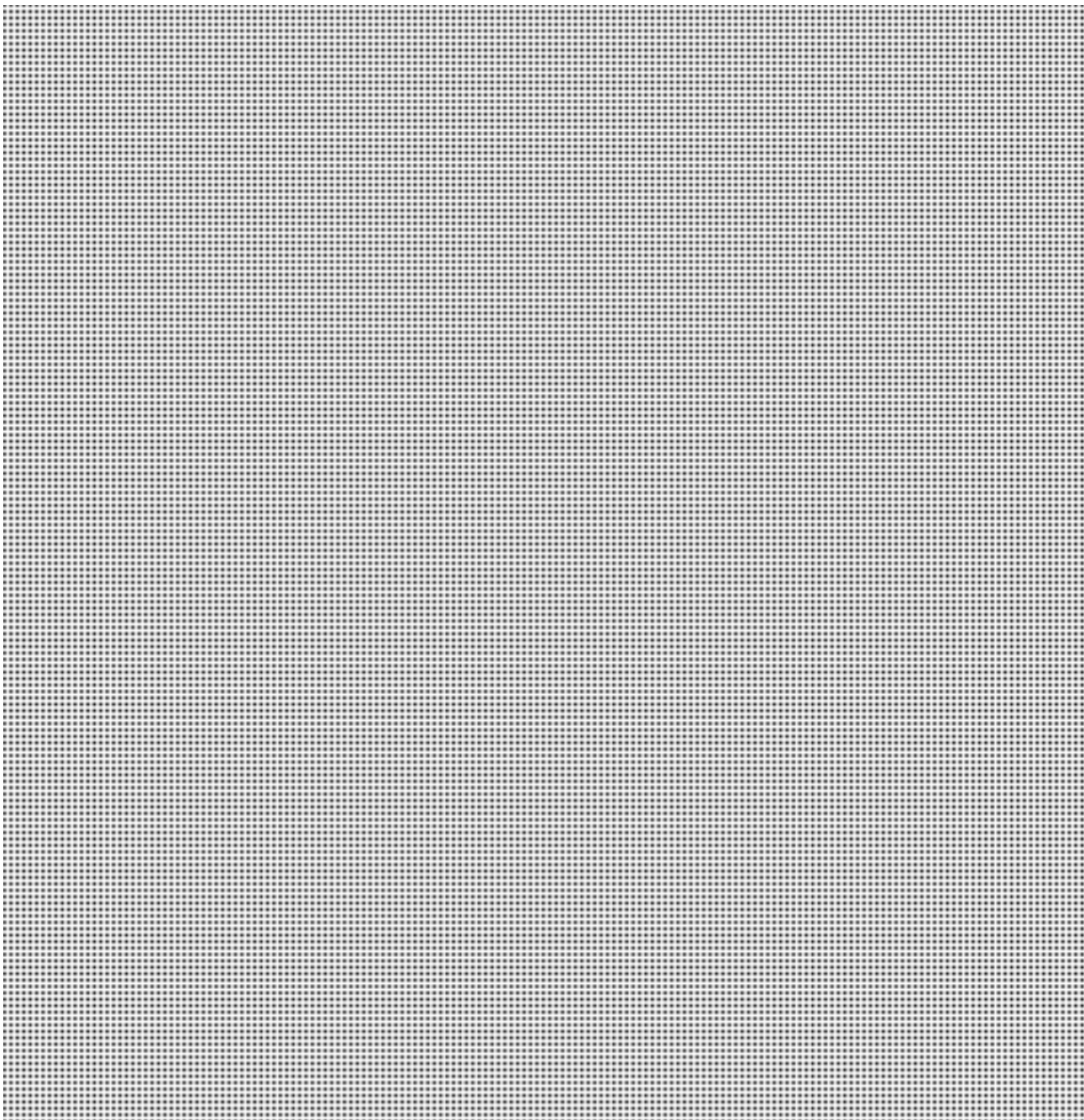
CONFIDENTIAL

DATE: **OCT 24 2012**

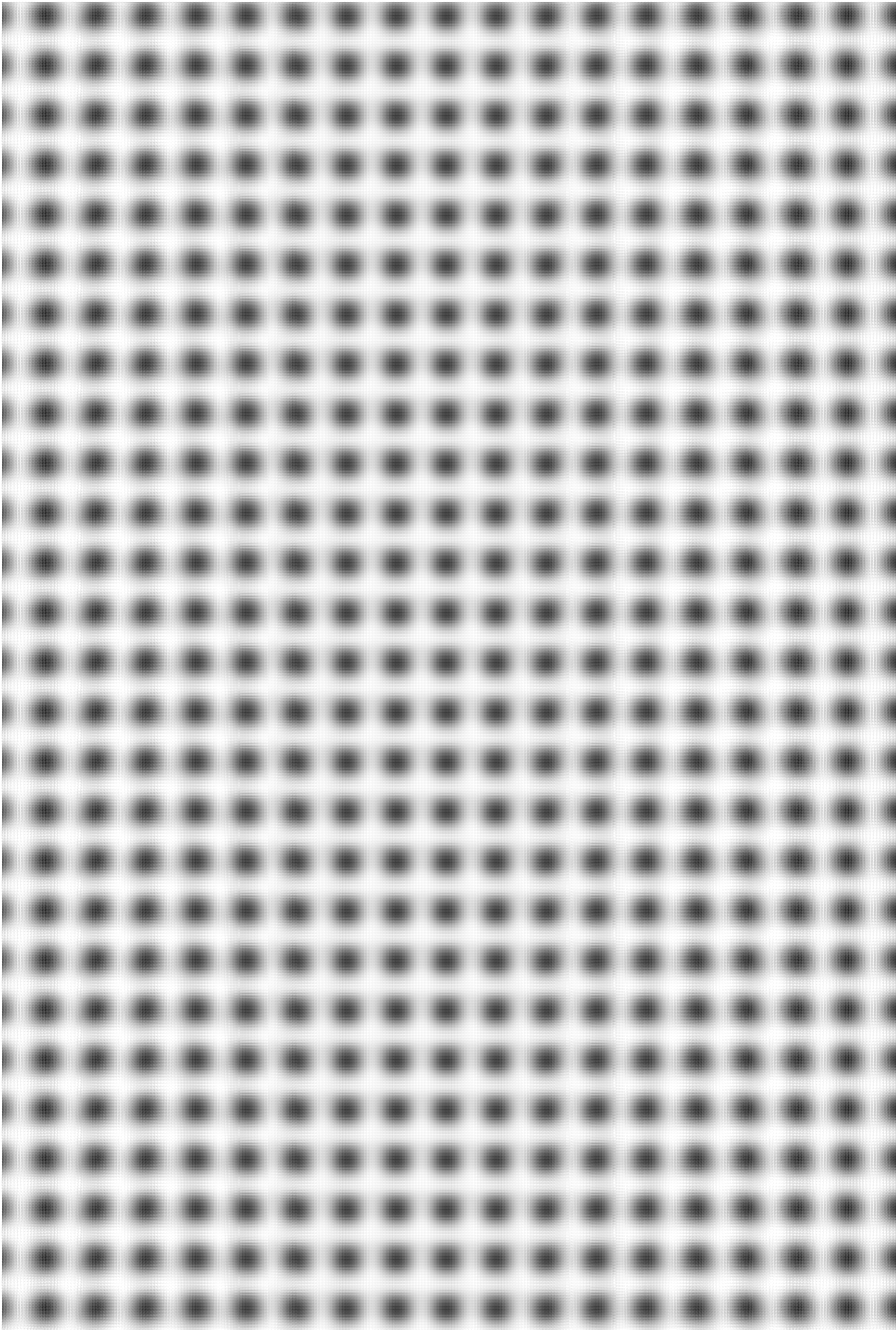
File No.: 390613

RDIMS No.: NS3005-687291

MEMORANDUM FOR THE ACTING DEPUTY MINISTER



.../2



A briefing note outlining hospitality needs related to this dialogue will follow once we have received the approval to issue an invitation.

RECOMMENDATION

It is recommended that you approve [REDACTED]

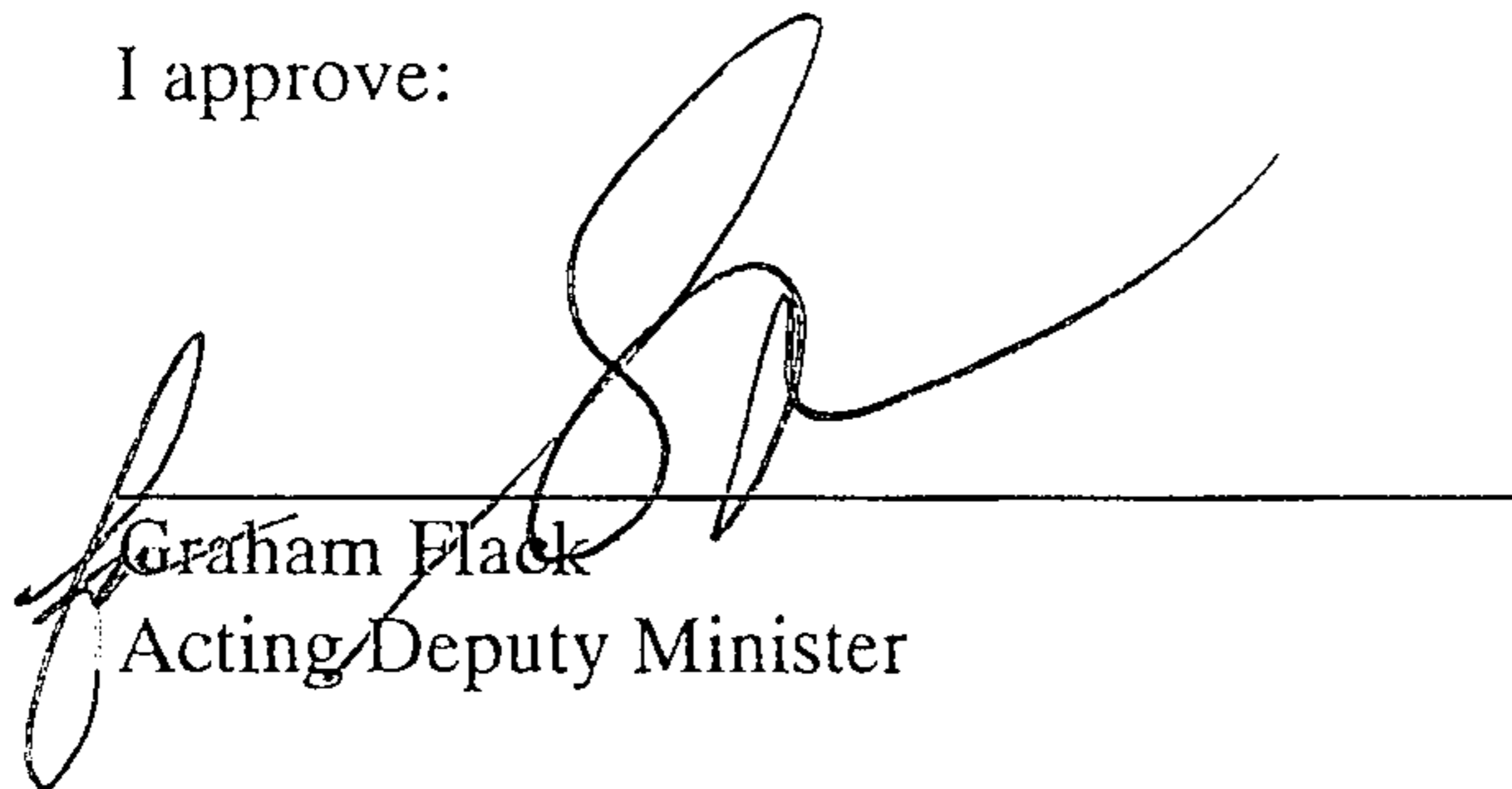
Should you require additional information, please do not hesitate to contact me or Robert Dick, Director General, National Cyber Security, at 613-990-2661.



Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (3)

I approve:



Graham Flack
Acting Deputy Minister

NOV - 1 2012

Prepared by: Ian Anderson

s.15(1) - Int'l

Sodexo Catering Estimate

January 29, 2013:

| | |
|---|--------------|
| 8:00: 45 continental #1 @ \$5.25/pers. (decaf coffee available) | = \$ 236.25 |
| 10:30: 45 Spice of Life @ \$7.50 <i>4.95</i> /pers. <i>Healthy Choice</i> | = \$ 337.50 |
| 12:00: 35 Charcuterie Buffets @ \$17.95/pers. (decaf coffee available) Caesar/Marinated Vegetables are the choices for the 2 salads | = \$ 628.25 |
| 3:30: 45 Stopover Breaks @ \$6.25/pers. (decaf coffee available) | = \$ 281.25 |
| sub total | = \$1,483.25 |
| 15% service | = \$ 222.49 |
| sub total | = \$1,705.74 |
| 13% hst | = \$ 221.75 |

January 29, 2013 total: **\$1927.49**

Afternoon break to be picked up at 3:55pm max to 4:00pm, supplementary labour charges (\$32.00/hour) charges. If break is needed after 4:00pm, supplementary labour charges (\$32.00/hour) charges.

January 30, 2014:

FORMER TAB A

| | |
|---|--------------|
| 8:00: 45 continental #1 @ \$5.25/pers. (decaf coffee available) | |
| 10:30: 45 Spice of Life @ \$7.50 <i>4.95</i> /pers. <i>Healthy Choice</i> | = \$ 337.50 |
| 12:00: 45 Wrapstravaganza @ \$17.95/pers. (decaf coffee available) Macaroni/Field Mix & Fresh Fruit | = \$ 807.75 |
| sub total | = \$1,381.50 |
| 15% service | = \$ 207.23 |
| sub total | = \$1,588.73 |
| 13% hst | = \$ 206.54 |

January 30, 2013 total: **\$1,795.27**

Grand total: **\$3,722.76**



Government Catering Services
Department of Foreign Affairs and International Trade
Phone Number: (613) 789-3518
Fax Number (613) 789-2218
Director – Robert A. Prud'homme
E-Mail: robert.prudhomme@sodexo.com

Advance Notice

To provide you with the best possible service, we require 48 business hours notice. As always, we will work with you to find solutions for your last minute needs. Catering orders with less than 24hrs notice will be based on the product and staff availability. Guaranteed numbers are required 48 business hours prior to the event.

Large corporate events consisting of 100 people or more, please place your order a minimum of 2 weeks in advance. This will allow for time to order all appropriate items, such as linen, china, flowers and specialty food items.

Planning Guidelines

The menu selections and services described should serve as a guide for planning your event. While offering great variety, this catering guide is merely a sampling of what we can do. Let us know of any dietary restrictions or specialty items that you may have in mind.

Ordering and Billing

All items are based on a per person charge unless otherwise specified.
Applicable taxes will be applied to all orders.
A surcharge may apply for orders less than the minimum quantity indicated for some menu items.
There is a minimum of \$25.00 per delivery.
We may request full payment the day of the service.
Luncheons and dinners will be charged a 15% service fee when a server is required
Prices are subject to change without notice

Cancellations

We know that at times you may need to cancel an event with short notice. Please notify us 24hrs in advance to avoid any cancellation fees due to advance preparation.

Standard Service

A catering attendant will set up and retrieve the buffet, including chafing dishes and platters. There will be a charge if additional labor is required. Labor charges will apply for services after 4pm and weekends

Equipment

Thank you for your catering order. Sodexo must recover all catering equipment. If you remove equipment from the delivery location, please notify the catering department of the new location. Any catering equipment that is not recovered will be billed to your order.

Sodexo Catering Menu

Beverages

| | |
|---------------------|---------------------------|
| Coffee | \$17.50/pot (serves 10) |
| Starbucks coffee | \$22.00/pot (serves 10) |
| Tea | \$1.75 |
| Herbal Tea | \$1.75 |
| Bottled juice | \$1.95 |
| V-8 | \$2.20 |
| Milk | \$1.75 |
| Soft drinks | \$1.75 |
| Bottled Water 591ml | \$2.25 |
| Perrier | \$2.50 |
| Water pitcher | \$3.00 (with catering) |
| Water pitcher | \$6.00 (without catering) |

Breakfast A La Carte

| | |
|-------------------------|------------|
| Muffin | \$1.75 |
| Croissant | \$1.75 |
| Danish | \$1.95 |
| Cookie | \$1.60 |
| Tea Biscuit | \$1.60 |
| Mini Breakfast Pastries | \$15.00/dz |
| Sliced fresh fruit | \$3.25 |
| Fresh fruit salad | \$3.25 |
| Whole fresh fruit | \$1.25 |
| Homemade dessert loaf | \$2.25 |
| Yogurt | \$2.00 |

BREAKFAST BUFFETS

Minimum 10 people

Continental #1 \$5.25
 Coffee, tea and juice
 Mini Breakfast pastries (2 per person)

Continental #3 \$8.25
 Coffee, tea and juice
 Mini croissants (2 per person)
 Assorted yogurt and sliced fresh fruit platter

Continental #2 \$8.25
 Coffee, tea and juice
 Homemade dessert loaf
 Sliced fresh fruit platter

Continental #4 \$8.25
 Coffee, tea and juice
 Assortment of Muffin, Danish and Croissant
 Sliced fresh fruit platter

The Executive \$12.75
 Coffee, tea and juice
 Bacon, sausage, scrambled eggs
 Mini croissants & mini muffins
 Sliced fresh fruit platter

Bagel Breakfast \$8.95
 Coffee, tea and juice
 Fresh fruit platter
 Mini bagels with cream cheese & smoked salmon,
 Light cream cheese & fruit jams

Breakfast Sandwich Buffet \$9.25
 Coffee, tea and juice
 English muffins with bacon, cheese & egg
 Sliced fresh fruit platter

COFFEE BREAKS

Minimum 10 people

| | | |
|--|------------|-----------------------------|
| <i>Spice of Life</i> | \$7.50 | <i>no</i> |
| <i>Water & juice bottles</i> | | |
| <i>Fresh fruit platter</i> | | |
| <i>Assorted yogurt</i> | | |
| <i>Low fat pretzels</i> | | |
| <i>Salty Snacks</i> | \$7.95 | |
| <i>Soft drinks & Water bottles</i> | | |
| <i>Bags of Peanuts & Chips</i> | | |
| <i>Tortilla chips & Salsa</i> | | |
| <i>Stop Over</i> | \$6.25 | <i>✓</i> |
| <i>Coffee and tea</i> | | |
| <i>Juice & water bottles</i> | | |
| <i>Assorted gourmet cookies (2 per person)</i> | | |
| <i>Sweet Tooth</i> | \$6.50 | |
| <i>Coffee and Tea</i> | | |
| <i>Water bottles & milk</i> | | |
| <i>Chocolate brownies & Nanaimo bars</i> | | |
| <i>Healthy Choice</i> | \$4.95 | <i>use this one instead</i> |
| <i>Juice & Water bottles</i> | | |
| <i>Basket of Fresh whole fruit</i> | | |
| <i>Granola bars</i> | | |

A LA CARTE

Minimum 10 people

| | |
|---|--------|
| <i>Cheese & fresh fruit, served with crackers and baguette (2.50oz)</i> | \$4.50 |
| <i>Cheese & fresh fruit served with crackers and baguette (4oz)</i> | \$5.75 |
| <i>Imported cheese tray served with crackers and baguette(4oz)</i> | \$7.25 |
| <i>Crudites & Dip</i> | \$3.25 |
| <i>Mediterranean platter</i> | \$6.50 |
| <i>Hummus, tabouleh, mini pitas & tortilla chips</i> | \$4.25 |
| <i>Nacho chips & Salsa dip</i> | \$3.95 |
| <i>Choice of Salad</i> | \$3.50 |
| <i>Deli sandwiches</i> | \$5.50 |
| <i>Assorted Wraps</i> | \$6.95 |
| <i>Deli, Open faced & wrap</i> | \$6.95 |
| <i>Signature Sandwiches</i> | \$7.95 |
| <i>Dessert squares</i> | \$2.95 |
| <i>Gourmet desserts</i> | \$4.50 |

SANDWICH LUNCHEONS

Minimum 10 people

Working Lunch Buffet..... \$14.95

Assorted deli, open-faced & wrap sandwiches
Cheese & fruit platter
Vegetable Platter & House trempette
Assorted squares
Coffee & Tea

Traditional Lunch Buffet..... \$14.95

Assorted deli sandwiches on Kaiser roll, rye & whole wheat breads
Choice of two salads
Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or Field Mix & Fresh Fruit, Tomatoes & Cucumbers, Nicoise
Vegetable Platter & House trempette
Assorted squares
Coffee & Tea

Wrapstravaganza \$17.95

An assortment of tortillas, shaved premium meats, egg, tuna & grilled vegetables
Choice of two salads:
Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise
Vegetable Platter & House trempette
Fruit Platter
Assorted Squares
Coffee & Tea

Specialty Sandwich Buffet \$18.25

Assorted open faced sandwiches
Choice of two salads:
Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise
Vegetable Platter & House trempette
Fruit Platter
Assorted squares
Coffee & Tea

Charcuterie buffet \$17.95

*Assorted cold cuts, grilled chicken breasts and grilled marinated vegetables
Breads, Panini, Kaiser & wraps
Condiments (lettuce, tomatoes, mayonnaise & mustard)*

Choice of two salads:

*Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne,
Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, French
Nicoise*

Fruit Platter

*Assorted squares
Coffee & Tea*

Signature Sandwich Buffets \$24.95

Greek

*Thinly sliced smoked turkey breast, goat's cheese, roasted red peppers & fresh basil
Served with honey mustard on Pita*

"Il Roma"

*Grilled seasonal vegetables, fresh mozzarella, roasted red peppers, basil, lettuce & tomato
Served on Panini*

Chutney Chicken

Grilled chicken breast with a mango chutney served on Ciabatta bread.

