Control Systems Security Workshop

Atelier sur la sécurité des systèmes de contrôle

St. John's, Newfoundland and Labrador | Terre-Neuve et Labrador
November | novembre 22-23, 2011

RCMP·GRC

Public Safety Canada | Sécurité publique Canada

2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

Tuesday, November 22, 2011

08:30 – 09:00 **Registration** (identification required)

09:00 – 10:15 **State of Control Systems Cyber Security**
[redacted] Department of Homeland Security

10:15 – 10:30 **Health break**

10:30 – 11:15 **Exercising Security: A look inside the NERC Cyber Risk Preparedness Assessment Program**
Mark Fabro, Lofty Perch

11:15 – 12:00 **Evaluating the Safety and Security of Automation Products & Systems**
John Cusimano, Exida

12:00 – 13:30 **Lunch break**

13:30 – 14:15 **SCADA security in the oil and gas sector**
Mark Fabro, Lofty Perch

14:15 – 15:00 **Control Systems Security Program (CSSP) cyber security products and services for owners and operators of Control Systems**
[redacted] Department of Homeland Security

15:00 – 15:15 **Health break**

15:15 – 16:00 **Canadian Cyber Incident Response Centre (CCIRC)**
Luc Beaudoin, Canadian Cyber Incident Response Centre

16:00 – 16:45 **Intrusion Detection/Prevention in Critical Networks**
Frank Marcus, Wurldtech

16:45 – 17:00 **Closing remarks**

s.15(1) - Subv

s.19(1)

2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

Wednesday, November 23, 2011

08:45 – 09:00 **Registration** (identification required)

09:00 – 09:30 **Canada's Cyber Security Strategy**
Tom Campbell, Public Safety Canada

09:30 – 10:15 **Cybercrime and Critical Infrastructure Protection**
Jacques Boucher, Royal Canadian Mounted Police

10:15 – 10:30 **Health break**

10:30 – 11:15 **Cyber Security Evaluation Tool (CSET)**
[redacted] Department of Homeland Security

11:15 – 12:00 **Smart Grid and Advanced Metering Infrastructure Security Research Activities**
Mark Fabro, Lofty Perch

12:00 – 13:30 **Lunch break**

13:30 – 14:15 **Government of Canada Control Systems Security Research**
Rodney Howes, Defence Research and Development Canada

14:15 – 15:00 **Briefing**
[redacted] Canadian Security Intelligence Service

15:00 – 15:15 **Health break**

15:15 – 16:00 **Control Systems Cyber Security Training Opportunities**
[redacted] Department of Homeland Security

16:00 – 16:45 **Break-out Session**

16:45 – 17:00 **Closing remarks**

Atelier sur la sécurité des systèmes de contrôle 2011
St. John's (Terre-Neuve et Labrador)
Programme

Le mardi 22 novembre 2011

08h30 – 09h00 **Inscription** (pièce d'identité requise)

09h00 – 10h15 **Cybersécurité des systèmes de contrôle : situation actuelle**
[redacted] Département de la Sécurité intérieure

10h15 – 10h30 **Pause-santé**

10h30 – 11h15 **Évaluer la sécurité : Un aperçu du programme d'évaluation de préparation contre les risques cybernétiques de NERC**
Mark Fabro, Lofty Perch

11h15 – 12h00 **Évaluer la sûreté et la sécurité des produits et systèmes d'automatisation**
John Cusimano, Exida

12h00 – 13h30 **Pause-repas**

13h30 – 14h15 **Sécurité des SCADA dans le secteur pétrolifère et gazifière**
Mark Fabro, Lofty Perch

14h15 – 15h00 **Programme de sécurité des systèmes de contrôle : produits et services pour la cybersécurité pour les propriétaires et opérateurs des systèmes de contrôle**
[redacted] Département de la Sécurité intérieure

15h00 – 15h15 **Pause-santé**

15h15 – 16h00 **Centre canadien de réponse aux incidents cybernétiques (CCRIC)**
Luc Beaudoin, Centre canadien de réponse aux incidents cybernétiques

16h00 – 16h45 **Détection d'intrusion / Prévention dans les réseaux essentiels**
Frank Marcus, Wurldtech

16h45 – 17h00 **Mot de la fin**

Sécurité publique Canada | Public Safety Canada

RCMP·GRC

Atelier sur la sécurité des systèmes de contrôle 2011
St. John's (Terre-Neuve et Labrador)
Programme