Beef Melt

*Pesto topped Focaccia bread beneath layers of beef with caramelized onions and slices
of Asiago Cheese*

Imported Cheese tray

Mediterranean Platter

Hummus & Tabouleh served with mini pitas & tortilla chips

Gourmet dessert selection

Coffee & Tea

Ultimate Deli Packages

| | |
|--|-------------|
| <i>Tijuana Turkey Chipotle Club.....</i> | <i>\$13</i> |
| <i>Tuscan Grilled Chicken.....</i> | <i>\$13</i> |
| <i>Roast Beef and Cheddar on Baguette.....</i> | <i>\$11</i> |
| <i>Vegetarian Wrap.....</i> | <i>\$11</i> |

Served with vegetables & dip, assorted cookies, coffee & tea

Light HoT Buffet

(min 10)

| | | |
|--------------------------------------|---|-------------|
| <i>Chicken Supreme</i> | <i>roasted potatoes, seasonal vegetables.....</i> | <i>\$15</i> |
| <i>Chicken Korma</i> | <i>Jasmine rice, seasonal vegetables, Naan bread.....</i> | <i>\$15</i> |
| <i>Chicken à la King</i> | <i>white rice, seasonal vegetables</i> | <i>\$13</i> |
| <i>Turkey Vol-au-vent</i> | <i>seasonal vegetables</i> | <i>\$13</i> |
| <i>Oven baked Lasagna (min 15)</i> | <i>garlic bread, Caesar salad.....</i> | <i>\$13</i> |
| <i>Vegetarian Lasagna (min 15)</i> | <i>garlic bread, Caesar salad.....</i> | <i>\$13</i> |
| <i>Vegetarian Quiche</i> | <i>field mix salad</i> | <i>\$12</i> |
| <i>Swedish Meat Balls</i> | <i>rice Pilaf, seasonal vegetables</i> | <i>\$13</i> |
| <i>Beef Stroganoff</i> | <i>egg noodles, seasonal vegetables</i> | <i>\$14</i> |
| <i>Shepherd's Pie (min 15)</i> | <i>seasonal vegetables</i> | <i>\$13</i> |
| <i>Roast Beef</i> | <i>mashed potatoes, gravy, seasonal vegetables</i> | <i>\$14</i> |
| <i>Marinated Beef Teriyaki Kabob</i> | <i>curried rice, seasonal vegetables</i> | <i>\$14</i> |
| <i>Salmon filet</i> | <i>rice Pilaf, seasonal vegetables</i> | <i>\$15</i> |
| <i>Pizza</i> | <i>Caesar salad, vegetable & dip</i> | <i>\$13</i> |

*All Light Hot Buffet served with
Assorted squares or cookies
Coffee, tea*

Buffet 1 \$ 25.95

Crusty roll & butter

Choice of two salads

Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise

Domestic cheese tray

Vegetable & dip

Roast beef au jus & horseradish

Steamed filet of Atlantic salmon with lemon dill sauce

Chateau potatoes with herbs

Oven roasted vegetables

Choice of dessert

Cheesecake with berry topping, chocolate mouse cake with raspberry coulis, fresh fruit salad, strawberry tart, cream horns, homemade banana cake, fruit pie, key lime pie, chocolate cake, carrot cake, assorted squares

Coffee & Tea

Buffet 2 \$24.95

Crusty roll & butter

Choice of two salads

Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise

Domestic cheese tray

Vegetable & dip

Vegetarian lasagna

Tarragon chicken breast

Roasted Parisienne potatoes

Green bean Almondine

Glazed baby carrots

Choice of dessert

Cheesecake with berry topping, chocolate mouse cake with raspberry coulis, fresh fruit salad, strawberry tart, cream horns, homemade banana cake, fruit pie, key lime pie, chocolate cake, carrot cake, assorted squares

Coffee & Tea

Buffet 3 \$24.95

Crusty roll & butter

Choice of two salads

Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise

Domestic cheese tray

Vegetable & dip

Marinated beef teriyaki kabob

Traditional pan seared rainbow trout with lemon butter sauce

Curried Rice

Seasonal Vegetables

Choice of dessert

Cheesecake with berry topping, chocolate mouse cake with raspberry coulis, fresh fruit salad, strawberry tart, cream horns, homemade banana cake, fruit pie, key lime pie, chocolate cake, carrot cake, assorted squares

Coffee & Tea

Buffet 4..... \$23.95

Crusty roll & butter

Choice of two salads

Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise

Domestic cheese tray

Vegetable & dip

Pasta Primavera

Chicken cordon bleu

Rice Pilaf

Vegetable medley: baby carrots, yellow & green beans

Choice of dessert

Cheesecake with berry topping, chocolate mouse cake with raspberry coulis, fresh fruit salad, strawberry tart, cream horns, homemade banana cake, fruit pie, key lime pie, chocolate cake, carrot cake, assorted squares

Coffee & Tea

Buffet 5 \$23.95

Crusty roll & butter

Choice of two salads

Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise

Domestic cheese tray

Vegetable & dip

Veal Madeleine

Manicotti in white cream sauce

Rice Pilaf

Buttered baby carrots

Choice of dessert

Cheesecake with berry topping, chocolate mouse cake with raspberry coulis, fresh fruit salad, strawberry tart, cream horns, homemade banana cake fruit pie, key lime pie, chocolate cake, carrot cake, assorted squares

Coffee & Tea

Buffet 6 \$22.95

Crusty roll & butter

Choice of two salads

Caesar, Coleslaw, Garden, Greek, Macaroni, Marinated Vegetables, Tuna & Penne, Red Potatoes, Spinach or field mix & fresh fruit, Tomatoes & Cucumbers, Nicoise

Domestic cheese tray

Vegetable & dip

Chicken Alfredo

Beef Bourguignon

Fettuccini pasta

Zucchini & tomato

Choice of dessert

Cheesecake with berry topping, chocolate mouse cake with raspberry coulis, fresh fruit salad, strawberry tart, cream horns, homemade banana cake, fruit pie, key lime pie, chocolate cake, carrot cake, assorted squares

Coffee & Tea

THEME BUFFETS

Minimum 20 people

LAVINCITA ITALIAN BUFFET..... \$20.95

(add 6oz chicken breast with Portobello mushroom sauce \$6.95)

- Bruschetta*
- Marinated Antipasto Platter*
- Caesar or tomato basil salad*
- Choice of 2 Pastas & 2 sauces*
- Vegetable & dip*
- Sliced fresh fruit platter*
- Tiramisu*
- Coffee & Tea*

PACIFIC RIM ORIENTAL BUFFET..... \$20.95

- Thai salad or Szechuan Noodle salad*
- Spring Rolls*
- Ginger Beef & broccoli*
- Chicken Stir Fry*
- Rice*
- Vegetable & dip*
- Sliced fresh fruit platter*
- Fresh fruit Tarts & Fortune cookies*
- Coffee & Tea*

TIERRA DEL SOL (tex-Mex)..... \$20.95

- Black bean & corn salad*
- Tri-colored chips & salsa*
- Beef or chicken Fajitas*
- Mexican rice & refried beans*
- Vegetable & dip*
- Sliced fresh fruit platter*
- Bunuelos with chocolate & nuts*
- Coffee & Tea*

CHEZ MIDI \$20.95

- Fresh vegetables served with Tzatziki*
- Greek salad*
- Chicken & Pork Souvlaki*
- Rice & roasted potatoes*
- Vegetable & dip*
- Sliced fresh fruit platter*
- Baklava*
- Coffee & Tea*

DINNER BUFFETS

Minimum 30 people

Choice of one appetizer

Soups

- Carrot & ginger*
- Butternut squash*
- Bisque*
- Wild mushroom*

Salads

- Baby spinach with raspberry vinaigrette*
- Mixed greens with strawberries & mandarins*
- California Greens with citrus vinaigrette*
- Summer sensation salad*

Choice of main course

- Prime Rib au Jus \$32.95*
Served with roasted Parisienne potatoes & seasonal vegetables
- Chicken Kiev or Cordon Bleu..... \$27.95*
Served with choice of rice & seasonal vegetables
- Three-pepper crusted salmon with a white wine sauce \$27.95*
Served with Basmati rice & seasonal vegetables
- Pork tenderloin served with Portobello mushrooms \$27.95*
Served with choice of rice or potatoes & seasonal vegetables
- Thai Curry chicken with an avocado sauce \$23.95*
Served with rice & roasted vegetables

Choice of gourmet dessert

- Cheesecake with berry topping*
- Chocolate mousse cake with raspberry coulis*
- Fresh fruit in a chocolate cup*
- Black Forest Cake*
- Carrot Cake*
- Hazelnut Cake*

Coffee & Tea

RECEPTION SELECTIONS

- Hot Hors D'Oeuvres \$20.95/dz*
A selection of hot hors d'oeuvres will be served
- Cold Canapés \$20.95/dz*
A selection of cold hors d'oeuvres will be served
- SUSHI \$20.95/dz*
California rolls, Vegetable Futomaki, Spicy Salmon roll
Spicy crab roll, Cali-Shogun & Deluxe combo

ESTIMATE

**Office of Protocol
Bureau du Protocole**

*Ninth Floor/Neuvième Étage
7, Rideau Gate*

Services Provided for: **Conference on Cyber Security**
 Room or Location: **A9 - S12** Date: **January 29, 2013**
 Host or Hostess: **TBC** Contact Name: **J. Hayward**
 Number of Guests: **11** Estimate per guest incl. Service and HST: \$ **45.77**

Meal Period: **Lunch - Hot Plated**

| Category: | Qty | Price Per | Sub Total | HST | Total |
|------------------------------|-----------|--------------|---------------|--------------|---------------|
| Lunch - Hot Plated | 10 | 28.88 | 288.80 | 37.54 | 326.34 |
| <i>Alcoholic Beverages</i> | | | | | |
| Beer | 0 | 1.50 | - | - | - |
| Spirits | 0 | 3.00 | - | - | - |
| Wine | 3 | 12.50 | 37.50 | 4.88 | 42.38 |
| <i>Sub Total</i> | <i>3</i> | | <i>37.50</i> | <i>4.88</i> | <i>42.38</i> |
| <i>Miscellaneous Charges</i> | | | | | |
| Flowers | | | 90.00 | 11.70 | 101.70 |
| Rental | | | - | - | - |
| Movers | | | - | - | - |
| <i>Sub Total</i> | | | <i>90.00</i> | <i>11.70</i> | <i>101.70</i> |
| Total Estimate | | | 292.30 | 54.12 | 430.42 |

These figures are provided as estimates for budgeting purposes only and are subject to change.
Charges are based on consumption. Amount(s) transferred will not include HST.

Service provided by/Les services fournis par:

THE WESTIN
OTTAWA

Courtyard Restaurant
 21 George St., Byward Market
 Ottawa, ON K1N 8W5 Canada
 Telephone Number: (613) 241-1516
 Fax Number: (613) 241-5738
 E-mail: info@courtyardrestaurant.com

EVENT ORDER: CY10218

Event Date: Tuesday, January 29, 2013
Event Name: PUBLIC SAFETY CANADA GROUP
 DINNER
Site: Courtyard Restaurant
Salesperson: Miranda Forbes

Contact: Melanie Mohammed
Mailing Address: Public Safety Canada
E-mail: Melanie.Mohammed@ps-sp.gc.ca

Daytime Phone: (613) 991-2700
Fax Number:
On-Site Contact:

| Day/Date | Start/End Time | Location | Function | Set-Up | Est | Gte | Set | Rental |
|---------------|----------------|-----------------------|----------|--------|-----|-----|-----|--------|
| Tue., 1/29/13 | 7:00PM-10:00PM | Bar Area Loft Room | Dinner | | 35 | | | \$0.00 |

| FOOD | QTY | PRICE | TOTAL |
|--|---------------|--------------------|-----------------------|
| 7:00 PM / BAR AREA / LOFT ROOM / DINNER | | | |
| 2012 Hors d'oeuvres | | | |
| <i>Served at 7:00pm</i> | | | |
| Small - Antipasto Platter with Proscuitto, Cappicola, Marinated Bocconcini, Spicy Eggplant, Honeydew Melon, Cantaloupe, Black Olive Tapenade and Crostini (serves 20 to 25 guests) | 1 | \$120.00 | \$120.00 |
| Crostini with Pear Jam and Oven Dried Tomatoes - Per Dozen | 2 | \$14.00 | \$28.00 |
| 2013 Winter Dinner Menu - Indulge | 35 | \$52.00 | \$1,820.00 |
| <i>Appetizers</i> | 36 | | 1,972.00 |
| 2 appetizers to be confirmed | | | |
| <i>Sorbet</i> | | | |
| House-Made Sorbet | | | |
| <i>Main Courses</i> | | | |
| 3 main courses to be confirmed | | | |
| <i>Desserts</i> | | | |
| 3 desserts to be confirmed | | | |
| <i>Includes The Following</i> | | | |
| Freshly Baked Bread and Butter | | | |
| Freshly Brewed Coffee and Specialty Teas | | | |

| BEVERAGE | QTY | PRICE | TOTAL |
|---|---------------|--------|---------------------|
| 7:00 PM / BAR AREA / LOFT ROOM / DINNER | | | |
| Host Bar | | | |
| Bar Estimate - Standard Bar Drink Tickets (beverages up to \$6.19 plus tax) - two per guest | 70 | \$5.95 | \$416.50 |
| ** tickets provided by client ** | 72 | | 429.40 |

| SET-UP & SERVICE | QTY | PRICE | TOTAL | | | |
|--|-----|-------|-------|--|--|--|
| <p>7:00 PM / BAR AREA / LOFT ROOM / DINNER</p> <p>GROUP BOOKING POLICIES: Guaranteed Guest Count required 48 hours in advance of bookings, with all charges based on Guest Count Guarantee. Menu selections required at the latest one week in advance of the booking. We reserve the right to reallocate function space should the final number of guests either exceed the maximum capacity or not meet the minimum number of guests required.</p> <p>MINIMUM GUEST COUNT: The Loft Room requires a minimum guest count of 25 guests.</p> <p>If the final guest count provided two days prior to the event is lower than the minimum guest count required a minimum bill of \$1870.00 plus tax and gratuity will apply if you wish to remain in the private room. All food and beverages purchased through the Courtyard Restaurant goes towards the minimum bill with any shortfall being charged as a room charge. If available, your group may switch a smaller room that may suit your event more appropriately. Another option may be to make your event a semi-private reservation; there is no minimum bill for a semi-private reservation.</p> <p>CANCELLATION POLICY: There is no charge for cancellations made up to 2 days prior to your event. Cancellations made on the day prior to the event will be subject to a charge of 25% of the estimated food and beverage costs. Cancellations made on the day of the event will be subject to a charge of 50% estimated food and beverage costs. No-shows will be subject to a charge of 100% estimated food and beverage costs. Please note all cancellations must be received in writing.</p> | | | | | | |

| ESTIMATED CHARGES (Actual Charges Presented At Conclusion of Event) | | | | | | |
|---|--------------------------------|----------------------------|------------|----------------------------|--------------------------------|------------|
| | Charges | Service Charge 17.50 % | Subtotal | Sales Tax | Total | |
| Facility Rental | \$0.00 | \$0.00 | \$0.00 | \$0.00 | \$0.00 | |
| Food | 1992 \$1,068.00 | 348.6 \$344.40 | \$2,312.40 | 258.96 \$255.84 | 2,599.96 \$2,568.24 | |
| Beverage | 428.4 \$416.50 | 74.97 \$72.89 | \$489.39 | 55.69 \$54.15 | 559.06 \$543.54 | |
| Set-Up | \$0.00 | \$0.00 | \$0.00 | \$0.00 | \$0.00 | |
| Grand Totals | 2,420.40 \$2,384.50 | 423.57 \$417.29 | \$2,801.79 | 314.65 \$309.99 | 3,158.62 \$3,111.78 | |
| Payments Received | | | | | \$0.00 | |
| Payment Arrangements: Upon Conclusion | | | | | Balance Due | \$3,111.78 |

Comments:



COURTYARD
RESTAURANT

Group Menu

The Courtyard Restaurant is committed to culinary excellence and to using local and sustainable ingredients whenever possible. This commitment means our menu selections change seasonally allowing us to bring you the freshest local ingredients at their peak. We consult with our farmer and supplier partners in order to create innovative menus using organic and sustainable ingredients.

Seasonal Menu Dates:

Winter - Begins January 29th, 2013

Spring - Begins April 3rd, 2013

Summer - Begins June 26th, 2013

Fall - Begins August 20th, 2013

Prices in this document are valid
until January 28th 2013

COURTYARD
RESTAURANT

21 George Street Ottawa,
Ontario, Canada K1N 8W5

t. 613.241.1516
f. 613.241.5738

info@courtyardrestaurant.com
www.courtyardrestaurant.com



Signatures Bistro at Le Gordon Bleu

453 Laurier Avenue East

Notes:

- Room is not private

| Food | Qty | Price | Total |
|--|------------|--------------|--------------|
| Charcuterie platter, French bread and condiments | 25 | \$11.00 | \$275.00 |
| Cromesquis of blue cheese and pear (served by dozen) | 2 | \$34.00 | \$68.00 |
| Warm roasted butternut squash, apple and romaine salad, Manchego cheese; Zucchini and spinach velouté, truffle oil; Beef tenderloin with wild mushrooms, port reduction, potato purée, seasonal vegetables; Light cheesecake with seasonal fruit compote | 35 | \$66.00 | \$2,310.00 |

| Beverage | Qty | Price | Total |
|--|------------|--------------|--------------|
| Host bar Estimate – Premium bar drink tickets (beverages up to \$8.00 plus tax) – two per guest | 70 | \$8.00 | \$560.00 |

| Estimated Charges | | | | | |
|--------------------------|-------------------|---------------------------|-------------------|----------------------|-------------------|
| | Charges | Service Charge 15% | Subtotal | Sales Tax 11% | Total |
| Facility rental | \$0.00 | \$0.00 | \$0.00 | \$0.00 | \$0.00 |
| Food | \$2,653.00 | \$397.95 | \$3,050.95 | \$335.60 | \$3,386.55 |
| Beverage | \$560.00 | \$84.00 | \$644.00 | \$70.84 | \$714.84 |
| Grand totals | \$3,213.00 | \$481.95 | \$3,694.95 | \$406.44 | \$4,101.39 |

Metropolitan Brasserie and Restaurant

700 Sussex Drive

Notes:

- Room is private; can accommodate 45 people

| Food | Qty | Price | Total |
|--|-----|---------|------------|
| Selection of Fine Canadian and European Cheeses | 25 | \$12.00 | \$300.00 |
| Smoked duck, arugula, tomato preserves with Asiago toasts | 2 | \$25.00 | \$50.00 |
| Dinner #2: Lobster bisque; choice of two salads; choice of four mains; choice of two desserts | 35 | \$58.00 | \$2,030.00 |

| Beverage | Qty | Price | Total |
|--|-----|--------|----------|
| Host bar Estimate – Premium bar drink tickets (beverages up to \$8.00 plus tax) – two per guest | 70 | \$7.50 | \$525.00 |

| Estimated Charges | | | | | |
|---------------------|-------------------|-----------------------|-------------------|-----------------|-------------------|
| | Charges | Service Charge 18% | Subtotal | Sales Tax 11% | Total |
| Facility rental | \$0.00 | \$0.00 | \$0.00 | \$0.00 | \$0.00 |
| Food | \$2,380.00 | \$428.40 | \$2,808.40 | \$308.92 | \$3,117.32 |
| Beverage | \$525.00 | \$94.50 | \$619.50 | \$68.15 | \$687.65 |
| Grand totals | \$2,905.00 | \$522.90 | \$3,427.90 | \$377.07 | \$3,804.97 |

Hy's Selection of Set Menus

Dinner Menu 1

Daily Homemade Soup

or

Tossed Green Salad

Peppercorn New York Steak

or

Buttermilk Fried Chicken

or

Filet of Salmon with White Wine Butter Sauce

Coffee, Tea or Decaf Coffee

\$49.95

Add Dessert of Crème Brulee or Apple Crumble

+\$ 8.95/per.