Le mercredi 23 novembre 2011

08h45 – 09h00 **Inscription** (pièce d'identité requise)

09h00 – 09h30 **Stratégie de cybersécurité du Canada**
Tom Campbell, Sécurité publique Canada

09h30 – 10h15 **Crimes cybernétiques et protection des infrastructures essentielles**
Jacques Boucher, Gendarmerie royale du Canada

10h15 – 10h30 **Pause-santé**

10h30 – 11h15 **Outil d'évaluation en matière de cybersécurité**
[redacted] Département de la Sécurité intérieure

11h15 – 12h00 **Réseau intelligent et activités de recherche sur la sécurité de l'infrastructure de mesure avancée**
Mark Fabro, Lofty Perch

12h00 – 13h30 **Pause-repas**

13h30 – 14h15 **Recherche sur la sécurité des systèmes de contrôle du gouvernement du Canada**
Rodney Howes, Recherche et développement pour la défense Canada

14h15 – 15h00 **Breffage**
[redacted] Service canadien du renseignement de sécurité

15h00 – 15h15 **Pause-santé**

15h15 – 16h00 **Occasions de formation sur la cybersécurité des systèmes de contrôle**
[redacted] Département de la Sécurité intérieure

16h00 – 16h45 **Réunion en petits groupes**

16h45 – 17h00 **Mot de la fin**

Speakers

s.19(1)

Control Systems Security Workshop
St. John's, Newfoundland
November 22-23, 2011

[redacted]
Department of Homeland Security
[redacted]nq.dhs.gov
Washington, D.C.
www.us-cert.gov/control_systems

John Cusimano
Director, Security Services Division
Exida
215-453-1720
jcusimano@exida.com
www.exida.com

Mark Fabro
President and Chief Security Scientist
Lofty Perch, Inc.
[redacted]oftyperch.com
15-505 Hood Road
Markham, Ontario, L3R 5V6
www.loftyperch.com

Frank Marcus
Manager, Threat Intelligence
Wurldtech Security Technologies
[redacted]wurldtech.com
(604) 669 6674
Suite 1000 - 1090 West Georgia Street
Vancouver, BC V6E 3V7
www.wurldtech.com

Jacques Boucher
NCO i/c "B" Division Technological Crime Unit
709-772-8272
jacques.boucher@rcmp-grc.gc.ca
100 East White Hills Road
P.O. Box 9700, Station "B"
St. John's, NL
A1A 3T5
www.rcmp-grc.gc.ca

Luc Beaudoin, PhD.
Chief
Canadian Cyber Incident Response Centre (CCIRC)
Public Safety Canada
613-991-9949
LucS.Beaudoin@ps-sp.gc.ca
340 Laurier Ave West
Ottawa, Canada, K1A 0P8
www.publicsafety.gc.ca/ccirc | www.securitepublique.gc.ca/ccirc

Tom Campbell
Senior Policy Advisor
National Cyber Security
Public Safety Canada
613-990-3577
tom.campbell@ps-sp.gc.ca
340 Laurier Ave West
Ottawa, Canada, K1A 0P8
www.publicsafety.gc.ca/cyber | www.securitepublique.gc.ca/cyber

Federal points of contact

Control Systems Security Workshop
St. John's, Newfoundland
November 22-23, 2011

Public Safety Canada

www.publicsafety.gc.ca/cyber | www.publicsafety.gc.ca/ci

Tom Campbell
Senior Policy Advisor
National Cyber Security
613-990-3577
tom.campbell@ps-sp.gc.ca
340 Laurier Ave West
Ottawa, Canada, K1A 0P8

Ryan Hunt
Senior Policy Advisor
Critical Infrastructure and Strategic Coordination
613-949-3994
ryan.hunt@ps-sp.gc.ca
269 Laurier Avenue West
Ottawa, Canada, K1A 0P8

Kevin Cooper
Critical Infrastructure Analyst
Newfoundland and Labrador, Regional Office
kevin.cooper@ps-sp.gc.ca
10 Barters Hill, 8th Floor
St John's, Newfoundland and Labrador, A1C 5L4

Allison Araneta
Policy analyst
National Cyber Security
613-993-8258
allison.araneta@ps-sp.gc.ca
340 Laurier Ave West
Ottawa, Canada, K1A 0P8

Tom Pacha
Policy analyst
Critical Infrastructure and Strategic Coordination
613-991-3415
tomasz.pacha@ps-sp.gc.ca
269 Laurier Avenue West
Ottawa, Canada, K1A 0P8

Royal Canadian Mounted Police

www.rcmp-grc.gc.ca

Dave Black
Manager
Cyber Crime Fusion Team
Technical Crime Branch
613-993-6579
dave.black@rcmp-grc.gc.ca
TPOF, 1426 St Joseph Blvd.
Ottawa, Canada

Jacques Boucher
NCO i/c "B" Division Technological Crime Unit
709-772-8272
jacques.boucher@rcmp-grc.gc.ca
100 East White Hills Road
P.O. Box 9700, Station "B"
St. John's, NL
A1A 3T5

Public Safety Canada is working with the RCMP to organize a Control Systems Security workshop for the Atlantic Provinces in St. John's, Newfoundland on November 22-23. Below you will find some information regarding the workshop.

The workshop is a two-day training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators better secure their most critical control system and information technology assets. It is part of a series of workshops that have taken place in other regions of Canada over the past several years.

The goal of the workshop is to provide a greater awareness of the threats and what resources are available to assist in mitigating them; provide a trusted forum where control systems owners and operators can exchange information and ideas to help improve their security posture; and help develop a trusted relationship between the federal, provincial and territorial governments; and control systems owners and operators.

Recognized experts along with representatives from the federal Government will provide briefs on the latest threats and steps that can be taken to increase the security of control systems. As we continue to work on the planning of the workshops we welcome your input and support. Additionally, if someone from your provincial government would be interested in delivering a presentation on a cyber security topic related to critical infrastructure please contact us.

Should you require more information, please do not hesitate to contact Tom Campbell by email at Tom.Campbell@ps-sp.gc.ca or phone at 613-990-3577.

Good day,

Public Safety Canada (PS) and the RCMP cordially invite you to a two-day **SCADA and Industrial Control Systems Security Workshop on January 31 to February 1, 2012 in Montréal, Québec**, at the Palais des congrès de Montréal. **There is no cost to participants to attend this workshop.**

The workshop is a two-day training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators to better secure their most critical control system and information technology assets. It is part of a series of workshops that have taken place in other regions across Canada over the past several years. Additional information is enclosed, including the topics to be presented and registration instructions. An agenda will follow in the coming weeks.

The goal of the workshop is to provide a greater awareness of the threats and resources are available to assist in mitigating them, to provide a trusted forum for control systems owners and operators to exchange information to help improve their security posture, and help develop trusted relationships between federal, provincial and territorial governments; and control systems owners and operators.

You are encouraged to circulate this invitation to anyone in your organization or network whom you deem appropriate. More than one person from an organization can attend the workshop.

Please contact Lukasz Johaniuk, Public Safety Canada, at Lukasz.Johaniuk@ps-sp.gc.ca or 613-991-3643, with any questions you may have and in order to register. We ask that you register by Friday, January 20, 2012.

Thank you,

www.publicsafety.gc.ca/ccirc | www.publicsafety.gc.ca/ci

Bonjour,

Sécurité publique Canada et la Gendarmerie royale du Canada vous invitent cordialement à un **atelier de deux jours sur la sécurité des systèmes de surveillance et d'acquisition de données (SCADA) et des systèmes de contrôle industriel qui se tiendra les 31 janvier et 1er février 2012 au Palais des congrès de Montréal, au Québec. Il n'y a pas de frais de participation.**

L'atelier de deux jours est une occasion de recevoir de la formation et de développer un sentiment d'appartenance à une collectivité. Il vise à permettre aux propriétaires et aux exploitants d'infrastructures essentielles au Canada d'améliorer la sécurité de leurs ressources les plus essentielles en matière de systèmes de contrôle et de technologies de l'information. Cette activité fait partie d'une série d'ateliers qui ont eu lieu ailleurs au Canada au cours des dernières années. Vous trouverez ci-joint des renseignements supplémentaires, y compris les sujets qui seront présentés et les directives pour s'inscrire. Un ordre du jour suivront dans les semaines à venir.