Dinner Menu 2

Daily Homemade Soup

or

Caesar Salad

or

Jumbo Shrimp Cocktail

New York Striploin Steak

or

Buttermilk Fried Chicken

or

Filet of Salmon with White Wine Butter Sauce

Hy's Famous Cheesecake

or

Crème Brulee

Coffee, Tea or Decaf

\$59.95

Dinner Menu 3

Hy's Caesar Salad

or

Daily Soup

or

Escargot

baked with a garlic parsley butter

Roast Prime Rib of Beef Au Jus

or

Filet Mignon

or

Filet of Salmon with White Wine Butter Sauce

or

Buttermilk Fried Chicken

Hy's Famous Cheesecake

or

Apple Crumble

Coffee or Tea

\$65.95

Dinner Menu #4

Prawn Cocktail

or

Escargot

baked with a garlic parsley butter

Tossed Green Salad

or

Daily Homemade Soup

Peppercorn New York Steak

or

Filet Mignon

or

Prawn and Scallop Newburg

or

Buttermilk Fried Chicken

Hy's Famous Cheesecake

or

Crème Brulee

or

Apple Crumble

Coffee or Tea

\$75.95

Dinner Menu 5

Garlic Prawns

or

Escargot

baked with a garlic parsley butter

or

Dungeness Crab Cake

With housemade coleslaw

Lobster Bisque

or

Daily Homemade Soup

Caesar Salad

Filet Neptune

(Topped with Crabmeat, Asparagus and Hollandaise Sauce)

or

Roast Prime Rib of Beef Au Jus

or

Roast Rack of Lamb

or

Cuban Lobster Tails

Hy's Famous Cheesecake

or

Crème Brulee

or

Apple Crumble

Tea or Coffee

OTTAWA HYS CANAPE SELECTIONS

Cheese Platter \$95.00

An assortment of fine cheeses, local and imported.

Vegetable Platter \$55.00

Fresh market vegetables arranged on a platter with Hys house dipping sauce

Apple walnut salad on endive petal \$30 per dozen

Finely diced apple, red pepper, and crushed walnuts mixed with crème fraiche and white raisins. Placed on and endive petal.

Beef Carpaccio on Lotus Root \$35.00 per dozen

Peppered and seared tenderloin tips thinly sliced and placed on lotus root with shaved ginger and diced green onion.

Tuna Tartar \$40.00 per dozen

Finely diced Ahi Tuna tossed in a shallot, sesame oil, soy sauce and lime juice mixture. Placed on wonton soup spoons and topped with wasabi masago and tobiko.

Tempura Prawns \$40.00 per dozen

Tempura battered prawns with a mango chutney.

Garlic sautéed prawns \$40.00 per dozen

Prawns sautéed with garlic, shallots, tomato concasser, fresh tarragon and green peppercorns. Flambéed with pernod and white wine in a cream sauce.

Mini Yorkshire puddings with shaved Prime Rib \$35.00 per dozen

Mini Yorkshires cut in half with the caramelized onion and balsamic remoulade spread on top and bottom halves.

Marinated Lamb Chops \$60.00 per dozen

Frenched lamb chops marinated in oil, garlic, rosemary and thyme. Grilled and cooked to medium rare.

Mini Crab Cakes with Caramelized Onion Remoulade \$45.00 per dozen

Red Wine
Canada
Cabernet Sauvignon & Cabernet-Based Blends

| | | |
|------|---|-----|
| 1112 | Lailey Vineyards Cabernet-Merlot 2010, Niagara Peninsula, Ontario | 35 |
| 509 | Fielding Cabernet Franc 2010, Niagara Peninsula, Ontario | 49 |
| | Stanner's Vineyard Cabernet Franc 2010, Prince Edward County | 50 |
| 3021 | Fielding Estate Cabernet Sauvignon/Syrah 2008, Beamsville Bench, Ontario | 65 |
| 311 | Cave Spring Vintners "La Penna" 2006, Beamsville Bench, Ontario | 65 |
| 407 | Lailey Vineyards Cabernet Sauvignon 2010, Niagara River, Ontario | 66 |
| 4062 | Pillitteri "Exclamation Series Reserve" Cabernet Franc 2007, Niagara Peninsula, Ontario | 74 |
| 306 | Southbrook "Whimsy Lot 19" Cabernet Sauvignon 2007, Niagara Peninsula, Ontario | 76 |
| 407 | Hidden Bench "Terroir Cache" Bordeaux Blend 2008, Beamsville Bench, Ontario | 77 |
| 3041 | Harbour Estates "Premier Vintage" 2002, Niagara Peninsula, Ontario | 80 |
| 5103 | Rosehall Run "Carriage House Select" Cabernet Franc 2007, Prince Edward County, Ontario | 80 |
| 1182 | Stratus Cabernet Franc 2007, Niagara Peninsula, Ontario | 80 |
| 307 | Chateau des Charmes "Equuleus" 2007, St. David's Bench, Ontario | 90 |
| 9052 | Reif Estate "1st Growth" Cabernet Sauvignon/Merlot 2007, Niagara Peninsula, Ontario | 95 |
| 907 | Reif Estate "1st Growth" Cabernet Sauvignon 2007, Niagara Peninsula, Ontario | 95 |
| 9242 | Poplar Grove "The Legacy" 2006, Okanagan Valley, BC | 95 |
| 906 | Stratus "Red" 2007, Niagara Peninsula, Ontario | 97 |
| 941 | Kacaba Vineyards Meritage 2007, Niagara Escarpment, Ontario | 98 |
| 9122 | Fielding Estate Cabernet Sauvignon 2007, Beamsville Bench, Ontario | 115 |
| 4051 | Karlo Estates "The Fifth Element" Petit Verdot 2010, Ontario | 86 |
| | Fielding Estate "Chosen Few" 2008, Beamsville Bench, Ontario | 115 |
| 903 | Fielding Estate Meritage 2007, Beamsville Bench, Ontario | 132 |
| 937 | Mission Hill "Oculus" 2005, Okanagan Valley, BC | 160 |
| 915 | Stratus Cabernet Sauvignon 2007, Niagara Peninsula, Ontario | 160 |
| 9112 | Hidden Bench "La Brunante" Bordeaux Blend 2007, Beamsville Bench, Ontario | 190 |
| | Painted Rock "Red Icon" 2008, Okanagan Valley, BC | 185 |
| | Mike Weir Estate Cabernet/Shiraz 2003, Niagara Peninsula, Ontario 3L | 300 |

\$93.95

Some Guidelines to Consider

- **A minimum of twelve persons is required for all pre-set menus**
- **Fresh vegetables and potatoes accompany all pre-set dinner and lunch menus.**
- **Special needs or requests will be accommodated if at all possible, i.e.: Vegetarian or allergy requirements.**
- **All menus are flexible according to the customer's wishes.**
- **All prices are pre tax and gratuities.**
- **For any special occasion, that may require a different menu, Please call our restaurant.**

Please contact us with any questions!

Sincerely,

**Craig Stevenson
General Manager
(613) 234 - 4545
(613) 234 - 1229 fax
ottawa@hyssteakhouse.com**

Hy's Steakhouse Set Menu
Package

Please call for more information.

Phone: 613 - 234 - 4545

Fax: 613 - 234 - 1229

e-mail:

ottawa@hyssteakhouse.com

**Thanks for thinking of Hy's for
your group function!**

Craig Stevenson
General Manager



47 Clarence In the Market

- Home
- Reservations
- Menus
- Announcements
- Contact
- Gift Certificate
- Holiday Bookings & NY Eve
- Private Planning & Group Events
- Weddings
- Showcase

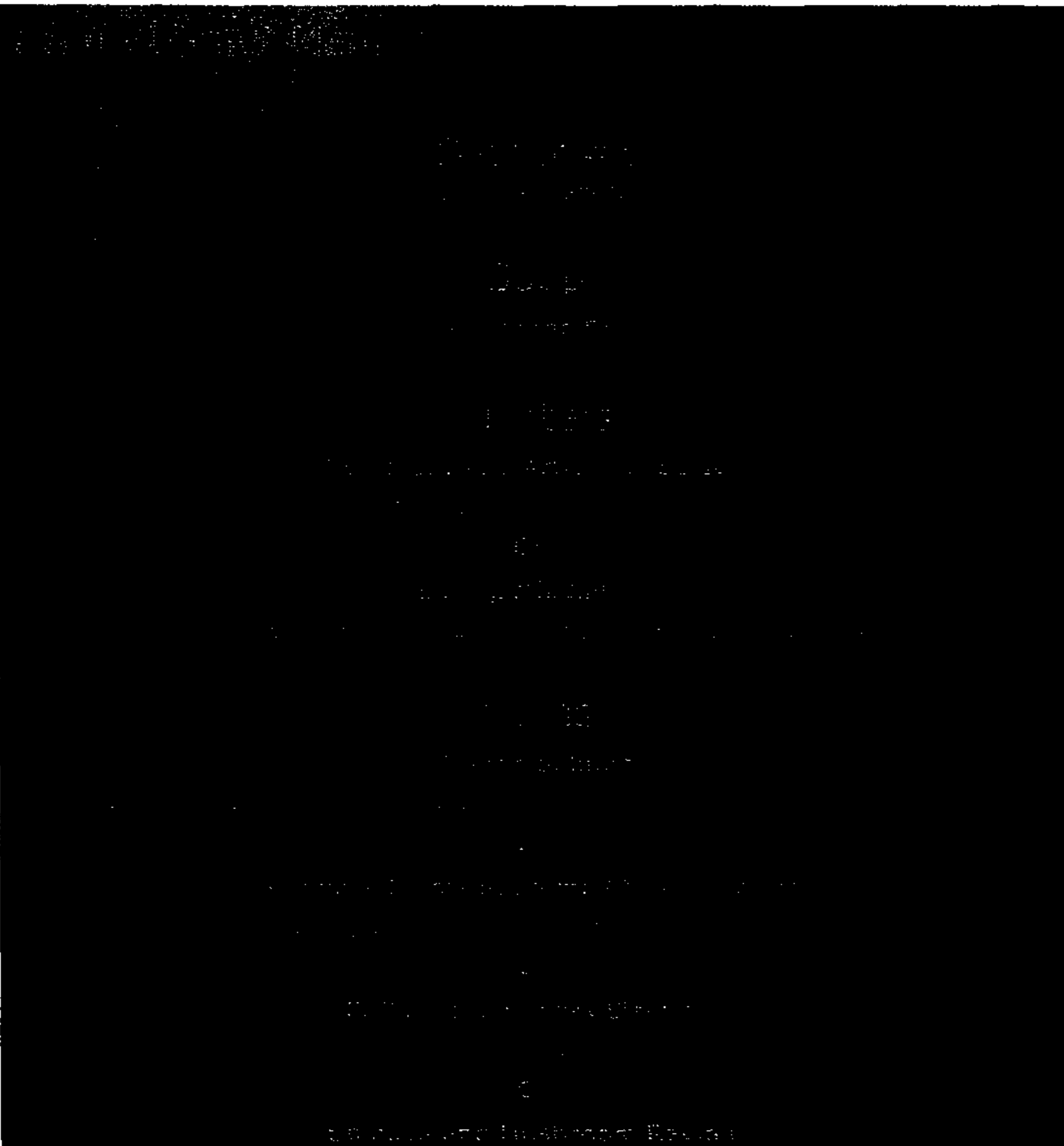
Reservation

2 Guests

Mon Dec 10

1:15 PM

Tel: 613-241-1343
Sign up for our eBulletin





47 Clarence In the Market

- Home
- Reservations
- Menus
- Announcements
- Contact
- Gift Certificate
- Holiday Bookings & NY Eve
- Private Planning & Group Events
- Weddings
- Showcase

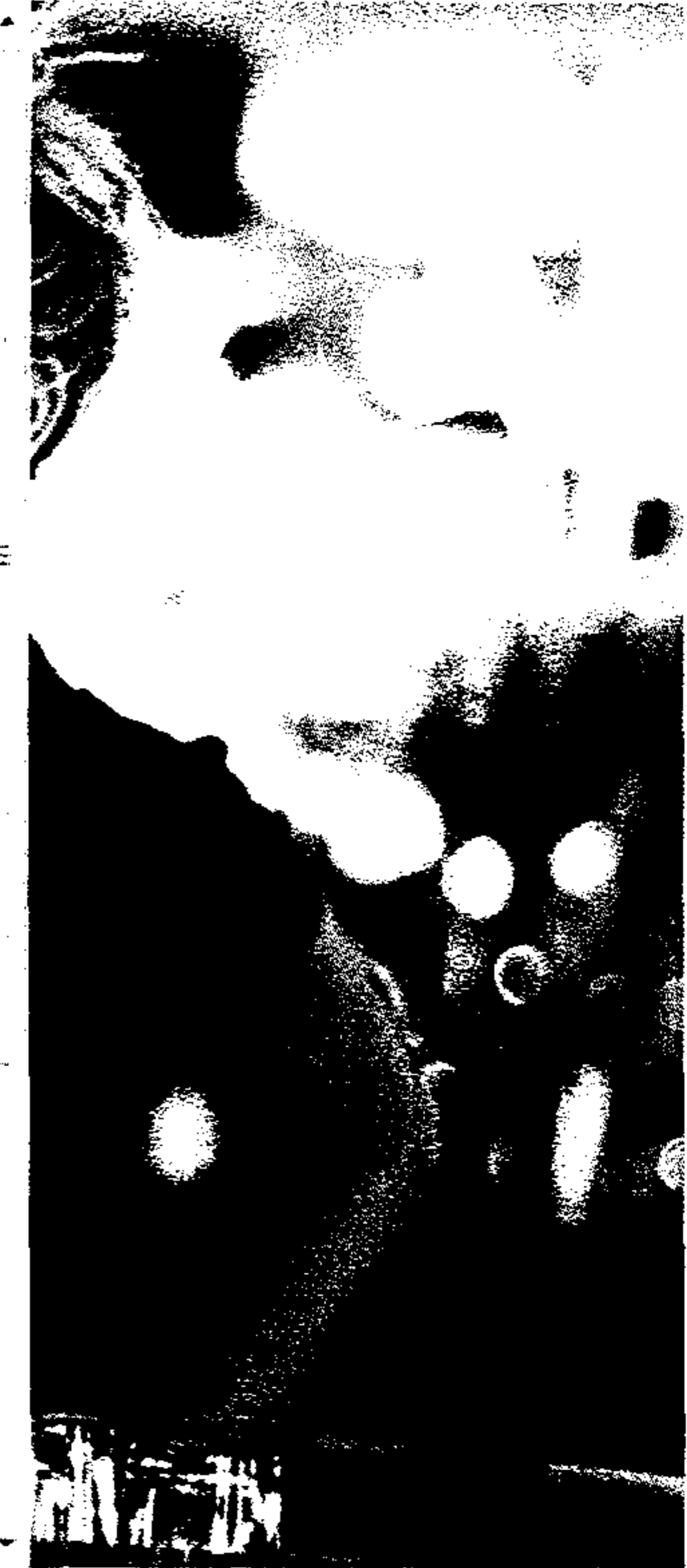
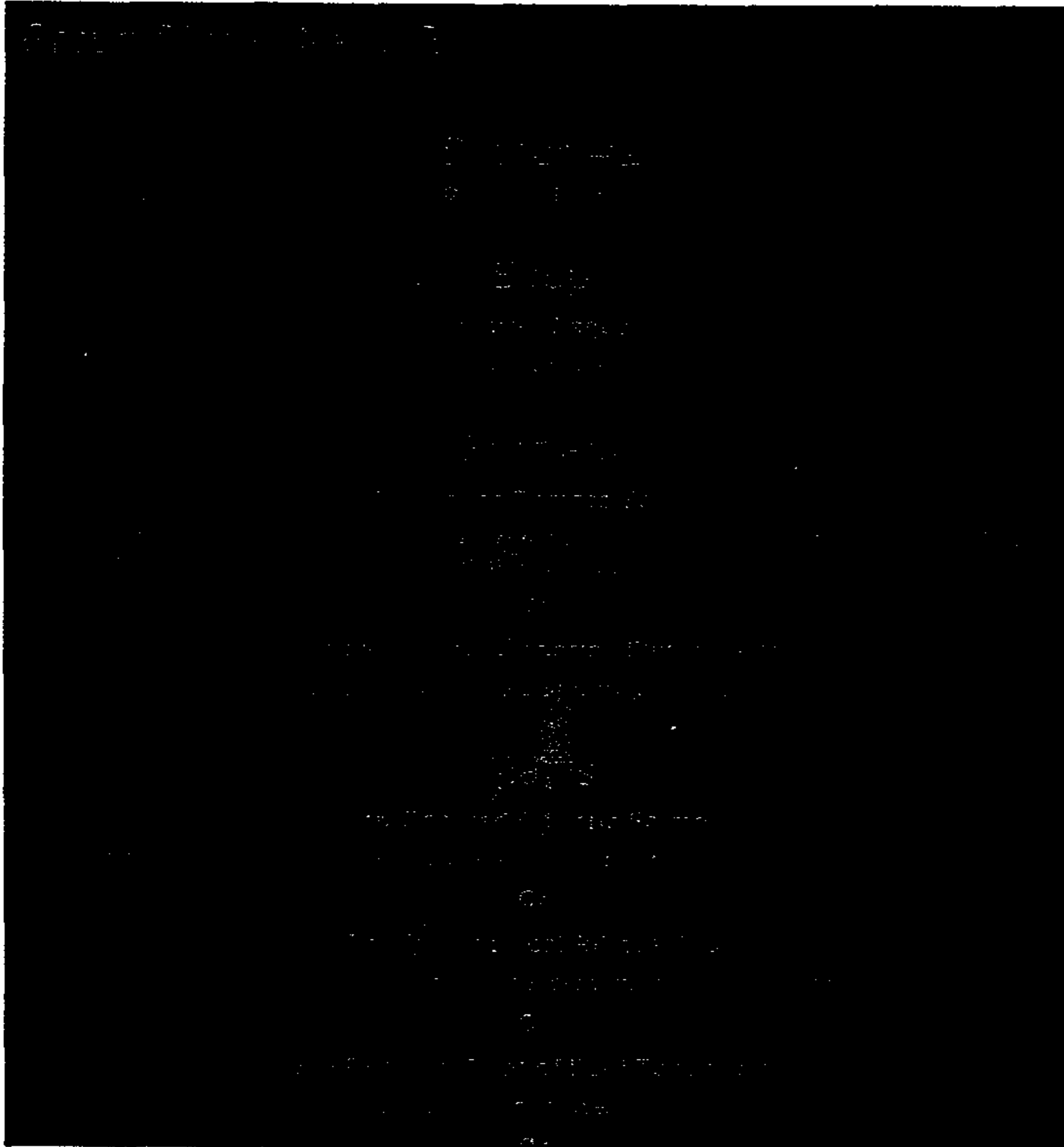
Reservation

2 Guests

Mon Dec 10

1:15 PM

Tel: 613-241-1343
Sign up for our eBulletin





47 Clarence In the Market

- Home
- Reservations
- Menus
- Announcements
- Contact
- Gift Certificate
- Holiday Bookings & NY Eve
- Private Planning & Group Events
- Weddings
- Showcase