Le but de l'atelier est de mieux faire connaître les menaces et les ressources qui existent en vue de les atténuer; d'offrir un forum fiable où les propriétaires et les exploitants de systèmes de contrôle peuvent échanger des renseignements et des idées pour renforcer leur sécurité; et d'établir une relation de confiance entre les gouvernements fédéral, provinciaux et territoriaux et les propriétaires et exploitants de systèmes de contrôle.

Des spécialistes reconnus et des représentants du gouvernement fédéral décriront brièvement les menaces les plus récentes et les étapes à suivre pour augmenter la sécurité des systèmes de contrôle.

Vous êtes encouragés à inviter d'autres membres de votre organisation ou réseau si vous jugez que cela est pertinent. Plusieurs personnes d'une même organisation peuvent participer à l'atelier.

Si vous avez des questions, n'hésitez pas à communiquer avec Lukasz Johaniuk, Sécurité publique Canada, par courriel à l'adresse Lukasz.Johaniuk@ps-sp.gc.ca ou par téléphone, au 613-991-3643.

Merci.

www.securitepublique.gc.ca/ccirc | www.securitepublique.gc.ca/ie

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

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

Dates January 31 2012 – February 1 2012

Event details

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

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

Benefits of attending

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

Technical level

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

Who should attend

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

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

Speakers

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

Topics

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

Cost

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

Venue

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

Application to attend

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

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

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

Contact

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

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

2012 Control Systems Security Workshop
Montreal, Quebec
Agenda

Tuesday, January 31, 2012

08:00 – 08:30	**Registration** (identification required)
08:30 – 09:15	**State of Control Systems Cyber Security** s.19(1) [redacted] Department of Homeland Security
09:15 – 10:00	**Canada's Cyber Security Strategy** Luc Beaudoin, Public Safety Canada **Canadian Cyber Incident Response Centre (CCIRC)** Luc Beaudoin, Canadian Cyber Incident Response Centre
10:00 – 10:15	**Networking break**
10:15 – 11:00	**Threat Brief** [redacted] Canadian Security Intelligence Service **Government of Canada Control Systems Security Research** Rodney Howes, Defence Research and Development Canada
11:00 – 11:45	**Exercising Security: A look inside the NERC Cyber Risk Preparedness Assessment Program** Mark Fabro, Lofty Perch
11:45 – 13:00	**Lunch break**
13:00 – 13:45	**Control Systems Security Program (CSSP) cyber security products and services for owners and operators of Control Systems** [redacted] Department of Homeland Security s.19(1)
13:45 – 14:30	**Coordinated Vulnerability Disclosure and Vendor Software Development Procedures** Ernest Rakaczky, Invensys
14:30 – 14:45	**Networking break**
14:45 – 15:30	**Hack Session** Joel Langill, SCADAhacker
15:30 – 16:15	**Threat Brief** David Girard, Trend Micro
16:15 – 16:30	**Closing remarks**

s.15(1) - Subv

*** Report cyber incidents to CCIRC at: Cyber-incident@ps-sp.gc.ca ***

2012 Control Systems Security Workshop
Montreal, Quebec
Agenda

Wednesday, February 1, 2012

08:00 – 08:30	**Registration** (identification required)
08:30 – 09:15	**Smart Grid and Advanced Metering Infrastructure Security Research Activities** Mark Fabro, Lofty Perch
09:15 – 10:00	**Towards a Capability for Cyber Intelligence** Dr. Mourad Debbabi, National Cyber Forensics & Training Alliance (NCFTA)
10:00 – 10:15	**Networking break**
10:15 – 11:00	**Cybercrime and Critical Infrastructure Protection** Inspector Manon McSween-Seguin, Royal Canadian Mounted Police Lieutenant Martin Charette, Sûreté du Québec Commander Francesco Secondi, Service de Police de la Ville de Montréal SSA John Caruthers, Federal Bureau of Investigation
11:00 – 11:45	**Cyber Security Evaluation Tool (CSET)** Baird McNaught, Department of Homeland Security
11:45 – 13:00	**Lunch**
13:00 – 13:45	**The Canadian Common Ground Alliance (CCGA) a Unified Approach to Damage Prevention** Mike Sullivan, Alberta One-Call
13:45 – 14:30	**Government of British Columbia Security Risk Management Practices** Ken Prosser, Office of the Chief Information Officer, British Columbia
14:30 – 14:45	**Networking break**
14:45 – 15:30	**Real Time Forensics on SCADA/ICS: A Technical Case Study** Mark Fabro, Lofty Perch
15:30 – 16:15	***Control Systems Cyber Security Training Opportunities*** Baird McNaught, Department of Homeland Security
16:15 – 16:30	**Closing remarks**