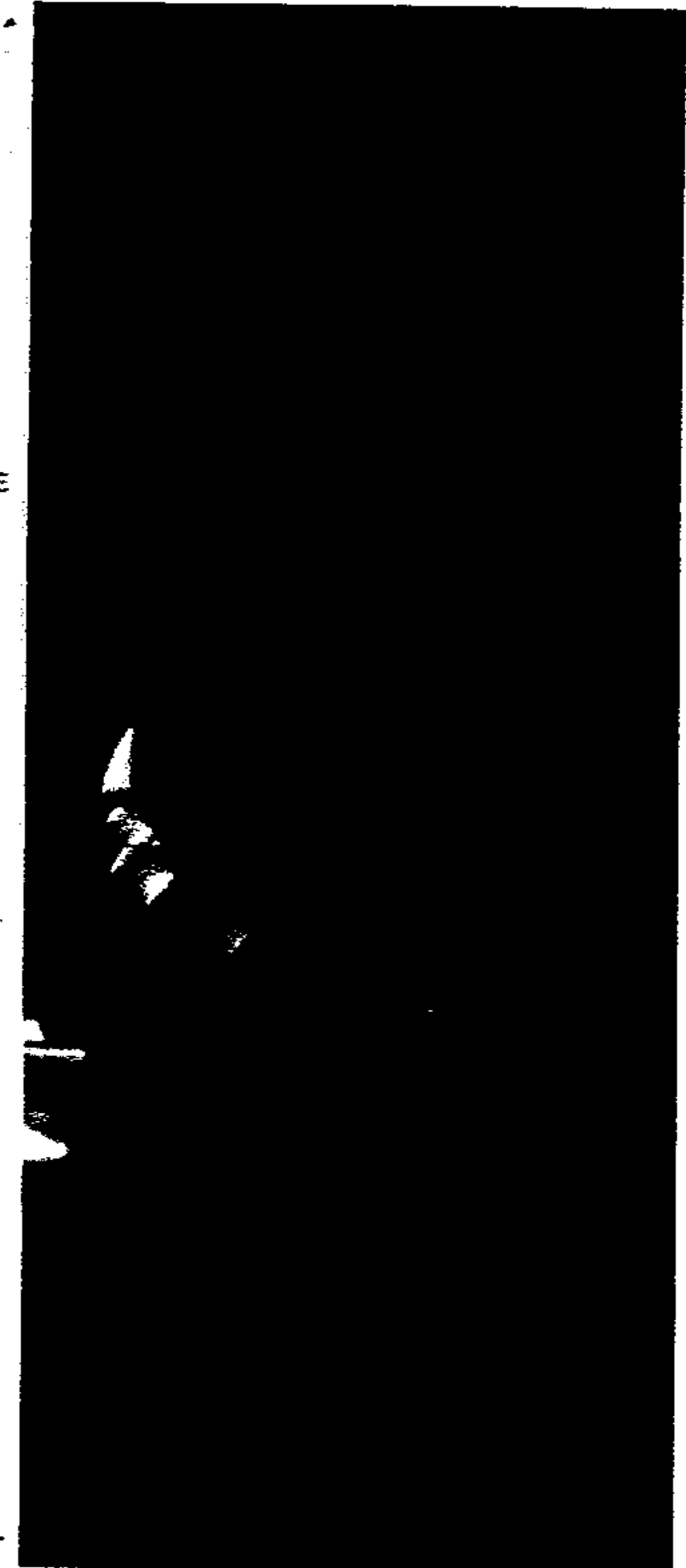
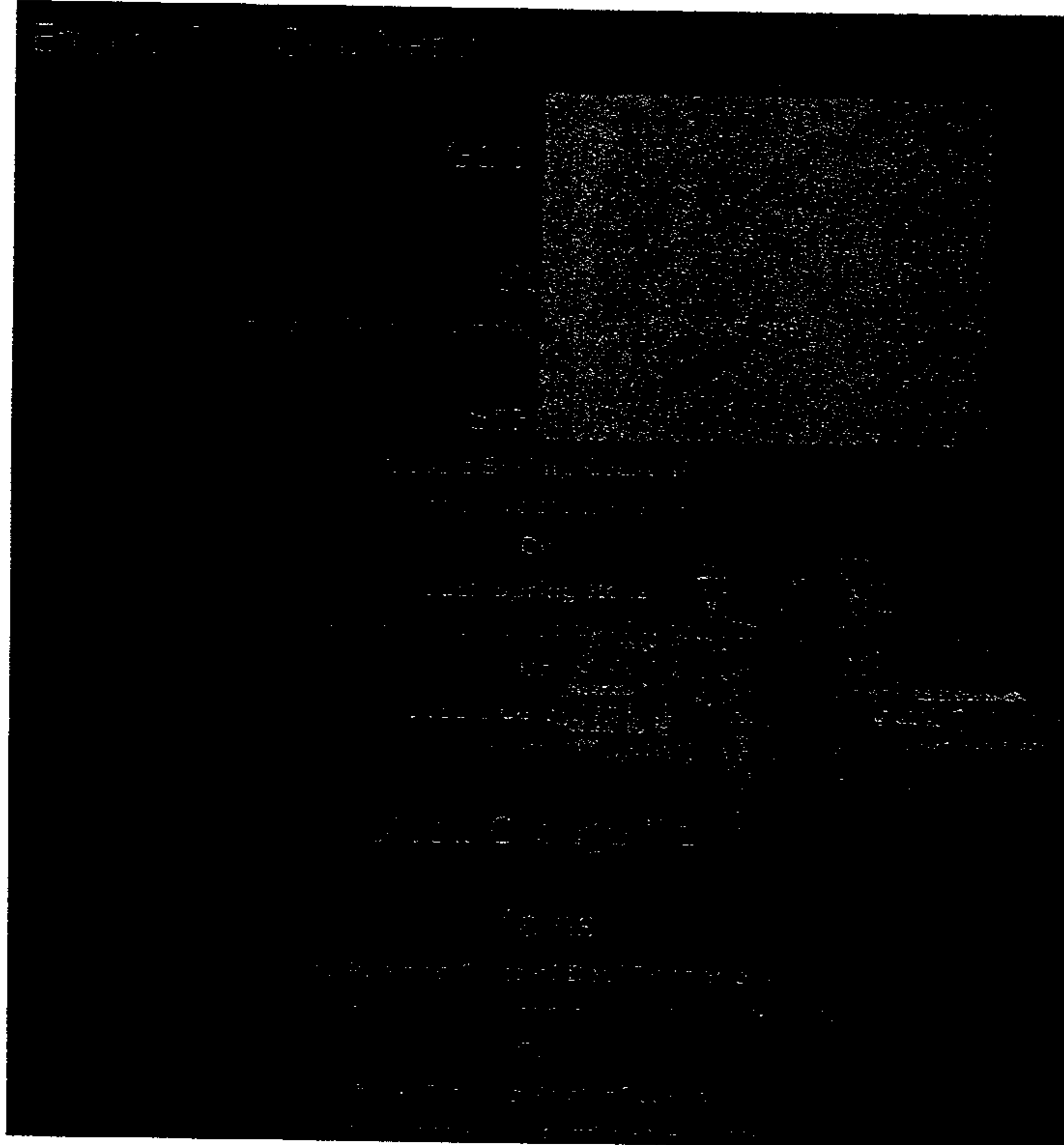
Reservation

2 Guests

Mon Dec 10

1:15 PM

Tel: 613-241-1343
Sign up for our eBulletin



Canapés

Our canapés are freshly prepared in-house and beautifully presented on silver trays.

Poultry & Game Selections

Roasted tandoori chicken brochettes with cilantro yogurt
Ishmael's blackened chicken with wilted spinach & Brie crostini
Smoked duck, arugula, tomato preserves with Asiago toasts
Moroccan chicken Phyllo

\$30 per dozen

Meat Selections

Spicy chorizo empanada with onion marmalade
Jamaican jerk beef skewers
Mini beef Wellingtons with veal jus
Lamb popsicles with minted jalapeño pesto (please add \$6 per dozen)
Mini beef burgers with chipotle aioli, sharp cheddar
Grilled beef topped with Stilton
Shepherds pie with truffle potato whip spoons
Mini Asiago, genoa salami pizzas

\$30 per dozen

Seafood Selection

Crispy phyllo shrimp skewers with wasabi aioli
Smoke salmon with lemon, dill cream cheese
Lobster carrot phyllo rolls with saffron aioli
Mini crab cakes with sweet chili gastrique

\$32 per dozen

Prices do not include taxes or gratuities. Prices and items are subject to change.

Sushi Selections

Minimum order 5 dozen

Cucumber maki *\$25 per dozen*

California rolls *\$32 per dozen*

Assorted sushi to include salmon, tuna, shrimp *\$36 per dozen*

Vegetarian Selections

Mini Asiago pizzas

Portobello & leek crescents
Parmesan breaded artichokes with ancho chili marinara sauce
Vegetable spring rolls with lime ponzu dipping sauce
\$25 per dozen

Selection of Fine Canadian Cheeses

Cars water crackers, baguette, spiced nuts and preserves
\$8 per guest

Selection of Fine Canadian & European Cheeses

Cars water crackers, baguette, spiced nuts and preserves
\$12 per guest

Assorted Crudités Basket

3 dipping sauces
\$5 per guest

Prices do not include taxes or gratuities. Prices and items are subject to change.

EMPIRE GRILL

s t e a k s ★ w i n e s ★ m a r t i n i s

Wine Selection

White

| | |
|---|----|
| Unoaked Chardonnay, Vineland, Niagara, Ontario, Canada | 35 |
| Sauvignon Blanc, Vineland, Niagara, Ontario, Canada | 45 |
| Chardonnay, "Elevation", Vineland, Niagara, Ontario, Canada | 55 |

Red

| | |
|---|----|
| Cabernet Franc, Vineland, Niagara, Ontario, Canada | 35 |
| Cabernet/Merlot, Vineland, Niagara, Ontario, Canada | 45 |
| Cabernet, "Elevation", Vineland, Niagara, Ontario, Canada | 55 |

Sparkling

| | |
|--|-----|
| 2008 Sauvignon Blanc, 'Archangel', Angels Gate, Niagara, Ontario, Canada | 50 |
| NV Cuvee Catharine Brut, Henry of Pelham, Niagara Peninsula, Ontario, Canada | 60 |
| 2009 Chardonnay, 'The Pup', Dogridge, McLaren Vale, Australia | 60 |
| 2006 Huff Estates, Prince Edward County, Ontario, Canada | 75 |
| NV Ice Cuvee Rose, Peller Estates, Niagara, Ontario, Canada | 88 |
| NV Veuve Clicquot, Champagne, France | 115 |
| NV Laurent Perrier Rose, Champagne, France | 150 |
| 1998 Noble Cuvee, Lanson, Champagne, France | 220 |
| 2000 Dom Perignon, Moet & Chandon, Champagne, France | 398 |

Prices do not include taxes or gratuities. Prices and items are subject to change.

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.

| | | | | | | |
|-------------------------------------|---|---|---|--|---|---|
| <input checked="" type="checkbox"/> | Questions Hospitality - Cyber Security Conference, Luncheon and Dinner January 29-30 2012 | | | | | |
| <input checked="" type="checkbox"/> | Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments? | | | | | |
| <input checked="" type="checkbox"/> | Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)? | | | | | |
| | <input type="checkbox"/> Travel Authority and Advance Form (TAA) | <input type="checkbox"/> Advanced Authorization to Extend Hospitality Form (AAEH) | <input type="checkbox"/> Request to Attend Conferences Form | <input type="checkbox"/> Training Application and Authorization Form | <input type="checkbox"/> Membership Approval Form | <input checked="" type="checkbox"/> Other Specify: Quote |
| <input checked="" type="checkbox"/> | Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)? | | | | | |
| <input checked="" type="checkbox"/> | 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? | | | | | |
| | <input checked="" type="checkbox"/> Is the Sole Source Checklist complete and attached? | | | | | |
| | <input type="checkbox"/> 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? | | | | | |
| | <input checked="" type="checkbox"/> 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). | | | | | |
| | <input checked="" type="checkbox"/> 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. | | | | | |
| | <input checked="" type="checkbox"/> Does the cost exceed \$10k, have a useful life of more than 1 year and does Public Safety control / own the item? | | | | | |
| | <input checked="" type="checkbox"/> Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? | | | | | |
| | <i>*Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.</i> | | | | | |

| Purchase Requisition # | Purchase Order # | Funds Commitment #: | RDIMS # |
|------------------------|------------------|---------------------|---------|
| | | 50097787 Line 4 | |

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/dfsaf/dfsaf-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/dfsaf/dfsaf-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.



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.

| | | | |
|-------------------------------------|---|---|---|
| <input checked="" type="checkbox"/> | Questions | Translation [REDACTED] | Jan 29-30 2013 |
| <input checked="" type="checkbox"/> | Is there evidence of Expenditure Initiation approval by a Delegated Official in accordance with the Public Safety DFSA Instruments? | | |
| <input checked="" type="checkbox"/> | Do I have the required forms signed and attached to this request for Commitment Authority (S32 FAA)? | | |
| | <input type="checkbox"/> Travel Authority and Advance Form (TAA) | <input type="checkbox"/> Advanced Authorization to Extend Hospitality Form (AAEH) | <input type="checkbox"/> Request to Attend Conferences Form |
| | | <input type="checkbox"/> Training Application and Authorization Form | <input type="checkbox"/> Membership Approval Form |
| | <input checked="" type="checkbox"/> Other | | Specify: Quote |
| <input checked="" type="checkbox"/> | Do I have authority, as per my FASSR, to approve Commitment Authority (S32 FAA)? | | |
| <input checked="" type="checkbox"/> | 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? | | |
| | <input checked="" type="checkbox"/> Is the Sole Source Checklist complete and attached? | | |
| | <input type="checkbox"/> 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? | | |
| | <input checked="" type="checkbox"/> 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). | | |
| | <input checked="" type="checkbox"/> 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. | | |
| | <input checked="" type="checkbox"/> Does the cost exceed \$10k, have a useful life of more than 1 year and does Public Safety control / own the item? | | |
| | <input checked="" type="checkbox"/> Is this expense a betterment of a capital asset? Does this expenditure extend the useful life of the asset being repaired / renovated? | | |
| | <i>*Betterments are repairs/renovations expenditures relating to the alteration or modernization of an asset that prolong the item's period of usefulness.</i> | | |

| Purchase Requisition # | Purchase Order # | Funds Commitment #: | RDIMS # |
|------------------------|------------------|---------------------|---------|
| | | 500073527 Line 5 | 739681 |

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.



ADVANCED AUTHORIZATION TO EXTEND HOSPITALITY DEMANDE D'AUTORISATION POUR OFFRIR UNE RÉCEPTION OFFICIELLE

NOTE: To be used by employees to whom authority has not been delegated but who may be required to extend hospitality in **exceptional circumstances**.

REMARQUE: Doit être remplie par les employés à qui l'autorisation n'a pas été déléguée mais qui peuvent être appelés à offrir des réceptions officielles dans **des circonstances exceptionnelles**.

| Employee's Name - <i>Nom de l'employé</i> | | Branch - <i>Direction</i> | | |
|---|--|--|-------|---|
| François Guimont | | Public Safety Canada | | |
| Type of Function - <i>Nature de l'événement</i> | | Place of Function - <i>Lieu de l'événement</i> | | |
| Working Lunch of Senior Officials | | A9- Lester B. Pearson Building (DFAIT) | | |
| Function Date <i>Date de l'événement</i> | Number In Attendance - <i>Nombre de participants</i> | | | Total Estimated Cost <i>Coût total prévu</i> |
| | Gov't of Canada - <i>Gouv. du Canada</i> | Other - <i>Autres</i> | Total | |
| January 29, 201 | 5 | 5 | 10 | \$326.34 |

Purpose of Hospitality - *Objet de la dépense*

The purpose is to provide hospitality for a luncheon of 10 senior officials to be hosted by Deputy Minister Guimont. The purpose of the luncheon is to discuss national security issues. The proposed luncheon will be held on January 29, 2013 at the Department of Foreign Affairs and International Trade. Hospitality will include a table d'hôte menu to be decided by the chef as well as wine.

In addition to the hospitality, we would request authorization to provide flowers at an additional cost of \$90 + hst of \$11.70.

All costs are within maximum rate per person.

I hereby request authorization to extend hospitality as stated above, in accordance with Treasury Board Policy and Guidelines on Hospitality.

Je demande par la présente l'autorisation d'offrir la réception officielle susmentionnée, conformément aux politiques et lignes directrices concernant les réceptions officielles publiées par le Conseil du Trésor.

Employee's - Signature - de l'employé

Date

Authorizing Officer's - Signature - de l'agent responsable

Date



ADVANCED AUTHORIZATION TO EXTEND HOSPITALITY DEMANDE D'AUTORISATION POUR OFFRIR UNE RÉCEPTION OFFICIELLE

NOTE: To be used by employees to whom authority has not been delegated but who may be required to extend hospitality in **exceptional circumstances**.

REMARQUE: Doit être remplie par les employés à qui l'autorisation n'a pas été déléguée, mais qui peuvent être appelés à offrir des réceptions officielles dans **des circonstances exceptionnelles**.

| Employee's Name - <i>Nom de l'employé</i> | | Branch - <i>Direction</i> | | |
|---|--|--|-------|---|
| Robert Dick | | NCSD, National Security Branch | | |
| Type of Function - <i>Nature de l'événement</i> | | Place of Function - <i>Lieu de l'événement</i> | | |
| Health Breaks (3) Breakfast, Lunch (2) and Dinner | | 125 Sussex Drive, Ottawa, ON | | |
| Function Date <i>Date de l'événement</i> | Number In Attendance - <i>Nombre de participants</i> | | | Total Estimated Cost <i>Coût total prévu</i> |
| | Gov't of Canada - <i>Gouv. du Canada</i> | Other - <i>Autres</i> | Total | |
| January 29-30, 2013 | 15 | 30 | 55 | \$6,834.55 |

Purpose of Hospitality - *Objet de la dépense*

[Redacted content]

The present Dialogue will take place over a two-day period and will provide an opportunity for the Government of Canada to engage with [Redacted] counterparts on several cyber related issues of mutual interest.

This hospitality request includes two breakfasts, three health breaks, two lunches and a dinner/reception on the evening of January 29, 2013 at which time liquor will be served.

Note: a separate hospitality request has been prepared for a luncheon that will be hosted by the Deputy Minister.

I hereby request authorization to extend hospitality as stated above, in accordance with Treasury Board Policy and Guidelines on Hospitality.

Je demande par la présente l'autorisation d'offrir la réception officielle susmentionnée, conformément aux politiques et lignes directrices concernant les réceptions officielles publiées par le Conseil du Trésor.

Employee's - Signature - de l'employé

Date

Authorizing Officer's - Signature - de l'agent responsable

Date

Page 140
is a duplicate
est un duplicata

Page 141
is a duplicate
est un duplicata

**Pages 142 to / à 143
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**



Public Safety Sécurité publique
Canada Canada

Senior Assistant Sous-ministre
Deputy Minister adjoint(e) principal(e)

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: **JAN 08 2013**

File No.: 391834

RDIMS No.: 732067

MEMORANDUM FOR THE MINISTER

**INTERNATIONAL TRAVEL AUTHORITY FOR ROBERT PITCHER AND
WINDY ANDERSON TO TRAVEL TO THE HAGUE, THE NETHERLANDS,
JANUARY 21-25, 2013, TO ATTEND
THE NATIONAL CYBER SECURITY CENTRUM, AND
MEETING OF THE INTERNATIONAL WATCH AND WARNING NETWORK**

(Decision sought)

ISSUE

Windy Anderson, Director of the Canadian Cyber Incident Response Centre (CCIRC) and Robert Pitcher, Senior Analyst, Partnerships and Engagements, National Cyber Security Directorate (NCSD), are requesting international travel authority to attend the International Watch and Warning Network (IWWN) planning meeting for the upcoming Cyber Storm 4 exercise and the National Cyber Security Centrum conference in The Hague, Netherlands, January 22-24, 2013.

BACKGROUND

The IWWN is a network of Computer Emergency Readiness Teams (CERTs) established by the United States (U.S.) in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities. Canada was a founding member, and other participating countries include Australia, Hungary, Norway, Italy, Sweden, Finland, Japan, Switzerland, France, the Netherlands, United Kingdom, Germany and New Zealand.

Apart from its role in coordinating the efforts of various national CERTs and government agencies in addressing cyber threats and vulnerabilities, the IWWN would serve as a focal point for international collaboration during a major cyber event. As such, the IWWN undertakes planning and coordination in the lead-up to, and during, the U.S. led bi-annual cyber exercise, Cyber Storm.

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 Training Application and Authorization form (**TAB B**) and the International Travel Request form are also attached for your information (**TAB C**).

Should you require any additional information, please do not hesitate to contact me or Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.


François Guimont

Enclosures: (3)

I approve:

I do not approve:

Vic Toews, P.C., Q.C., M.P.

Vic Toews, P.C., Q.C., M.P.

Prepared by: Robert Pitcher



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

U bevindt zich op: [Home](#) [Conference](#) > Programme

Conference Programme

The NCSC Conference 2013 is all about cyber security

We have a promising line-up of speakers, including names such as **Richard Stiennon**, a thought-provoking speaker on topics like cyber warfare and exploit trading, **Raj Goel** on the effect of Social Media in our daily lives, and **Jacob Appelbaum** and **Roger Dingledine** from the Tor project on privacy.

This year's conference is hosted by BBC presenter Nicholas Witchell.

Overview

The conference is an international two-day conference, consisting of both plenary sessions and parallel tracks. There will be technical subjects, such as malware, monitoring, etc, but also less technical subjects about organizational aspects of security and privacy.

On the evening of the first day, there is a social event where you will have time to network.

In the coming weeks the programme will be completed, updates will be posted frequently.