*** Report cyber incidents to CCIRC at: Cyber-incident@ps-sp.gc.ca ***

Good day,

Public Safety Canada and the RCMP cordially invite you to a two-day **SCADA and Industrial Control Systems Security Workshop on March 27 to March 28, 2012 in Calgary, Alberta,** at the Delta Bow Valley Hotel. **There is no cost to participants to attend this workshop.**

The workshop is a two-day training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators to better secure their most critical control system and information technology assets. It is part of a series of workshops that have taken place in other regions across Canada over the past several years. Additional information is enclosed, including the topics to be presented and registration instructions. An agenda will follow in the coming weeks.

The goal of the workshop is to provide a greater awareness of the threats and the resources that can assist in mitigating them; to provide a trusted forum for control systems owners and operators to exchange information to help improve their security posture; and to help develop trusted relationships between federal, provincial and territorial governments and control systems owners and operators.

You are encouraged to circulate this invitation to anyone in your organization or network whom you deem appropriate.

If you have any questions, please contact Allison Araneta (Allison.Araneta@ps-sp.gc.ca or 613-993-8258) and Lukasz Johaniuk (Lukasz.Johaniuk@ps-sp.gc.ca or 613-991-3643) at Public Safety Canada. We ask that you register by Friday, March 16, 2012.

Thank you.

www.publicsafety.gc.ca/ccirc | www.publicsafety.gc.ca/ci

Bonjour,

Sécurité publique Canada et la Gendarmerie royale du Canada vous invitent cordialement à un **atelier de deux jours sur la sécurité des systèmes de surveillance et d'acquisition de données (SCADA) et des systèmes de contrôle industriel qui se tiendra les 27 mars et 28 mars 2012 à Calgary, en Alberta, à l'hôtel Delta Bow Valley. Il n'y a pas de frais de participation.**

L'atelier de deux jours est une occasion de recevoir de la formation et de développer un sentiment d'appartenance à une collectivité. Il vise à permettre aux propriétaires et aux exploitants d'infrastructures essentielles au Canada d'améliorer la sécurité de leurs ressources les plus essentielles en matière de systèmes de contrôle et de technologies de l'information. Cette activité fait partie d'une série d'ateliers qui ont eu lieu ailleurs au Canada au cours des dernières années. Vous trouverez ci-joint des renseignements supplémentaires, y compris les sujets qui

seront présentés et les directives pour s'inscrire. Un ordre du jour suivront dans les semaines à venir.

Le but de l'atelier est de mieux faire connaître les menaces et les ressources qui existent en vue de les atténuer; d'offrir un forum fiable où les propriétaires et les exploitants de systèmes de contrôle peuvent échanger des renseignements et des idées pour renforcer leur sécurité; et d'établir une relation de confiance entre les gouvernements fédéral, provinciaux et territoriaux et les propriétaires et exploitants de systèmes de contrôle.

Vous êtes encouragés à inviter d'autres membres de votre organisation ou réseau si vous jugez que cela est pertinent.

Si vous avez des questions, n'hésitez pas à communiquer avec Allison Araneta (Allison.Araneta@ps-sp.gc.ca ou 613-993-8258) et Lukasz Johaniuk (Lukasz.Johaniuk@ps-sp.gc.ca ou 613-991-3643), à Sécurité publique Canada. Vous avez jusqu'au vendredi 16 mars 2012 pour vous inscrire.

Merci.

www.securitepublique.gc.ca/ccirc | www.securitepublique.gc.ca/ie

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

Protecting Canada's Critical Infrastructure: 2012 SCADA and Industrial Control Systems Security Workshop Calgary, Alberta

Dates March 27-28, 2012

Event details

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

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

Benefits of attending

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

Technical level

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

Who should attend

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

Speakers

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

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

Topics

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

Cost

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

Venue

Delta Bow Valley
Bow Valley Ballroom
209-4th Avenue SE
Calgary, AB
T2G 0C6
(403) 266-1980