Timetable

Tuesday 22 January (times are tentative)

- 08.30 registration desk open
- 09.00 opening and plenary session
- 11.15 parallel tracks (4 different subjects)
- 12.45 networking break including lunch
- 13.45 parallel tracks (4 different subjects)
- 16.00 plenary session
- 17.00 closing
- 18.00 - 22.00 Social Event and dinner

Wednesday 23 January (times are tentative)

- 08.30 registration desk open
- 09.00 opening and plenary session
- 11.00 parallel tracks (4 different subjects)
- 12.45 networking break including lunch



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

U bevindt zich op: [Home](#) > [Conference](#) > [Registration](#)

Registration NCSC Conference 2013

Registration is open for the NCSC Conference 2013. To register please complete the registration form.

Registration fee & admittance

As many of you will know, [registration \(https://www.ncsc.nl/conference/conference-2013/registration/form.html\)](https://www.ncsc.nl/conference/conference-2013/registration/form.html) and entrance to the NCSC Conference is free of charge. It will take a number of days to process your registration. You will receive an email confirmation once your registration has been accepted. We have the right to limit the number of registrations that we accept per organisation.

Please note: Participation will require a valid ID, to be presented when picking up your badge on-site.

Privacy

We will only use the information that you provide us with on this form to facilitate your registration, communicate with you and provide you with conference material right after the event. We will never disclose your personal information to any third party unless required by law. Please respect your privacy and review our full [privacy statement \(/english/privacy-statement\)](/english/privacy-statement).

Should you have any concerns about registering online, please contact us by phone on +31-70-8887555 so that we may process your registration manually.

Original / Prem. demande

Amended (Same levels of approval as original dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

Department - Ministère
Public Safety Canada

Address - Adresse
340 Laurier Ave W.

Branch Contact - Personne ressource à la direction
Jane Hayward

Purpose of travel - Objet du voyage
Attend Conference and Plan IWWN exercise

14A Travel Authority No. (TAN) / N° d'aut de voyager (NAV)
LNW9

Type 2 Name of traveller - Nom du voyageur
Robert Pitcher

Document No. RDIMS - N° du document SGGDI
740494

Classification
CS-03

Branch / Division / Group - Direction / Division / Groupe
NS-NCSD- Canadian Cyber Institute Response Centre

Telephone No. - No. de téléphone
613-990-7050

Telephone No. - No. de téléphone
613-991-1982

No. of days / Nbre de jours
7

Do you have a Gov't 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, 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 - Arrival Départ - Arrivée | Transportation Transport | | No. of meals prepaid Nbre de repas prépayés | Accommodation Hébergement | File locator number N° de repérage du dossier |
|----------------|-----------------|-----------------|---|--------------------------|----------|--|---------------------------|--|
| | | | | Mode | Class | | | |
| 19-Jan-13 | Ottawa (YOW) | Amsterdam (AMS) | 14:19 - 08:05 (+1 day) | Air | Business | 1 + snack | | |
| 19-Jan-13 | Amsterdam (AMS) | The Hague | 11:47 - 12:17 | Rail | Business | | Novotel | |
| 24-Jan-13 | The Hague | Amsterdam (AMS) | 18:00 - 18:30 | Rail | Business | | Radisson Blu Airport | |
| 25-Jan-13 | Amsterdam (AMS) | Ottawa (YOW) | 08:55 - 16:15 | Air | Business | 1 | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel |
|--|----------------------------------|---|----------------------------------|--|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif | |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$644.52 | Accommodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | Total travel time exceeds 9 hours. Part D - Partie D Estimated Cost - Coût estimatif Prepaid - Prépayé \$6,868.26 Other - Autre \$1,858.40 Trip Total - Coût total du voyage \$8,726.66 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 |
| 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) | \$0.00 | |
| Private vehicle requested by: Voiture particulière demandée par: <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$28.60 | Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | \$0.00 | |
| Transportation Transport | \$250.00 | <input checked="" type="checkbox"/> 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 | | |
| Meals and incidentals Repas et frais accessoires | \$735.28 | | | |
| Other (Specify) - Autre (préciser) | \$200.00 | | | |
| Breakfast | | Approval - Approbation | | |


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 Pitcher  Dec 19/2012

Signature Date

Recommended by (signature) - Recommandé par (signature) Date Approved by (signature) - Approuvé par (signature) Date

 Dec 21/12

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

Sub-type / Sous-type Vendor Code / Code du fourm. Departmental Ref. No. / No. de réf. Du ministère Coding - Cidification Amount - Montant

NCS D THC T15 493-PSABASE - 2001 - 500102427

Description Financial encumbrance No. / No. de consignation de fonds

Department pre-audit and account verification (signature) / Agent min. chargé de la vér. Préalable des comptes (signature) Requestion 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 responsable (TPSGC) (signature) Signature

WORKSHEET - FEUILLE DE TRAVAIL

| Estimated Cost - Coût estimatif: Prepaid - Prépayé | | | | Amount/Montant |
|--|----------------------------|--------------|------------|-----------------|
| Airfare / Frais d'avion | | | | \$6,800.00 |
| Train / Train | | | | \$68.26 |
| Other / Autres | | | | \$0.00 |
| | | | | \$6,868.26 |
| Estimated Cost - Coût estimatif: Other - Autre | | | | Amount/Montant |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du r | | \$161.13 | 4 | \$644.52 |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du r | | \$250.41 | 1 | \$250.41 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du réper | | | | \$0.00 |
| | | | | \$894.93 |
| 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 | 52.0 | \$28.60 |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Parking & Tolls / stationnement et frais de péage | | | \$0.00 | \$0.00 |
| Taxi/Limo | Home to Airport | | \$0.00 | \$250.00 |
| | Airport - Hotel / Meetings | | \$50.00 | |
| | Hotel - Airport | | \$50.00 | |
| | Airport to Home | | \$0.00 | |
| | Meeting - Meetings | | \$150.00 | |
| Transportation / Transportation (No receipt) | | \$10.00 | | \$0.00 |
| Ferry & Miscellaneous | | | \$0.00 | \$0.00 |
| | | | | \$250.00 |
| Canadian | | | | Amount/Montant |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Breakfast / Petits déjeuners | | \$15.50 | | \$0.00 |
| Lunch / Déjeuners | | \$15.00 | | \$0.00 |
| Dinner / Diners | | \$41.30 | | \$0.00 |
| Incidentals /Frais divers | | \$17.30 | 1 | \$17.30 |
| Total Canadian | | | | \$17.30 |
| Amsterdam | | | | Amount/Montant |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Breakfast / Petits déjeuners | | | 2 | \$0.00 |
| Lunch / Déjeuners | | \$41.32 | | \$0.00 |
| Dinner / Diners | | \$0.00 | 1 | \$0.00 |
| Incidentals /Frais divers | | \$42.29 | 2 | \$84.58 |
| Total Amsterdam | | | | \$84.58 |
| The Hague | | | | Amount/Montant |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Breakfast / Petits déjeuners | | | 4 | \$0.00 |
| Lunch / Déjeuners | | \$41.32 | 5 | \$206.60 |
| Dinner / Diners | | \$64.41 | 4 | \$257.64 |
| Incidentals /Frais divers | | \$42.29 | 4 | \$169.16 |
| Total The Hague | | | | \$633.40 |
| GRAND TOTAL | | | | \$735.28 |
| 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 - Breakfasts | | | | \$200.00 |
| | | | | \$200.00 |

**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 Pitcher | | Given name and initials - Prénom et initiales Robert | | | |
| 4. PRI - CIDP | 5. Sex - Sexe <input checked="" type="checkbox"/> Male Homme <input type="checkbox"/> Female Femme | 6. Classification Gr. S-gr. Lev.Niv. CS 8 3 | | 7. First official language - Première langue officielle <input checked="" type="checkbox"/> (1) English Anglais <input type="checkbox"/> (2) French Français | |
| 8. Position title - Titre du poste Engagement and Partnerships- Analyst | | | | | |
| 9. Employee's office telephone number - N° de téléphone de l'employé au bureau 613 990 7050 | | Facsimile - Télécopieur 613 996 0995 | | E-Mail - Courrier électronique robert.pitcher@ps-sp.gc.ca | |
| 10. Department name - Nom du ministère National Cyber Security Directorate | | 11. Dept. Code - Code min. 0880 | | 12. Branch/Division - Direction/Division | |
| 13. Office, Workstation, mailing address - Adresse postale, bureau, poste de travail 340 Laurier, Ottawa, Ontario 11th Floor | | | | City/Postal code - Ville/Code postal Ottawa K1A0W6 | |
| 14. Supervisor's name and title - Nom du surveillant et titre Sébastien Labelle | | | | Telephone No. - N° de téléphone (613) 990-2665 | |
| 15. Supervisor's Office, Workstation, mailing address - Adresse postale, bureau, poste de travail du superviseur 340 Laurier, Ottawa, Ontario, 11th floor | | | | City/Postal code - Ville/Code postal Ottawa/K1A0W6 | |
| 16. Objective of training * - Objectif de la formation * To attend open source briefings on emerging trends and threats in the field of Cyber Security. The conference also provides highly valuable networking opportunities within international Government, Industrial and Academic cyber security representatives. It would be of great benefit for Public Safety to have a presence at this conference to learn about the open source cyber security trends and innovations as well as engage with the broader international cyber security community on our current initiatives. | | | | | |
| Expenditure Initiation Approval - L'engagement des dépenses | | Date | Print Name - Imprimer Nom | Signature - (Authorized Signing Officer) / (Un dirigeant autorisé) | |
| Employee Name and Signature - Nom de l'employé et signature Dec 19 2012 Robert Pitcher | | Date | Print Name - Imprimer Nom | Employee's - Signature - Employé(e) | |

TRAINING INFORMATION - RENSEIGNEMENTS SUR LA FORMATION

| | | | | | | | | |
|--|---|--|--|----|---|---|---------------------------|--------------------------|
| 17. Course code * Code du cours * | 18. Course title - Titre du cours The National Cyber Security Centrum | | | | | | | |
| 19. Location of training * - Lieu de formation * The Hague, the Netherlands | | | 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 | 01 | 21 | 13 | 01 | 23 |
| 22. Time of training - Période retenue pour la formation <input type="checkbox"/> (1) Outside working hours En dehors des heures de travail <input checked="" type="checkbox"/> (2) During working hours Pendant les heures de travail | | | 23. Duration of training * (nearest half-day) Durée de la formation * (plus proche demi-journée) 2 d | | 24. Language of course - Langue de cours <input checked="" type="checkbox"/> English Anglais <input type="checkbox"/> French Français <input type="checkbox"/> Bilingual Bilingue <input type="checkbox"/> Other Autre | | | |
| 25. Source of training - Source de la formation <input type="checkbox"/> (1) TPB/PSC DGPF/CFP <input type="checkbox"/> (2) Dept'l Min. <input type="checkbox"/> (3) Interdept'l Intermin. <input type="checkbox"/> (4) University/College Université/Collège <input type="checkbox"/> (5) Other Autre | | | | | 26. Transit time (person-days) * Durée des déplacements (jours-personnes) 2 | | 27. Province OT | 28. Location * Lieu * |

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 * <input type="checkbox"/> 0% <input type="checkbox"/> 50% <input type="checkbox"/> 100% | | | a) * |
| Travel / Living Déplacement / Subsistance | 493-PSA045E-2001-500102427 | 8827.01 | b) |
| Other * Autres * | | | c) * |
| 30. Responsibility centre (collator) code Code du centre de responsabilité (destinataire) 493 | | TOTAL 8827.01 | d) |
| Recipient organization code Code d'organisation 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) * | | 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 |

DISTRIBUTION
 Original = PSC/Finance Division/Human Resources Division Copy = Originator
 Original = CFP/Division des finances/Division des ressources humaines Copie = Auteur



PRIVACY ACT STATEMENT

The information provided in this document is collected under the authority of the Public Service Staff Relations Act and the Public Service Employment Act. All personal information that you provide is protected under the provisions of the Privacy Act and controlled by the head of the institution where the information is stored. It will be stored in the following information banks for the purposes described:

- At Treasury Board: TBS/P-CE-719 for the purpose of managing training throughout the Public Service and TBS/P-CE-706 for Employment Equity statistical purposes.
- At the Public Service Commission: P-CE-735 for the purpose of administering courses provided by PSC Training Programs Branch.
- At departments and other agencies: P-SE-905 for the purpose of administering training and P-SE-918 for the purpose of administering Employment Equity programs in departments.

Note: Where the collection of personal information occurs verbally through a third party, e.g., in the case of a blind person, the Privacy Act Statement should be read to applicant before any personal information is collected.

TRAINING APPLICATION AND AUTHORIZATION

- Form GC 211 is to be completed when an employee is provided with formal training totalling one day or more. This is a multiple user form. Users will be the Public Service Commission, Treasury Board Secretariat and departments.
- Other training forms available are:
- Departmental Training Record, form GC 213, to be used for recording departmental bulk training. It may be used when two or more employees from the same responsibility centre are provided with formal training.
 - Longer-Term Training Documentation, form GC 212, is to be used to document longer-term training.

COMPLETION INSTRUCTIONS FOR ITEMS DESIGNATED WITH AN ASTERISK (*)

Note: Shaded areas reflect TBS requirements and must be completed.

- Fields 2* * -15, 17-20, 24, 29a-33 must be completed to ensure registration for PSC courses.

***2 Special Needs**

Enter applicable code:

- 01 Blind or Visually impaired
- 02 Deaf or Hearing impaired
- 03 Physically impaired
- 99 Other

Registration Services of the PSC Training Programs Branch will contact the departmental training coordinator to determine the special needs of individuals affected by one of the above situations.

N.B. * *: Completion of Field 2 is non-mandatory, but it is necessary to better serve applicants requiring any special assistance for training.

***4 Personal Record identifier**

Enter Social Insurance Number of employee until such time as a new federal identifier is implemented.

***16 Objective of training (For departmental use)**

To be completed jointly by the supervisor/manager and the employee.

***17 Course Code**

For PSC training Programs Branch courses, enter the code as provided in the Schedule of courses.

Departments and agencies may also make use of this field for departmental course administration.

***19 Location of Training**

For PSC Training Programs Branch courses, enter the region/city as provided in the PSC Schedule of Courses.

***21 Departmental Training Program Code**

- Enter applicable code only.

A. ANNUAL SERVICE-WIDE TRAINING GOALS

| Training Program | Code |
|-------------------------------|-------|
| Departmental operations | = 001 |
| Management/leadership | = 002 |
| Certification/licence | = 003 |

RDIMS / SGDDI # 473357

ÉNONCÉ DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les renseignements fournis dans le présent document sont recueillis en vertu de la Loi sur les relations de travail dans la Fonction publique et de la Loi sur l'emploi dans la Fonction publique. Tous les renseignements personnels fournis sont protégés en vertu de la Loi sur la protection des renseignements personnels et sont contrôlés par le chef de l'institution où les renseignements sont conservés. Ils seront stockés dans les fichiers de renseignements suivants aux fins décrites ci-dessous:

- Au Conseil du Trésor: SCT/P-CE-719 aux fins de l'administration de la formation à l'échelle de la fonction publique et SCT/P-CE-706 à des fins de statistiques portant sur l'équité en matière d'emploi.
- À la Commission de la Fonction publique: P-CE-735 aux fins de l'administration des cours dispensés par la Direction générale des programmes de formation de la CFP.
- Dans les ministères et autres organismes: P-OE-905 aux fins de l'administration de la formation à l'intérieur du ministère, et P-OE-918 afin d'administrer les programmes d'équité en matière d'emploi dans les ministères.

Note: Lorsque la collecte de renseignements personnels se fait verbalement par l'entremise d'un tiers, p.ex. dans le cas d'une personne aveugle, l'énoncé de la Loi sur la protection des renseignements personnels doit être lu au candidat avant que des renseignements personnels ne soient recueillis.

DEMANDE ET AUTORISATION DE FORMATION

- La formule GC 211 doit être remplie lorsqu'un employé(e) reçoit une formation d'une journée ou plus. Il s'agit d'une formule à usages multiples utilisée par la Commission de la Fonction publique, le Secrétariat du Conseil du Trésor et les ministères.

Les autres formules relatives à la formation sont:

- Rapport ministériel de formation. Lorsqu'ils doivent consigner de grandes quantités de données sur la formation, les ministères utilisent la formule GC 213. Celle-ci peut également servir lorsque plus d'un employé d'un centre de responsabilité reçoit une formation.
- Documentation pour la formation de plus longue durée, la formule GC 212, doit être utilisée dans le cas de la formation à long terme.

INSTRUCTIONS CONCERNANT LA FAÇON DE REMPLIR LES ÉLÉMENTS MARQUÉS D'UN ASTÉRISQUE (*)

Nota: Les cases ombrées correspondent aux exigences du SCT et doivent être remplies.

- Les zones 2* * à 15, 17 à 20, 24 et 29a à 33 doivent être remplies pour assurer l'inscription aux cours de la CFP.

***2 Besoins spéciaux**

Inscrire le code appropriée:

- 01 Personne aveugle ou handicapée visuellement
- 02 Personne sourde ou handicapée auditivement
- 03 Personne handicapée physiquement
- 99 Autre

Les services d'inscription de la Direction générale des programmes de formation de la CFP communiqueront avec le coordonnateur de la formation du ministère afin de déterminer les besoins spéciaux des candidats touchés par l'une des situations susmentionnées.

N.B. * *: Vous n'êtes pas tenu de remplir la zone 2, mais les renseignements permettent de mieux répondre aux besoins des candidats en matière d'aide spéciale à la formation.

***4 Code d'identité de Personnel**

En attendant que les nouveaux codes du gouvernement fédéral entrent en vigueur, inscrire le numéro d'assurance sociale de l'employé.

***16 Objectif de la formation (Réservé au ministère)**

Le superviseur ou gestionnaire et l'employé doivent remplir conjointement cette zone.

***17 Code du cours**

Pour les cours de la Direction générale des programmes de formation de la CFP, inscrire le code approprié figurant dans le calendrier des cours.

Les ministères et organismes peuvent également se servir de cette zone aux fins de l'administration interne des cours.

***19 Lieu de la formation**

Pour les cours de la Direction générale des programmes de formation de la CFP, inscrire la région ou la ville figurant dans le Calendrier des cours de la CFP.

***21 Code ministériel du programme de formation**

- Inscrire le code approprié seulement.

A. OBJECTIFS ANNUELS À L'ÉCHELLE DE LA FONCTION PUBLIQUE

| Programme de formation | Code |
|---------------------------------|-------|
| Opérations ministérielles | = 001 |
| Gestion/leadership | = 002 |
| Accréditation/brevet | = 003 |

International Travel Request Demande de voyage international

| | | | |
|--|---|---|--|
| Event title - Titre de l'événement Participation in the International Watch and Warning Network (IWWN) Cyber Storm 4 planning conference/Attendance at an international cyber security conference - National Cyber Security Centrum (NCSC) | | Date of event - Date de l'événement From - Du : January 20, 2013 To - Au : January 25, 2013 | |
| Location (City, Country) - Lieu (Ville, Pays) The Hague, the Netherlands | | Estimated total cost - Coût total prévu \$17,553.67 | |
| Description of meeting (provide agenda) / Description de l'événement (joindre l'ordre du jour) To finalize Canadian involvement in the upcoming Cyber Storm 4 exercise and attend a local cyber security conference (agenda is attached). | | Pre-approved under Branch travel plans? / Pré-approuvé selon les directives sur les voyages de la direction générale? <input checked="" type="checkbox"/> Yes/Oui <input type="checkbox"/> No/Non | |
| Participant(s) | | | |
| Name (s) / Nom (s) Windy Anderson Robert Pitcher | Directorate/Branch / Direction générale/Secteur NS - NCSD | Work address / Adresse au travail 257 Slater Street 340 Laurier Street | Telephone No. / N° de téléphone 613-991-7055 613-990-7050 |
| 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 IWWN is a network of Computer Emergency Readiness Teams (CERTs) established by the United States (U.S.) in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities. Canada was a founding member. Other participating countries include: Australia, Hungary, Norway, Italy, Sweden, Finland, Japan, Switzerland, France, the Netherlands, United Kingdom, Germany and New Zealand. Apart from its role in coordinating the efforts of various national CERTs and government agencies in addressing cyber threats and vulnerabilities, the IWWN would serve as a focal point for international collaboration during a major cyber event. As such, the IWWN undertakes planning and coordination in the lead-up to, and during, the U.S.-led bi-annual cyber exercise, Cyber Storm. Mr. Pitcher will act as the exercise coordinator to develop and finalize Canada's role in this exercise, and Mrs. Anderson will represent CCIRC in helping to shape national CERT participation, as well as take the opportunity to strengthen relationships with international counterparts to support operational collaboration. NCSC Ms. Anderson and Mr. Pitcher will be conference participants. | | | |
| Description of how event advances Department's priorities and expected outcomes / Comment l'événement permet-il l'avancement des priorités du Ministère et des résultats attendus One of the pillars of Canada's Cyber Security Strategy is to develop and improve cross border relations. As Cyber Storm 4 is led by the U.S. Department of Homeland Security, and composed of an international collection of allied nations, continuing participation is therefore important not only to Canada's cyber security posture, but also to signaling our commitment to international collaboration on this issue, as agreed among the Ottawa-5 members, and in support of the Department's International Strategic Framework. Cyber Storm 4 will not only exercise our ability to coordinate with international partners on an international cyber based event, it will also offer the ability to further develop our domestic skills through the exercising of existing staff to respond to a large international event. In addition to the exercise, the Netherlands is hosting its annual cyber security conference the same week. It is therefore recommended that the duration of this visit be extended two additional days so as to allow for attendance in this event on a cost-effective basis. Attendance will provide valuable training and insight into current and ongoing cyber security trends, and at the same time reinforce Canada's and CCIRC's activities in a highly respected international cyber security venue. | | | |
| Other Department, Portfolio or Government representatives attending event / Autres représentants du Ministère, du Portefeuille ou du gouvernement qui participeront à l'événement | | | |

Cyber Security Incident Response teams from the U.S., France, the Netherlands, Switzerland, Japan, Australia, Germany, and Finland.