Application to attend

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

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

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

To RSVP

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

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

Sécurité publique Canada | Public Safety Canada

RCMP·GRC

2012 Control Systems Security Workshop
Delta Bow Valley Ballroom
Calgary, Alberta
Agenda

Tuesday March 27, 2012

08:00 – 08:30	**Registration** (identification required)	
08:30 – 08:45	**Opening Remarks from Public Safety Regional Representative** James Gulak, Public Safety Canada	
08:45 – 09:15	**State of Control Systems Cyber Security** [redacted] Department of Homeland Security	s.19(1)
09:15 – 09:45	**Government of Canada Control Systems Security Research** Rodney Howes, Defence Research and Development Canada	
09:45 – 10:15	**Networking break**	
10:15 – 11:00	**Canada's Cyber Security Strategy** Robert Dick, Public Safety Canada **Canadian Cyber Incident Response Centre (CCIRC)** Bud Cameron, Canadian Cyber Incident Response Centre	
11:00 – 11:45	**Cybercrime Threat in Control Systems** Dave Black (RCMP) and [redacted] FBI)	s.19(1)
11:45 – 13:15	**Lunch break**	
13:15 – 14:30	**Smart Grid and Advanced Metering Infrastructure Security Research Activities** Mark Fabro, Lofty Perch	
14:30 – 15:15	**Coordinated Vulnerability Disclosure and Vendor Software Development Procedures** Paul Forney, Invensys	
15:15 – 15:45	**Networking break**	
15:45 – 16:45	**Panel Discussion: Reporting Cyber Incidents to Senior Management** Moderator: Mark Fabro Panelists: [redacted] FBI), Dave Black (RCMP), Paul Forney (Invensys), TBD	s.19(1)
16:45 – 16:50	**Closing remarks**	

*** Report cyber incidents to CCIRC at: Cyber-incident@ps-sp.gc.ca ***

Sécurité publique Canada | Public Safety Canada

RCMP·GRC

2012 Control Systems Security Workshop
Delta Bow Valley Ballroom
Calgary, Alberta
Agenda

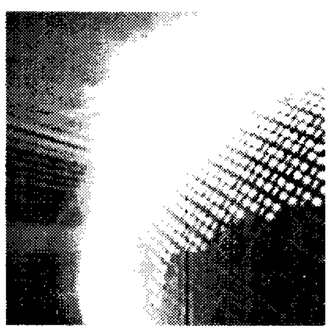
Wednesday March 28, 2012

08:00 – 08:30	**Registration** (identification required)
08:30 – 09:15	**Cyber Threat Intelligence Brief (TBD)** Bud Cameron, Public Safety Canada
09:15 – 10:00	**Control Systems Security Program (CSSP) cyber security products and services for owners and operators of Control Systems** Baird McNaught, Department of Homeland Security
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	**Exercising Security: A look inside the NERC Cyber Risk Preparedness Assessment Program** Tim Roxey, NERC
12:00 – 13:30	**Lunch**
13:30 – 14:15	**Unicorns and Air Gaps – Do They Really Exist?** Eric Byres, Byres Security
14:15 – 15:00	**Cyber Security Evaluation Tool (CSET) & Control Systems Cyber Security Training Opportunities** Baird McNaught, Department of Homeland Security
15:00 – 15:30	**Networking break**
15:30 – 16:30	**Discussion Panel: Cyber Security Best Practices in the Energy Sector** Moderator: Mark Fabro Panelists: Tim Roxey (NERC), Aris Espejo (Syncrude), Eric Byres (ByresSecurity), Pierre Janse van Rensberg (ENMAX) (TBD)
16:30 – 16:45	**Closing remarks**

*** Report cyber incidents to CCIRC at: Cyber-incident@ps-sp.gc.ca ***

Public Safety Canada | Sécurité publique Canada

SAFE RESILIENT CANADA

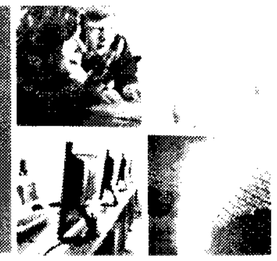


Public Safety Canada Cyber Security

Security and Emergency Management Workshop for Water & Wastewater Utilities, November 2011

Canada

Presentation Outline



SAFE RESILIENT CANADA

- An overview of Canada's *Cyber Security Strategy*
- The Canadian Cyber Incidence Response Centre (CCIRC)
- Control Systems / SCADA-Related Activities
- "Get Cyber Safe" – Canada's Public Awareness Campaign

Canada's Cyber Security Strategy

- Signals cyber security as a priority for the Government of Canada.