Prior Consultation within and outside Department
Consultations préalables intra- et inter-ministérielles

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 participant's Director General
Nom du Directeur Générale du voyageur


Date

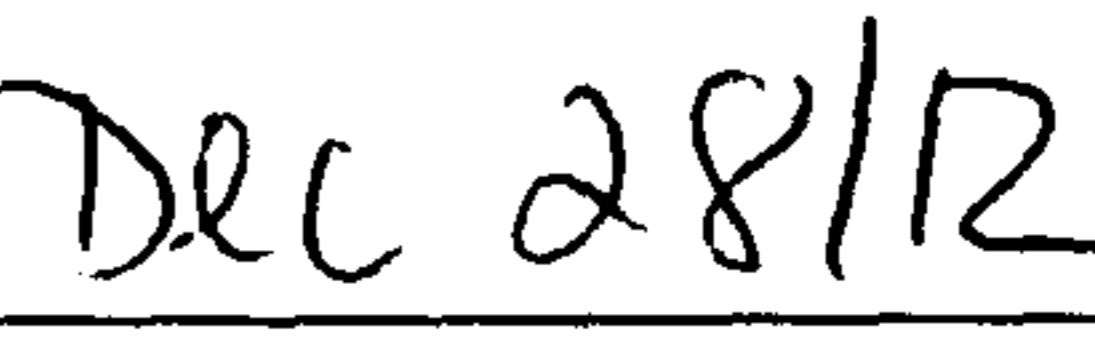
Reviewed by/
Examiné par :


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 Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: ~~FEB~~ **FEB 19 2013**

File No.: 392235
RDIMS No.: 730797

MEMORANDUM FOR THE MINISTER

**VANCOUVER INDUSTRIAL CONTROL
SYSTEMS SECURITY WORKSHOP**

(Signature required)

ISSUE

We are requesting your approval to host an Industrial Control Systems Security Workshop to be held in Vancouver on March 26-27, 2013. The estimated cost to Public Safety Canada (PS) for this event will not exceed \$45,000 for 120 participants.

BACKGROUND

The National Cyber Security Directorate (NCSD) and the Critical Infrastructure and Strategic Coordination Directorate (CID) are preparing the second of two workshops on Industrial Control Systems Security planned for this fiscal year. A copy of the draft agenda for this workshop is attached (**TAB A**). Considerable interest and positive feedback from stakeholders have been received further to the workshop held in Toronto, Ontario, in November 2012. In total, PS and the Royal Canadian Mounted Police (RCMP) have partnered to host workshops across the country on eight separate occasions. The cumulative participation at the workshops to date is over 750 attendees.

These training and community building opportunities are 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, with representation from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation.

.../2

The workshop series is a valuable tool in meeting several of PS' outcomes including enabling PS and DHS to provide joint cyber information sessions to critical infrastructure partners. The sessions also serve to increase awareness of the Canadian Cyber Incident Response Center (CCIRC) and its services, and therefore to expand information sharing, notably in the area of industrial control systems security.

CURRENT STATUS

PS regional offices, the RCMP, the Canadian Security Intelligence Service, and provinces and territories are engaged in preparing for and publicizing the Vancouver workshop. PS Communications have been made aware of the event.

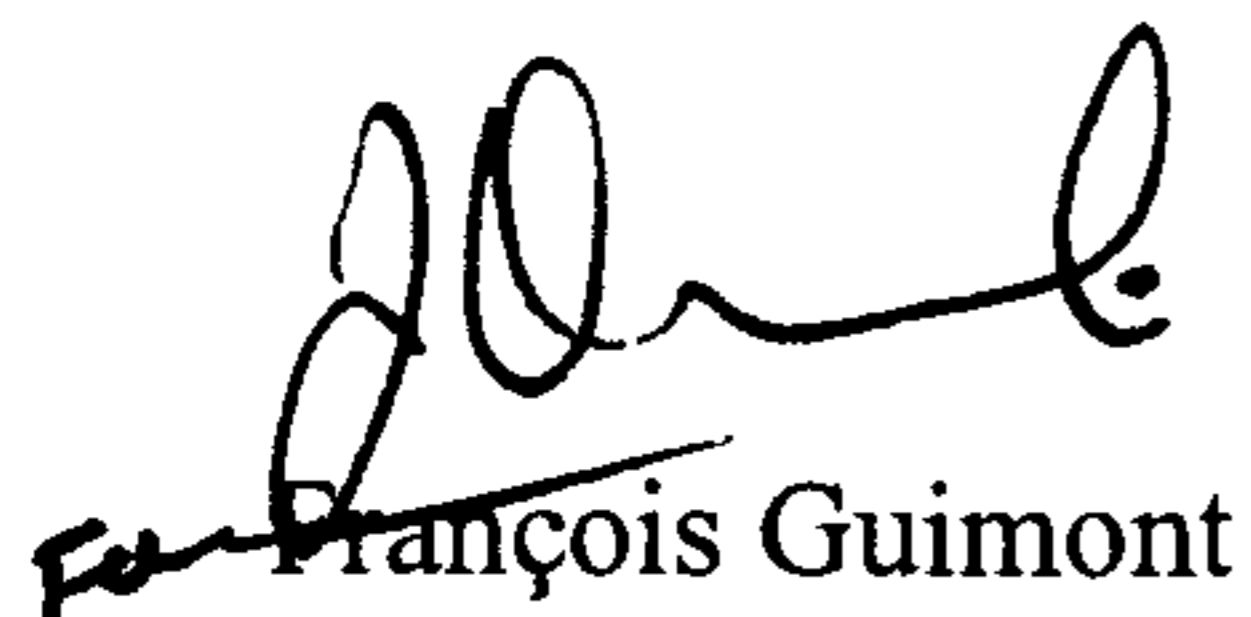
We are estimating the total event costs for PS will not exceed \$45,000 (including HST and gratuities) and are seeking approval of that amount. The proposed event costs fall within the Treasury Board *Directive on the Management of Expenditures on Travel, Hospitality and Conferences*. All costs related to this request fall within the National Security Branch's Travel, Hospitality and Conference Cap and no financial commitments will be made until the event has been approved:

- The workshop will take place at the Hyatt Regency Vancouver which was the least expensive option. The room rental rate is \$4,625.60 and the estimated hospitality cost with taxes and gratuities is \$2,801.79 (**TAB B**). Refreshments (tea and coffee) will be served over four breaks throughout the two-day workshop. The hospitality costs do not exceed the Treasury Board Standard Cost per Person as outlined in the Treasury Board *Directive on the Management of Expenditures on Travel, Hospitality and Conferences*. No alcohol will be served at this event.
- AVW TelAv will be providing the audio visual equipment for the event at an estimated cost of \$5,488.90.
- The total travel cost for presenters at the event is estimated to be \$19,051.70, which will be paid by PS. The official request for presenters will be made pending approval of this request. The agenda and estimate are based on previous workshops and speakers that have expressed interest in returning to future events. Final speakers' and travel costs may change slightly once approval is received and as presenters are contacted to finalize their arrangements.
- Travel costs for the National Security Branch are estimated to be \$9,132.97. Travel authorizations for Tom Campbell (NCSO, EC-07), Ashley Bencke (NCSO, AS-01), Frank Turbide (NCSO – CCIRC, CS-03), and Ryan Hunt (CID, PM-06) are enclosed (**TAB C**).
- It is anticipated that the RCMP and Natural Resources Canada will be incurring travel expenses (estimated to be \$2,500 each) to have employees (Dave Black, RCMP and Dr. Felix Kwamena, NRC) present at the workshop. This will bring the total estimated event cost for the Government of Canada to \$50,000.

RECOMMENDATION

It is recommended that you approve the estimated cost of up to \$45,000 for the workshop by signing below.

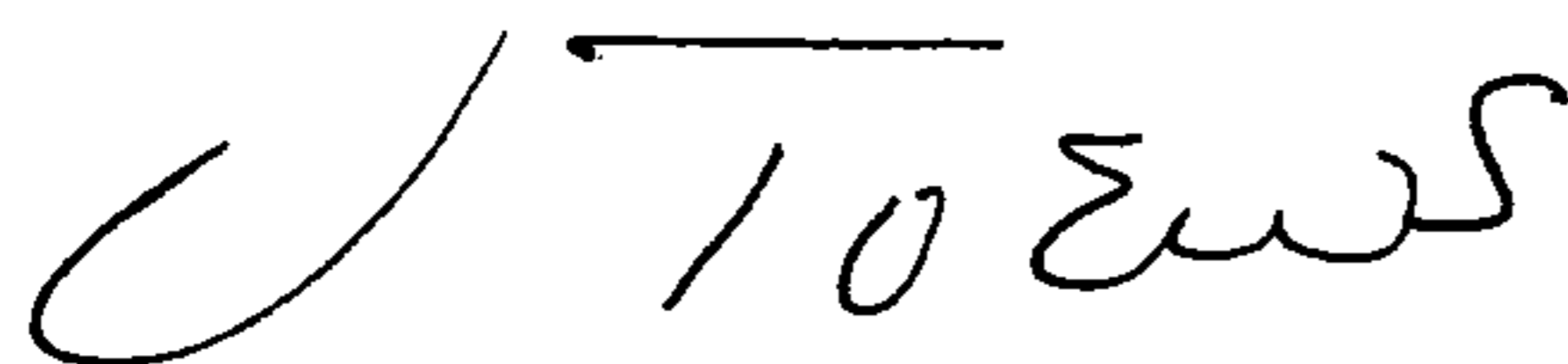
Should you require additional information, please do not hesitate to contact me or Ms. Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.


François Guimont

Enclosures: (3)

I approve:

I do not approve: FEB 27 2013



Vic Toews, P.C., Q.C., M.P.

Prepared by: Ashley Bencke



Public Safety
Canada

Sécurité publique
Canada



**2013 Control Systems Security Workshop
HYATT Regency, Vancouver, British Columbia
655 Burrard Street
DRAFT Agenda
Tuesday March 26, 2013**

- | | |
|---------------|---|
| 08:00 - 08:30 | Registration (identification required) |
| 08:30 - 08:45 | Welcome and Opening Remarks TBD |
| 08:45 - 09:15 | State of Control Systems Cyber Security Mike Chaney, Department of Homeland Security |
| 09:15 - 9:45 | Cybercrime Threat in Control Systems Lee Shields, Royal Canadian Mounted Police |
| 9:45- 10:30 | Networking break |
| 10:30 - 11:15 | Current Threats and Trends Joel Langill, SCADAhacker |
| 11:15 - 12:00 | Smart Grid and Advanced Metering Infrastructure Security Research Activities Mark Fabro, Lofty Perch |
| 12:00 - 13:00 | Lunch break |
| 13:00 - 13:45 | Hack Session Joel Langill, SCADAhacker |
| 13:45 - 14:30 | Cyber Security Evaluation Tool and Control Systems Cyber Security Training Opportunities Mike Chaney, Department of Homeland Security |
| 14:30 - 15:00 | Networking break |
| 15:00 - 15:45 | National Energy Infrastructure Test Centre Dr. Felix Kwamena, Natural Resources Canada |
| | Cyber Security Partnership Program Tom Campbell, Public Safety Canada |
| 15:45 - 16:00 | Closing remarks |



Public Safety
Canada

Sécurité publique
Canada



**2013 Control Systems Security Workshop
HYATT Regency, Vancouver, British Columbia
655 Burrard Street
DRAFT Agenda
Wednesday, March 27, 2013**

- | | |
|---------------|--|
| 08:00 – 08:30 | Registration (identification required) |
| 08:30 – 09:15 | SHODAN search engine Bob Radvanovsky, Infracritical |
| 09:15 – 10:00 | Analysis first! A Model for Actionable Critical Infrastructure Cyber Intelligence Sean McBride, Critical Intelligence |
| 10:00 – 10:30 | Networking break |
| 10:30 – 11:15 | Real Time Forensics on SCADA/ICS: A Technical Case Study Mark Fabro, Lofty Perch |
| 11:15 – 12:00 | Control Systems Security Program cyber security products and services for owners and operators of Control Systems Mike Chaney, Department of Homeland Security |
| 12:00 – 13:00 | Lunch |
| 13:00 – 13:45 | Using traffic analysis to secure the power grid SCADA system Antoine Lemay, Polytechnique Montréal |
| 13:45 – 14:30 | Canadian Cyber Incident Response Centre Frank Turbide, Canadian Cyber Incident Response Centre |
| 14:30 – 15:00 | Networking break |
| 15:00 – 15:45 | ICS-CERT/CCIRC Joint Operational Brief Mike Chaney, Department of Homeland Security Frank Turbide, Canadian Cyber Incident Response Centre |
| 15:45 – 16:30 | Closing remarks |



COST ESTIMATE

| PUBLIC SAFETY CANADA | | | |
|----------------------------------|-----------------|-------------|-------------------|
| Room Rental | Quantity | Cost | Total |
| Plaza B/C | 1 | \$3,500.00 | \$3,500.00 |
| Subtotal | | | \$3,500.00 |
| 18% Service Charge | | | \$630.00 |
| HST | | | \$495.60 |
| Total | | | \$4,625.60 |
| Food and Beverage Service | Quantity | Cost | Total |
| Food and Beverage Minimum | 1 | \$2,000.00 | \$2,000.00 |
| Subtotal | | | \$2,000.00 |
| 18% Service Charge | | | \$360.00 |
| HST | | | \$283.20 |
| Total | | | \$2,643.20 |
| Audio Visual | Quantity | Cost | Total |
| See AVW Telav Quote | 0 | \$0.00 | \$0.00 |
| Subtotal | | | \$0.00 |
| 18% Service Charge | | | \$0.00 |
| HST | | | \$0.00 |
| Total | | | \$0.00 |
| Grand Sub Total | | | \$5,500.00 |
| Service Charge | | | \$990.00 |
| HST | | | \$778.80 |
| Grand Total | | | \$7,268.80 |

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE / Autorisation de voyager et avance

- Original / Prem. demande
- Amended (Same levels of approval as original dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

| | | |
|---|---|--|
| 14A | Travel Authority No. (TAN) N°. d'aut de voyager (NAV) | Document No. - N° du document 730975 |
| Type 2 | Name of traveller - Nom du voyageur Tom Campbell | Classification EC-07 |
| Department - Ministère Public Safety Canada | Branch / Division / Group - Direction / Division / Groupe National Security/National Cyber Security Directorate | |
| Address - Adresse 240 Laurier Ave W, 11th Floor | Telephone No. - No. de téléphone | 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 SCADA Workshop | No. of days Nbre de jours 4 | Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage (CVP)? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> No / Non |
| | | If no, would you like to request one? Les cas échéant, aimeriez-vous en avoir une? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> 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 |
|-------------------|-----------|-----------|---|-------------------------------------|---|------------------------------|--|
| March 25, 2012 | Ottawa | Vancouver | 07:40-10:11 | Air | Economy | Hyatt Regency | |
| March 28, 2012 | Vancouver | Ottawa | 09:30-17:04 | Air | Economy | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel. |
|---|----------------------------------|---|----------------------------------|---|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif | |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$437.31 | Accommodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | <p>Part D - Partie D</p> <p>Estimated Cost - Coût estimatif</p> <p>Prepaid - Prépayé \$1,300.00</p> <p>Other - Autre \$927.64</p> <p>Trip Total - Coût total du voyage \$2,227.64</p> <p>Funding - Financement</p> <p>A) Travellers cheques / Chèques de voyage Cdn / Can \$0.00 US / É.U. \$0.00 Other / Autre \$0.00</p> <p>B) Other advance / Autre avance Cheque / Chèque \$0.00 Cash / Comptant \$0.00</p> <p>Total funding requested (A + B) Financement total demandé (A + B) \$0.00</p> |
| 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: <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$45.23 | Other (Specify) - Autre (préciser) | \$0.00 | |
| 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. | | Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | | |
| Transportation Transport | \$130.00 | <input type="checkbox"/> First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) <input type="checkbox"/> 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) | | |
| Meals and incidentals Repas et frais accessoires | \$315.10 | Approval - Approbation | | |
| Other (Specify) - Autre (préciser) | \$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. | Ticket pick-up date and location Date et lieu de la collecte des billets |
| Signature | Date 27/3/2013 |

| | | | |
|---|---------------------|--|---------------------|
| Recommended by (signature) - Recommandé par (signature) | Date FEB 19 2013 | Approved by (signature) - Approuvé par (signature) | Date FEB 27 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 0 | Due Date Date d'échéance |
|--------|--------------------------------|-------------------|------------------|-----------------------------|--|-----------------------------|

Accounting Information / Renseignement comptables

| | | | | | |
|--------|-----------------------|-------------------------------|--|--|------------------|
| Type 4 | Sub-type Sous-type | Vendor Code Code du fourn. | Departmental Ref. No. No. de réf. Du ministère NCS D THC T51 | Coding - Cidification 493-PSABASE-2000 | Amount - Montant |
|--------|-----------------------|-------------------------------|--|--|------------------|

| | |
|-------------|---|
| Description | Financial encumbrance No. No. de consignment de fonds 500102357 |
|-------------|---|

| | | |
|---|---|---------------------------|
| Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature) | Requestion 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) Vérfié conform (TPSGC) (signature) | | Date |
| Services officer (PWGSC) (signature) Agent responsable (TPSGC) (signature) | Signature | |

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé

| | Amount/Montant |
|-------------------------|-------------------|
| Airfare / Frais d'avion | \$1,300.00 |
| Train / Train | \$0.00 |
| Other / Autres | \$0.00 |

\$1,300.00

Estimated Cost - Coût estimatif: Other - Autre

| | Rate / Tarif | No. / Nbre | Amount/Montant |
|--|-----------------|------------|-----------------|
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du répertoire) | \$145.77 | 3 | \$437.31 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du répertoire) | \$0.00 | 0 | \$0.00 |
| | | | \$437.31 |
| 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 | 0.550 | 82 | \$45.23 |

| | Rate / Tarif | No. / Nbre | Amount/Montant |
|---|--|------------|----------------|
| Parking & Tolls / stationnement et frais de péage | | | \$80.00 |
| Taxi/Limo | Home to Airport (Train Station) | | \$0.00 |
| | Airport (Train Station) - Hotel / Meetings | | \$25.00 |
| | Hotel - Airport (Train Station) | | \$25.00 |
| | Airport (Train Station) to Home | | \$0.00 |
| | Meeting - Meetings | | \$0.00 |
| | | | \$50.00 |

| | | | |
|--|--|--|---------------|
| Transportation / Transportation (No receipt) | | | \$0.00 |
| Ferry & Miscellaneous | | | \$0.00 |

\$130.00

| | Rate / Tarif | No. / Nbre | Amount/Montant |
|------------------------------|----------------|------------|-----------------|
| Breakfast / Petits déjeuners | \$15.50 | 4 | \$62.00 |
| Lunch / Déjeuners | \$15.00 | 4 | \$60.00 |
| Dinner / Diners | \$41.30 | 3 | \$123.90 |
| Incidentals /Frais divers | \$17.30 | 4 | \$69.20 |

\$315.10

| | | | |
|---|--|--|---------------|
| Business Phone / Téléphone d'affaires | | | \$0.00 |
| Airport Improvement Fee / Frais de l'Aéroport | | | \$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

- Original / Prem. demande
- Amended (Same levels of approval as original dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

| | | |
|--|--|--|
| 14A | Travel Authority No. (TAN) N°. d'aut de voyager (NAV) | Document No. - N° du document 748329 |
| Type 2 | Name of traveller - Nom du voyageur Ryan Hunt | Classification PM-06 |
| Department - Ministère Public Safety Canada | | |
| Branch / Division / Group - Direction / Division / Groupe National Security/National Cyber Security Directorate | | |
| Address - Adresse 240 Laurier Ave W, 11th Floor | | Telephone No. - No. de téléphone 2 |
| Branch Contact - Personne ressource à la direction Jane Hayward | | Telephone No. - No. de telephone 613-991-1982 |
| If different address, send cheque to: Si adresse différente, envoyer chèque à 200 Glynn Avenue, Ottawa, K1K 4Y3 | | |
| Purpose of travel - Objet du voyage SCADA Workshop | No. of days Nbre de jours 4 | Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage (CVP)? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> No / Non |
| | | If no, would you like to request one? Les cas échéant, aimeriez-vous en avoir une? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> 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 |
|-------------------|-----------|-----------|---|-------------------------------------|---|------------------------------|--|
| March 25, 2012 | Ottawa | Vancouver | 07:40-10:11 | Air | Economy | Hyatt Regency | |
| March 28, 2012 | Vancouver | Ottawa | 09:30-17:04 | Air | Economy | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel. |
|---|----------------------------------|---|----------------------------------|---|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif | |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$437.31 | Accommodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | Part D - Partie D |
| 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: <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$0.00 | Other (Specify) - Autre (préciser) | | Estimated Cost - Coût estimatif |
| 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. | | Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | \$0.00 | Prepaid - Prépayé \$1,400.00 |
| Transportation Transport | \$150.00 | <input type="checkbox"/> First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) <input type="checkbox"/> 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 - Autre \$902.41 |
| Meals and incidentals Repas et frais accessoires | \$315.10 | | | Trip Total - Coût total du voyage \$2,302.41 |
| Other (Specify) - Autre (préciser) | \$0.00 | | | Funding - Financement |
| Approval - Approbation | | | | 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. | Ticket pick-up date and location Date et lieu de la collecte des billets Jan. 31 2013 |
| Signature | Date |

| | | | |
|---|----------------------------|--|----------------------------|
| Recommended by (Signature) - Recommandé par (signature) | Date FEB 19 2013 | Approved by (signature) - Approuvé par (signature) | Date FEB 27 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 0 | Due Date Date d'échéance |
|--------|--------------------------------|-------------------|------------------|-----------------------------|---|-----------------------------|

Accounting Information / Renseignement comptables

| | | | | |
|--------|-------------------------------|---|--|------------------|
| Type 4 | Vendor Code Code du fourn. | Departmental Ref. No. No. de réf. Du ministère | Coding - Cidification 209-2000 - PSCYBER | Amount - Montant |
|--------|-------------------------------|---|--|------------------|

| | |
|-------------------------------------|--|
| Description THC - CID-T19 | Financial encumbrance No. No. de consignment de fonds 500103107 |
|-------------------------------------|--|

| | | |
|---|---|---------------------------|
| Department pre-audit and account verification (signature) Agent min. chargé de la vér. Préalable des comptes (signature) | Requestion 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) Vérfié 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 responsable (TPSGC) (signature) | Signature | |

WORKSHEET - FEUILLE DE TRAVAIL

| Estimated Cost - Coût estimatif: Prepaid - Prépayé | | | | Amount/Montant |
|--|--|-----------------|----------------|-------------------|
| Airfare / Frais d'avion | | | | \$1,400.00 |
| Train / Train | | | | \$0.00 |
| Other / Autres | | | | \$0.00 |
| | | | | \$1,400.00 |
| Estimated Cost - Coût estimatif: Other - Autre | | | | Amount/Montant |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du répertoire) | | \$145.77 | 3 | \$437.31 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du répertoire) | | \$0.00 | 0 | \$0.00 |
| | | | | \$437.31 |
| 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 | | 0.550 | 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) | | \$50.00 | \$150.00 |
| | Airport (Train Station) - Hotel / Meetings | | \$25.00 | |
| | Hotel - Airport (Train Station) | | \$25.00 | |
| | Airport (Train Station) to Home | | \$50.00 | |
| | Meeting - Meetings | | \$0.00 | |
| Transportation / Transportation (No receipt) | | | | \$0.00 |
| Ferry & Miscellaneous | | | \$0.00 | \$0.00 |
| | | | | \$150.00 |
| | | Rate / Tarif | No. / Nbre | Amount/Montant |
| Breakfast / Petits déjeuners | | \$15.50 | 4 | \$62.00 |
| Lunch / Déjeuners | | \$15.00 | 4 | \$60.00 |
| Dinner / Diners | | \$41.30 | 3 | \$123.90 |
| Incidentals /Frais divers | | \$17.30 | 4 | \$69.20 |
| | | | | \$315.10 |
| Business Phone / Téléphone d'affaires | | | | \$0.00 |
| Airport Improvement Fee / Frais de l'Aéroport | | | | \$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 |



GOVERNMENT OF CANADA

GOVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE
Autorisation de voyager et avance

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Original / Prem. demande
- Amended (Same levels of approval as original dated)

Modifications (approbation par des agents du même niveau que pour la première demande, datée du)

Part A - Partie A

| | | |
|---|---|--|
| 14A | Travel Authority No. (TAN) N° d'aut de voyager (NAV) LNW912731 | Document No. - N° du document 730971 |
| Type 2 | Name of traveller - Nom du voyageur Ashley Bencke | Classification |
| Department - Ministère Public Safety Canada | | |
| Branch / Division / Group - Direction / Division / Groupe National Security/National Cyber Security Directorate | | |
| Address - Adresse 240 Laurier Ave W, 11th Floor | | Telephone No. - No. de téléphone 613-990-7533 |
| Branch Contact - Personne ressource à la direction Jane Hayward | | Telephone No. - No. de téléphone 613-991-1982 |
| Purpose of travel - Objet du voyage SCADA Workshop | No. of days Nbre de jours 4 | Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage (CVP)? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> No / Non |
| | | If no, would you like to request one? Les cas échéant, aimeriez-vous en avoir une? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> No / Non |

Part B - Travel Itinerary / Partie B - Itinéraire

| Date M / D - J | From - De | To - A | Time - Heure | Transportation Transport | No. of meals prepaid Nbre de repas prépayés | Accommodation Hébergement | File locator number N° de repérage du dossier |
|-------------------|-----------|-----------|---|-----------------------------|--|------------------------------|--|
| | | | Departure - Arrival Départ - Arrivée | Mode | | | |
| March 25, 2012 | Ottawa | Vancouver | 07:40-10:11 | Air | Economy | Hyatt Regency | |
| March 28, 2012 | Vancouver | Ottawa | 09:30-17:04 | Air | Economy | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel. | |
|---|----------------------------------|---|----------------------------------|---|--|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif | | |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$437.31 | Accommodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | Part D - Partie D | |
| 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: <input type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$0.00 | Other (Specify) - Autre (préciser) Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | \$0.00 | Estimated Cost - Coût estimatif | |
| 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 | <input type="checkbox"/> First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) <input type="checkbox"/> 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 | Prepaid - Prépayé \$1,400.00 | |
| Transportation Transport | \$150.00 | Approval - Approbation | | Other - Autre \$902.41 | |
| Meals and incidentals Repas et frais accessoires | \$315.10 | | | Trip Total - Coût total du voyage \$2,302.41 | |
| Other (Specify) - Autre (préciser) | \$0.00 | | | Funding - Financement | |
| | | | | A) Travellers cheques / Chèques de voyage Cdn / Can \$720.00 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) \$720.00 | |

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: *Ashley Bencke* Date: Jan 17 2013

Recommended by (signature) - Recommandé par (signature): *[Signature]* Date: **FEB 19 2013**
Approved by (signature) - Approuvé par (signature): *[Signature]* Date: **FEB 27 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 | 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

| Sub-type Sous-type | Vendor Code Code du four. | Departmental Ref. No. No. de réf. Du ministère | Coding - Cidification | Amount - Montant |
|-----------------------|------------------------------|---|-------------------------|------------------|
| | | NCS D THC T51 | 493-PSABASE-2000 | |

| | |
|-------------|--|
| Description | Financial encumbrance No. No. de consignation de fonds 500102357 |
|-------------|--|

| | | |
|---|--|---------------------------|
| 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) Vérfié conform (TPSGC) (signature) | | Date |
| Services officer (PWGSC) (signature) Agent responsable (TPSGC) (signature) | | Signature |
| | | |

GOVERNMENT OF CANADA / GOUVERNEMENT DU CANADA

TRAVEL AUTHORITY AND ADVANCE / Autorisation de voyager et avance

Original / Prem. demande
 Amended (Same levels of approval as original dated)

| | | |
|---|---|--|
| 14A | Travel Authority No. (TAN) N° d'aut de voyager (NAV) | Document No. - N° du document 730971 |
| Type 2 | Name of traveller - Nom du voyageur Frank Turbide | Classification CS-03 |
| Department - Ministère Public Safety Canada | | |
| Branch / Division / Group - Direction / Division / Groupe National Security/National Cyber Security Directorate | | |
| Address - Adresse 240 Laurier Ave W, 11th Floor | | Telephone No. - No. de téléphone 613-991-7751 |
| Branch Contact - Personne ressource à la direction Danielle St-Louis | | Telephone No. - No. de téléphone 613-991-7738 |
| Purpose of travel - Objet du voyage SCADA Workshop | No. of days Nbre de jours 4 | Do you have a Gov't Ind Travel Card (ITC)? Avez-vous une carte de voyage (CVP)? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> No / Non |
| | | If no, would you like to request one? Les cas échéant, aimeriez-vous en avoir une? <input type="checkbox"/> Yes / Oui <input checked="" type="checkbox"/> No / Non |

Part B - Travel Itinerary / Partie B - Itinéraire

| Date M/D/J | From - De | To - A | Time - Heures Departure - Arrivée Départ - Arrivée | Transportation Transport Mode | No. of meals prepaid Nbre de repas prépayés | Accommodation Hébergement | File locator number N° de repérage du dossier |
|----------------|-----------|-----------|--|-------------------------------------|--|------------------------------|--|
| March 25, 2012 | Ottawa | Vancouver | 07:40-10:11 | Air | Economy | Hyatt Regency | |
| March 28, 2012 | Vancouver | Ottawa | 09:30-17:04 | Air | Economy | | |

Part C - Expenses and Allowances / Partie C - Dépenses et indemnités

| Standard - Générales | | Non-standard - Spéciales | | Justification of non-standard items, including personal travel - Justification des dépenses spéciales, y compris les voyages à titre personnel. |
|---|----------------------------------|--|----------------------------------|---|
| Item Type de dépenses | Estimated cost Coût estimatif | Item Type de dépenses | Estimated cost Coût estimatif | |
| Accommodation (white page hotel) Hébergement (un des hôtels figurant dans la partie blanche du répertoire) | \$437.31 | Accommodation (green page hotel) Hébergement (un des hôtels figurant dans la partie verte du répertoire) | \$0.00 | Part D - Partie D Estimated Cost - Coût estimatif Prepaid - Prépayé \$1,400.00 Other - Autre \$900.51 Trip Total - Coût total du voyage \$2,300.51 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 |
| 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: <input checked="" type="checkbox"/> Traveller / Voyageur <input type="checkbox"/> Employer / Employeur | \$18.10 | Other (Specify) - Autre (préciser) Upgrade transportation (specify in "Class" above) Transport à tarif supérieur (préciser la <classe> si-dessus) | \$0.00 | |
| 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. | | <input type="checkbox"/> First class (Deputy Head or equivalent approval) Prem. Classe (approuvée par le sou-chef ou l'équiv.) <input type="checkbox"/> Business class / Other-Upgraded (other than article 3.1.9) 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) | | |
| Transportation Transport | \$130.00 | | | |
| Meals and incidentals Repas et frais accessoires | \$315.10 | | | |
| Other (Specify) - Autre (préciser) | \$0.00 | | | |
| Approval - Approbation | | | | |

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: Jan 15 / 2013

Recommended by (signature) - Recommandé par (signature): *[Signature]* Date: **FEV 19 2013**
 Approved by (signature) - Approuvé par (signature): *[Signature]* Date: **FEV 27 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 | 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 | |

Type 4

Accounting Information / Renseignement comptables

| Sub-type / Sous-type | Vendor Code / Code du fourm. | Departmental Ref. No. / No. de réf. Du ministère | Coding - Cidification | Amount - Montant |
|----------------------|------------------------------|--|-------------------------|------------------|
| | | NCSO THC T51 | 493-PSABASE-2000 | |

Description: _____
 Financial encumbrance No. / No. de consignation de fonds: 500102357

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: _____
 Date: _____
 Verified correct (PWGSC) (signature)
 Vérifié conform (TPSGC) (signature): _____
 Services officer (PWGSC) (signature)
 Agent responsable (TPSGC) (signature): _____
 Signature: _____

WORKSHEET - FEUILLE DE TRAVAIL

Estimated Cost - Coût estimatif: Prepaid - Prépayé

| | Amount/Montant |
|-------------------------|-------------------|
| Airfare / Frais d'avion | \$1,400.00 |
| Train / Train | \$0.00 |
| Other / Autres | \$0.00 |

\$1,400.00

Estimated Cost - Coût estimatif: Other - Autre

| | Rate / Tarif | No. / Nbre | Amount/Montant |
|--|-----------------|------------|-----------------|
| Accommodation (WHITE page hotel) / Hébergement (un des hôtels figurant dans la partie BLANCHE du répertoire) | \$145.77 | 3 | \$437.31 |
| Accommodation (GREEN page hotel) / Hébergement (un des hôtels figurant dans la partie VERT du répertoire) | \$0.00 | 0 | \$0.00 |

\$437.31

| | | | |
|--|---------------|----------|---------------|
| 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 | 0.550 | 33 | \$18.10 |

| | Rate / Tarif | No. / Nbre | Amount/Montant |
|---|--------------|------------|----------------|
| Parking & Tolls / stationnement et frais de péage | | | \$80.00 |

| | | | |
|-----------|--|----------------|----------------|
| Taxi/Limo | Home to Airport (Train Station) | \$0.00 | \$50.00 |
| | Airport (Train Station) - Hotel / Meetings | \$25.00 | |
| | Hotel - Airport (Train Station) | \$25.00 | |
| | Airport (Train Station) to Home | \$0.00 | |
| | Meeting - Meetings | \$0.00 | |

| | | | |
|--|--|--|---------------|
| Transportation / Transportation (No receipt) | | | \$0.00 |
|--|--|--|---------------|

| | | | |
|-----------------------|--|--|---------------|
| Ferry & Miscellaneous | | | \$0.00 |
|-----------------------|--|--|---------------|

\$130.00

| | Rate / Tarif | No. / Nbre | Amount/Montant |
|------------------------------|----------------|------------|-----------------|
| Breakfast / Petits déjeuners | \$15.50 | 4 | \$62.00 |
| Lunch / Déjeuners | \$15.00 | 4 | \$60.00 |
| Dinner / Dîners | \$41.30 | 3 | \$123.90 |
| Incidentals /Frais divers | \$17.30 | 4 | \$69.20 |

\$315.10

| | | | |
|---------------------------------------|--|--|---------------|
| Business Phone / Téléphone d'affaires | | | \$0.00 |
|---------------------------------------|--|--|---------------|

| | | | |
|---|--|--|---------------|
| Airport Improvement Fee / Frais de l'Aéroport | | | \$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 Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: FEB 21 2013

File No.: 393132
RDIMS No.: 766305

MEMORANDUM FOR THE MINISTER

THE CYBER SECURITY STRATEGY ACTION PLAN 2010-2015

(Signature required)

ISSUE

To seek your approval of the Cyber Security Strategy Action Plan 2010-15 (TAB A).

BACKGROUND

In October 2010, the Government of Canada launched *Canada's Cyber Security Strategy* (the Strategy).

On October 23, 2012, the Auditor General of Canada released his Fall 2012 report. Chapter 3 of the report looked at the Government's efforts to protect critical infrastructure against cyber threats. The report included a recommendation that "Public Safety Canada 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." In response to that recommendation, the Government committed to releasing a public interdepartmental action plan.

The Cyber Security Strategy Action Plan (the Action Plan) has been revised pursuant to comments of the interdepartmental community, and it has been approved at the Assistant Deputy Minister level in each organization.

CONSIDERATIONS

A medium profile communication approach for the Web-only release of the Action Plan has been developed. The Communications Directorate will be working with your office on the package, which will include a news release and media lines.

.../2


Canada

To ensure that all Ministers involved in the implementation of the Strategy are aware of the impending release of the Action Plan, the Privy Council Office has asked that you write to your colleagues informing them of the planned approach and send them a copy of the Action Plan. This will also allow them to provide any comments on the document. Letters are attached for your signature (**TAB B**).

RECOMMENDATION

It is recommend that you approve the Action Plan and sign the letters to your colleagues.


Should you require additional information, please do not hesitate to contact me or Ms. Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.


François Guimont

Enclosure: (2)

I approve: FEB 27 2013

I do not approve:


Vic Toews, P.C., Q.C., M.P.

Prepared by: Guillaume Lefebvre

**Pages 169 to / à 177
are withheld pursuant to section
sont retenues en vertu de l'article**

26

**of the Access to Information
de la Loi sur l'accès à l'information**

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

FEB 27 2013

The Honourable Robert Nicholson, P.C., Q.C., M.P.
Minister of Justice and Attorney General of Canada
Justice Canada
Room 105, East Block House of Commons
Ottawa, Ontario K1A 0A6

Dear colleague:

In 2010, the Government of Canada launched *Canada's Cyber Security Strategy*. Since its release, substantial progress has been achieved on all three pillars of the Strategy.

As you know, Chapter 3 of the Auditor General's Fall 2012 report examined the Government's efforts to protect critical infrastructure against cyber threats. It recommended that Public Safety Canada develop an interdepartmental action plan with deliverables and timelines for *Canada's Cyber Security Strategy* (2010). In response to that recommendation, the Government committed to releasing a public interdepartmental action plan.

Our Assistant Deputy Ministers have developed and approved the *Cyber Security Strategy Action Plan* (the Action Plan). Given that the Action Plan will be released on Public Safety Canada's website, I would like to provide you with a final opportunity to comment. Please provide any comments to Bob Gordon, Special Advisor, Cybersecurity, Public Safety Canada, at Robert.Gordon@ps-sp.gc.ca no later than March 8, 2013. The specific timing of this release will be subject to consultations with the Prime Minister's Office.

Thank you for your continued support in delivering on *Canada's Cyber Security Strategy*.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

FEB 27 2013

The Honourable Christian Paradis, P.C., M.P.
Minister of Industry
Industry Canada
235 Queen Street
Ottawa, Ontario K1A 0H5

Dear colleague:

In 2010, the Government of Canada launched *Canada's Cyber Security Strategy*. Since its release, substantial progress has been achieved on all three pillars of the Strategy.

As you know, Chapter 3 of the Auditor General's Fall 2012 report examined the Government's efforts to protect critical infrastructure against cyber threats. It recommended that Public Safety Canada develop an interdepartmental action plan with deliverables and timelines for *Canada's Cyber Security Strategy* (2010). In response to that recommendation, the Government committed to releasing a public interdepartmental action plan.

Our Assistant Deputy Ministers have developed and approved the *Cyber Security Strategy Action Plan* (the Action Plan). Given that the Action Plan will be released on Public Safety Canada's website, I would like to provide you with a final opportunity to comment. Please provide any comments to Bob Gordon, Special Advisor, Cybersecurity, Public Safety Canada, at Robert.Gordon@ps-sp.gc.ca no later than March 8, 2013. The specific timing of this release will be subject to consultations with the Prime Minister's Office.

Thank you for your continued support in delivering on *Canada's Cyber Security Strategy*.

Yours sincerely,

A handwritten signature in black ink that reads "Vic Toews".

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

FEB 27 2013

The Honourable Peter MacKay, P.C., Q.C., M.P.
Minister of National Defence
National Defence
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

Dear colleague:

In 2010, the Government of Canada launched *Canada's Cyber Security Strategy*. Since its release, substantial progress has been achieved on all three pillars of the Strategy.

As you know, Chapter 3 of the Auditor General's Fall 2012 report examined the Government's efforts to protect critical infrastructure against cyber threats. It recommended that Public Safety Canada develop an interdepartmental action plan with deliverables and timelines for *Canada's Cyber Security Strategy (2010)*. In response to that recommendation, the Government committed to releasing a public interdepartmental action plan.

Our Assistant Deputy Ministers have developed and approved the *Cyber Security Strategy Action Plan* (the Action Plan). Given that the Action Plan will be released on Public Safety Canada's website, I would like to provide you with a final opportunity to comment. Please provide any comments to Bob Gordon, Special Advisor, Cybersecurity, Public Safety Canada, at Robert.Gordon@ps-sp.gc.ca no later than March 8, 2013. The specific timing of this release will be subject to consultations with the Prime Minister's Office.

Thank you for your continued support in delivering on *Canada's Cyber Security Strategy*.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Vic Toews".

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

FEB 27 2013

The Honourable Tony Clement, P.C., M.P.
President of the Treasury Board
Treasury Board of Canada Secretariat
President's Office
140 O'Connor Street
Ottawa, Ontario K1A 0R5

Dear colleague:

In 2010, the Government of Canada launched *Canada's Cyber Security Strategy*. Since its release, substantial progress has been achieved on all three pillars of the Strategy.

As you know, Chapter 3 of the Auditor General's Fall 2012 report examined the Government's efforts to protect critical infrastructure against cyber threats. It recommended that Public Safety Canada develop an interdepartmental action plan with deliverables and timelines for *Canada's Cyber Security Strategy* (2010). In response to that recommendation, the Government committed to releasing a public interdepartmental action plan.

Our Assistant Deputy Ministers have developed and approved the *Cyber Security Strategy Action Plan* (the Action Plan). Given that the Action Plan will be released on Public Safety Canada's website, I would like to provide you with a final opportunity to comment. Please provide any comments to Bob Gordon, Special Advisor, Cybersecurity, Public Safety Canada, at Robert.Gordon@ps-sp.gc.ca no later than March 8, 2013. The specific timing of this release will be subject to consultations with the Prime Minister's Office.

Thank you for your continued support in delivering on *Canada's Cyber Security Strategy*.

Yours sincerely,

A handwritten signature in black ink that reads "Vic Toews".

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

FEB 27 2013

The Honourable John Baird, P.C., M.P.
Minister of Foreign Affairs
Foreign Affairs and International Trade Canada
Office of the Minister of Foreign Affairs
125 Sussex Drive
Ottawa, Ontario K1A 0G2

Dear colleague:

In 2010, the Government of Canada launched *Canada's Cyber Security Strategy*. Since its release, substantial progress has been achieved on all three pillars of the Strategy.

As you know, Chapter 3 of the Auditor General's Fall 2012 report examined the Government's efforts to protect critical infrastructure against cyber threats. It recommended that Public Safety Canada develop an interdepartmental action plan with deliverables and timelines for *Canada's Cyber Security Strategy* (2010). In response to that recommendation, the Government committed to releasing a public interdepartmental action plan.

Our Assistant Deputy Ministers have developed and approved the *Cyber Security Strategy Action Plan* (the Action Plan). Given that the Action Plan will be released on Public Safety Canada's website, I would like to provide you with a final opportunity to comment. Please provide any comments to Bob Gordon, Special Advisor, Cybersecurity, Public Safety Canada, at Robert.Gordon@ps-sp.gc.ca no later than March 8, 2013. The specific timing of this release will be subject to consultations with the Prime Minister's Office.

Thank you for your continued support in delivering on *Canada's Cyber Security Strategy*.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

FEB 27 2013

The Honourable Rona Ambrose, P.C., M.P.
Minister of Public Works and Government Services and Minister for Status of Women,
and Minister responsible for Shared Services Canada
Shared Services Canada
6th Floor, 434 Queen Street
Ottawa, Ontario K1A 0H9

Dear colleague:

In 2010, the Government of Canada launched *Canada's Cyber Security Strategy*. Since its release, substantial progress has been achieved on all three pillars of the Strategy.

As you know, Chapter 3 of the Auditor General's Fall 2012 report examined the Government's efforts to protect critical infrastructure against cyber threats. It recommended that Public Safety Canada develop an interdepartmental action plan with deliverables and timelines for *Canada's Cyber Security Strategy* (2010). In response to that recommendation, the Government committed to releasing a public interdepartmental action plan.

Our Assistant Deputy Ministers have developed and approved the *Cyber Security Strategy Action Plan* (the Action Plan). Given that the Action Plan will be released on Public Safety Canada's website, I would like to provide you with a final opportunity to comment. Please provide any comments to Bob Gordon, Special Advisor, Cybersecurity, Public Safety Canada, at Robert.Gordon@ps-sp.gc.ca no later than March 8, 2013. The specific timing of this release will be subject to consultations with the Prime Minister's Office.

Thank you for your continued support in delivering on *Canada's Cyber Security Strategy*.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

Canada

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?

[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)

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 [REDACTED] 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: [REDACTED]

s.13(1)(c)

s.19(1)

000184

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?

[REDACTED]

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

[REDACTED]

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: sarah.dafoe@gov.ab.ca

**Pages 186 to / à 187
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

Title of the proposed item

National Security [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 rationale and expected outcomes.

Rationale:

- The Minister of Public Safety is to lead an awareness briefing on a sensitive national security issue [REDACTED] and the steps that the federal government is taking to ensure its security.

Desired 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 [REDACTED]

Amount of time requested for this item:

5 minute presentation and 5 minute discussion

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

Acting Deputy Minister of Public Safety, Graham Flack, graham.flack@ps.gc.ca,
613-991-2895

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

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

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 190 to / à 191
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

Title of the proposed item

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)

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 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 194 to / à 195
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 196
is a duplicate
est un duplicata

Page 197
is a duplicate
est un duplicata

Page 198
is a duplicate
est un duplicata

Page 199
is a duplicate
est un duplicata

Request to Add an Agenda Item

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 rationale 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 [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 202 to / à 203
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 204
is a duplicate
est un duplicata

Page 205
is a duplicate
est un duplicata

Page 206
is a duplicate
est un duplicata

Page 207
is a duplicate
est un duplicata

2012-2013 Supplementary Estimates (B)

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

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

Budget supplémentaire des dépenses (B) 2012-2013

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 États-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 |
|---|---------------------|---|---------------------|

2012-2013 Supplementary Estimates (C)

CYBER SECURITY

PROPOSED RESPONSE:

- **Public Safety Canada is implementing its responses to the recommendations outlined by the fall 2012 report of the Office of the Auditor General. In particular, the Department will be releasing a public Cyber Security Action Plan.**
- **The Department has also increased 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.**
- **The Government 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 onsite hours to 15 hours a day, 7 days a week. The Canadian Cyber Incident Response Centre continues to have 24/7 capacity with emergency access to staff 24 hours a day.**
- **The Government 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 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 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 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.

Public Safety Canada (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. 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 PS doing to respond to the recommendations outlined in the fall 2012 Report of the Office of the Auditor General?

A2. PS will be releasing 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 is continuing 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, standard procedures and policies to provide greater clarity to its 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. How does the Strategy help me if my computer becomes infected, hacked or compromised?

A3. 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

Tel. no.
613-990-2661

Approved by (ADM level only)

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Tel. no.
613-990-4976

Budget supplémentaire des dépenses (C) pour 2012-2013

CYBERSÉCURITÉ

RÉPONSE PROPOSÉE

- **Sécurité publique Canada met actuellement en place des mesures en réponse aux recommandations formulées dans le rapport d'automne 2012 du Bureau du vérificateur général. Plus précisément, le Ministère publiera un plan d'action public sur la cybersécurité.**
- **Le Ministère a également renforcé la capacité opérationnelle et les moyens d'action du Centre canadien de réponse aux incidents cybernétiques afin d'aider encore plus les secteurs des infrastructures essentielles du Canada à détecter les cybermenaces, à les prévenir, à les atténuer et à intervenir le cas échéant.**
- **Le gouvernement a annoncé un financement supplémentaire de 155 millions de dollars sur cinq ans pour faciliter la mise en œuvre de la *Stratégie de cybersécurité du Canada*. Ces fonds contribuent à renforcer les infrastructures cybernétiques fédérales et ont permis de prolonger les heures d'ouverture du Centre canadien de réponse aux incidents cybernétiques, qui sont passées à 15 heures par jour, sept jours par semaine. Le Centre continue d'avoir une capacité de fonctionner 24 heures par jour, ayant accès à du personnel en tout temps en cas d'urgence.**
- **Récemment, le gouvernement et les États-Unis ont annoncé le *Plan d'action sur la cybersécurité entre Sécurité publique Canada et le Département de la Sécurité intérieure*. Ce plan d'action conjoint contribue à accroître la collaboration opérationnelle entre le Canada et les États-Unis afin de mieux protéger les infrastructures numériques communes et d'améliorer la coordination des interventions en cas de cyberincidents.**
- **Le gouvernement continuera de sensibiliser le public à l'aide de son site « Pensez cybersécurité », qui représente une source fiable de renseignements sur les risques en ligne ainsi que des conseils sur les moyens que peuvent prendre les Canadiens pour se protéger en ligne.**

QUESTIONS ET RÉPONSES

Q1. Quels progrès ont été réalisés en vue de mettre en œuvre la *Stratégie de cybersécurité du Canada*?

R1. Les ministères et organismes fédéraux mettent en place chacun des trois piliers de la Stratégie : renforcer les systèmes et les réseaux du gouvernement du Canada, nouer des partenariats pour protéger les cybersystèmes et réseaux essentiels à l'extérieur du gouvernement fédéral, et aider les Canadiens à se protéger en ligne.

Dans le cadre des efforts déployés pour protéger les systèmes gouvernementaux, le gouvernement du Canada a réalisé des investissements ciblés dans le but de renforcer les mesures de sécurité protégeant les réseaux fédéraux, a réduit le nombre de points d'accès à Internet et a modifié la *Politique sur la sécurité du gouvernement*. Le gouvernement a également créé Services partagés Canada, ce qui contribuera à réduire le nombre de centres de données, rationalisera le réseau du gouvernement, épargnera de l'argent et améliorera les services offerts aux Canadiens.

Sécurité publique Canada (SP) dirige les efforts déployés par le gouvernement fédéral pour nouer des partenariats avec les autres ordres de gouvernement et le secteur privé dans le but de protéger l'intégrité de l'information et des services. Nous avons resserré nos relations avec nos partenaires actuels et élargi nos activités d'information à d'autres secteurs. Nous améliorons la capacité technique et opérationnelle afin d'améliorer les conseils et le soutien offerts à nos intervenants. Par exemple, en octobre 2012, le ministre de la Sécurité publique a annoncé la publication d'un plan d'action sur la cybersécurité avec le département de la Sécurité intérieure des États-Unis visant à améliorer :

- la collaboration opérationnelle entre les centres nationaux des opérations de cybersécurité;
- la participation et l'échange d'information sur la cybersécurité avec le secteur privé;
- la coopération dans le contexte des activités en cours de sensibilisation du public au sujet de la cybersécurité.

Le Ministère dirige également les efforts déployés pour aider les Canadiens à se protéger en ligne dans le cadre d'activités, comme la campagne « Pensez cybersécurité ». En octobre, le Mois de la sensibilisation à la cybersécurité, le ministre de la Sécurité publique a fait un certain nombre d'annonces pour souligner les mesures prises par le gouvernement fédéral pour assurer la cybersécurité.

Q2. Que fait Sécurité publique Canada en réponse aux recommandations contenues dans le rapport d'automne 2012 du Bureau du vérificateur général?

R2. SP publiera un plan d'action public sur la cybersécurité, qui exposera les efforts déployés par le gouvernement pour renforcer la cybersécurité et guidera les activités de mise en œuvre prévues dans la Stratégie.

Le Ministère continue de collaborer avec les ministères et organismes fédéraux responsables pour renforcer les réseaux sectoriels, échanger de l'information avec les intervenants et offrir des outils à l'appui des activités de gestion du risque de chaque secteur, notamment le *Guide de planification sur les infrastructures essentielles* et un guide d'exercice sur table. Puisque chaque secteur des infrastructures essentielles a des besoins différents et des représentants variés, le Ministère s'est engagé à fournir des conseils sur les façons de protéger adéquatement les réseaux sectoriels ainsi qu'à élaborer un profil national des infrastructures essentielles d'ici décembre 2013.

Le gouvernement a récemment annoncé un financement supplémentaire de 155 millions de dollars sur cinq ans pour faciliter l'atteinte des objectifs de la *Stratégie de cybersécurité du Canada*. De ce montant, 13 millions de dollars sur cinq ans ont permis de prolonger à 15 heures par jour, 7 jours par semaine, les heures d'ouverture du Centre canadien de réponse aux incidents cybernétiques, lequel a accès à du personnel en tout temps en cas d'urgence. Le Ministère a également :

- mis à jour le mandat, les procédures normalisées 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. En quoi la Stratégie m'aide-t-elle si mon ordinateur est infecté, piraté ou compromis?

R3. Le gouvernement sensibilise également les citoyens directement par l'entremise de son site Web « Pensez cybersécurité », qui constitue une source fiable d'information sur les risques en ligne de même que des conseils concrets sur les moyens que peuvent prendre les Canadiens pour mieux se protéger en ligne.

| | | | |
|---|---------------------------------|--|---|
| PERSONNE-RESSOURCE : Préparé par Robert Dick Directeur général Cybersécurité nationale | N° de téléphone 613-990-2661 | Approuvé par (SMA) Lynda Clairmont Sous-ministre adjointe principale Sécurité nationale | N° de téléphone 613-990-4976 000296 |
|---|---------------------------------|--|---|

CYBER INCIDENT AGAINST TELVENT

PROPOSED RESPONSE:

- **The Government will respond decisively to address any emerging threats to Canada's digital infrastructure.**
- **One of the three pillars of this Government's Cyber Security Strategy is to use partnerships to protect these vital systems.**
- **The Government provides threat and warning information, along with mitigation advice, to industry. Private sector operators are ultimately responsible for acting on this information, and for seeking help and advice from Government during an incident.**
- **In this case, the system worked as it should. The Canadian Cyber Incident Response Centre was in touch with its allies, victims and other partners within hours of becoming aware of this incident in order to ensure industry had the information and advice needed to protect vital systems.**
- **The Canadian company came forward to seek help, and to help its clients take action before they, too, could be victimized.**
- **The Government has taken action under Canada's Cyber Security Strategy and by establishing Shared Services Canada to protect its own systems and the information Canadians entrust to us.**

CONTACTS:

Prepared by
Corey Dvorkin
Senior Stratgeist
National Cyber Security
Directorate

Tel. no.
613-990-9608

Approved by (ADM level only)
Lynda Clairmont
Senior ADM, National Security

Tel. no.
613-990-4976

QUESTION PERIOD NOTE

Date: February 22, 2013

Classification: UNCLASSIFIED

Branch / Agency: NS

Question Period Note

CYBER INCIDENT AGAINST TELVENT

ISSUE: Media reports on allegations of delayed PS response to cyber incident

BACKGROUND:

A CBC News article reported that Telvent, a Canadian manufacturing company that provides industrial control systems for the energy sector, was recently targeted by a cyber intrusion. This intrusion reportedly affected the company's operations in the United States (U.S.), Canada, and in Spain. The story alleges that it was ten days before Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) was informed of the breach.

Telvent's systems are used to control oil and gas pipelines in most of North and Latin America and some parts of Europe.

In the summer of 2012, Telvent became aware that their networks appeared to have been compromised by a cyber intrusion. This intrusion is said to have targeted files related to a specific project, principally a software system used in smart grid technologies.

Telvent, which operates in the U.S., Canada and Europe, initially reached out to a specialized incident response centre in the United States, ICS-CERT, with which it had an existing relationship. On 21 September, Telvent informed its clients that it was compromised and recommended actions to its clients for detecting and, if needed, reversing the intrusions. A Canadian energy provider which received this warning information notified CCIRC directly on 26 September.

CCIRC began working with ICS-CERT in the U.S. and with intelligence officials in Canada immediately to provide mitigation advice to Canadian industry and critical infrastructure operators, and undertook an assessment of the severity of the incident.

The news report by CBC fundamentally misconstrues the role and authorities of the Government of Canada in responding to a cyber intrusion against a private sector entity. First, while CCIRC had previously documented the specific threats which penetrated Telvent's networks and provided warnings to its stakeholders, CCIRC has no authority to ensure that private sector companies act on the information it provides.

Second, the report infers that CCIRC was negligent in detecting this threat. It is illegal for the Government to monitor the private communications of Canadians and Canadian businesses. As such, CCIRC relies on voluntary reporting.

Telvent behaved in an extremely responsible manner by notifying its clients of the intrusion, so that they too could begin acting to protect themselves. Companies are often wary of admitting they have been victimized, due to fears over liability or loss of investor confidence.

The incident whereby the networks at the Treasury Board Secretariat and Department of Finance were hacked has been widely reported. The Government has taken significant steps under Canada's Cyber Security Strategy to strengthen the security of its own systems, and has created Shared Services Canada to consolidate e-mail, networks and data centres.

Question Period Note / Note pour la Période des questions

SECURITY OF BLACKBERRY MESSAGES

ISSUE: Media reports on the use of Blackberries at Public Safety Canada.

BACKGROUND:

On 27 February, 2013, Postmedia reported that Public Safety Canada had issued its employees guidance on the use of Blackberry messaging that indicated that PIN-to-PIN messages were vulnerable and not secure. The media report is based internal guidance provided to employees that was released through an *Access to Information Act* request. The guidance provided to Public Safety Canada employees by the Corporate Management Branch is consistent with guidance provided by the Government's Information Technology (IT) security authority, the Communications Security Establishment Canada (CSEC).

CSEC is responsible for developing and providing guidance to departments and agencies for the protection of Government systems and information.

Mobile devices, and especially Blackberries, are increasingly used to transact Government business and yield considerable operational efficiencies. Blackberries make up the vast majority of mobile devices issued in Government because they are well suited to e-mail applications, are easily integrated into existing corporate IT systems, and offer a higher level of security and central control than other devices.

There are, however, inherent vulnerabilities in this technology with respect to the secure storage and exchange of sensitive information. Guidance is issued to ensure employees are aware of limitations on the type of information that should be exchanged over email or PIN messages, in order to protect sensitive Government information. As such, Public Safety Canada regularly issues best practice guidance on the secure use of this technology to its employees in order to appropriately safeguard business sensitive information.

While there is sufficient encryption controlled by the Government that is applied to email messages to allow information up to CONFIDENTIAL or PROTECTED B to be transmitted via Public Safety Canada's Blackberries, making reference to matters above that classification level is not permitted.

BlackBerry PIN-to-PIN messaging is similar to e-mail in that it allows BlackBerry device users to send messages directly to another Blackberry device. Although the messages are encrypted, the global encryption key used to secure these messages is common to all Blackberry devices. As such, it is extremely simple to intercept and read any and all messages sent using PINs. Consequently, it is not permitted to refer to any classified information, even at the CONFIDENTIAL level, in a PIN.

CSEC's guidance to departments on the use PIN-to-PIN messaging to departments was issued in March 2011 and is available on its website. It highlights the technical and business risks associated with using this medium and outlines a series of recommendations on supplementary measures that can assist in protecting the privacy and confidentiality of PIN-to-PIN messaging.

SECURITY OF BLACKBERRY MESSAGES

PROPOSED RESPONSE:

- **The Government takes very seriously its obligation to protect the sensitive information entrusted to it.**
- **Mobile devices, and especially Blackberries, are widely deployed in Government as in the private sector because they enable employees to work more efficiently.**
- **Anyone with a Government mobile device is responsible for ensuring they comply with policies for the protection of sensitive information.**
- **Public Safety Canada permits Blackberry email and approved Apple I pads to store or transmit information up to the CONFIDENTIAL or PROTECTED B security classification level. PIN messages may not be used to exchange any sensitive information.**
- **Public Safety Canada reinforces this obligation to its employees through training, awareness, and regular reminders on its internal web sites.**

CONTACTS:

Prepared by
Robert Dick

Tel. no.
613-990-9631 (work)
[REDACTED] (cell)

Approved by (ADM level only)
Lynda Clairmont
Senior Assistant Deputy Minister
National Security Branch

Tel. no.
613-990-4976 (work)
[REDACTED] (cell)

SECURITY OF BLACKBERRY MESSAGES

RÉPONSE PROPOSÉE :

- **Le gouvernement prend très au sérieux son obligation de protéger les renseignements de nature délicate qui lui sont confiés.**
- **Les appareils mobiles, particulièrement les BlackBerry, sont largement répandus au gouvernement et dans le secteur privé, car ils permettent aux employés de travailler plus efficacement.**
- **Toutes les personnes disposant d'un appareil mobile du gouvernement sont chargées de s'assurer qu'elles respectent les politiques en matière de protection des renseignements de nature délicate.**
- **Sécurité publique Canada permet l'utilisation des BlackBerry pour les courriels ainsi que des Apple iPad pour la conservation et la transmission de renseignements classifiés jusqu'au niveau de sécurité CONFIDENTIEL ou PROTÉGÉ B. On ne peut pas utiliser les messages PIN à PIN pour échanger des renseignements de nature délicate.**
- **Sécurité publique Canada renforce cette obligation auprès de ses employés au moyen de formations, de sensibilisation et de rappels réguliers sur ses sites Web internes.**

PERSONNES-RESSOURCES :

Rédigé par :
Robert Dick

Numéros de téléphone :
613-990-9631 (travail)
[REDACTED] (cellulaire)

Approuvé par (SMA seulement) :
Lynda Clairmont
Sous-ministre adjointe principale
Secteur de la sécurité nationale

Numéros de téléphone :
613-990-4976 (travail)
[REDACTED] (cellulaire)