- Demonstrates leadership and coordinates domestic and international action.

- Leverages existing efforts, both within the Government of Canada and by our key partners.

- The Strategy is built on **three** pillars:

  1. **Secure Government systems**

  2. **Partner to secure systems outside the Government of Canada**

  3. **Help Canadians to be secure online**

Progress in Implementation

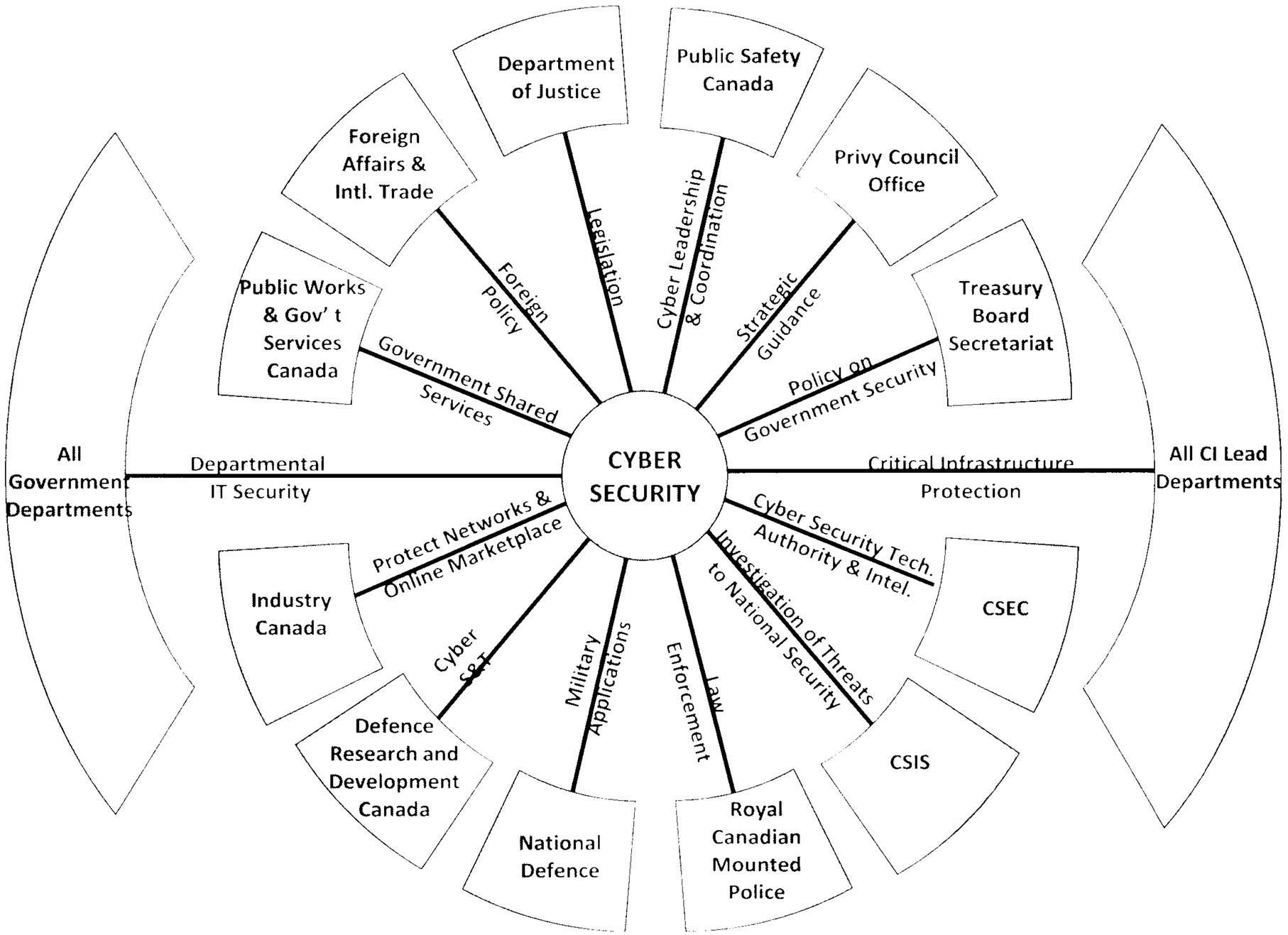
Since the release of the Government of Canada's Cyber Security Strategy in 2010, Public Safety Canada has been working to implement the three pillars:

1. Secure Government systems
   - Shared Services Canada established to consolidate Government networks
   - Realigned the Government's cyber incident response coordination through the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre

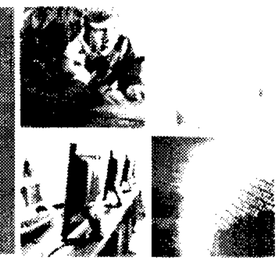
2. Partner to secure systems outside the Government of Canada
   - Engaging with critical infrastructure sectors to establish collaborative mechanisms and work-plans, including the development of *Information Sharing arrangements*
   - Strengthened the Canadian Cyber Incident Response Centre's relationships and service offerings
   - Strengthening policy and operational partnerships with key allies

3. Help Canadians to be secure online
   - Prepared a nationwide communications campaign and developing partnerships for "Cyber Security Awareness Month" in October 2011

Cyber Security Roles and Responsibilities within the Government of Canada



Cyber Security Roles and Responsibilities within Public Safety Canada



SAFE RESILIENT CANADA

INCIDENT MANAGEMENT & INFORMATION SHARING

Canadian Cyber Incident Response Centre

CYBER POLICY & COORDINATION

National Cyber Security Directorate

CRITICAL INFRASTRUCTURE PROTECTION

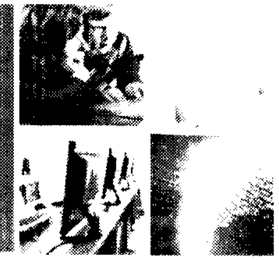
Critical Infrastructure Protection Directorate

PUBLIC AWARENESS

Communications Directorate

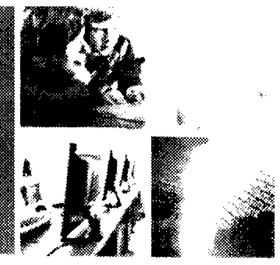
NCSD

Canadian Cyber Incidence Response Centre (CCIRC) Mandate and Roles



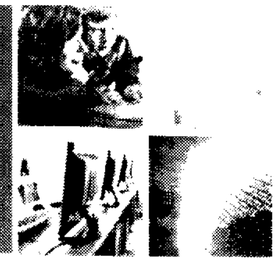
- Mandate:
  - CCIRC, as the Canadian national CERT, is the designated entity within the federal government entrusted with coordinating the response to cyber security incidents of national interest and protecting critical infrastructure.
- Directorate
  - Located within the National Cyber Security Directorate of Public Safety Canada (Since Nov 14, 2011)
- Roles:
  - Reduce Cyber Vulnerability and Risk
  - Provide Effective Cyber Response
  - Coordination with Partners

CCIRC Services



- **Incident Coordination** between national and international cyber security stakeholders;
- Dissemination of **Cyber Awareness** Products;
- **Notifying** domestic **stakeholders** of compromised systems;
- Malicious sites **takedown**;
- **Facilitate** Information **sharing**;
- **Analysis** of malicious software;
- **Repatriation** of stolen data;
- Vulnerability **disclosure coordination.**

The CCIRC Landscape



SAFE RESILIENT CANADA

Cyber Response unit (CRU)

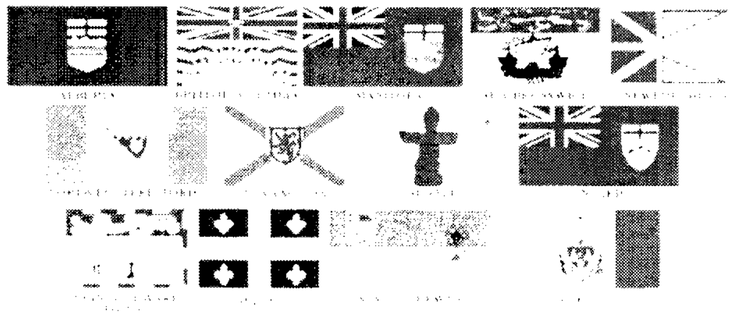
CA Authorities

CRTC

cira

CRC

Provinces



Canada

Government

CCIRC

ISP's

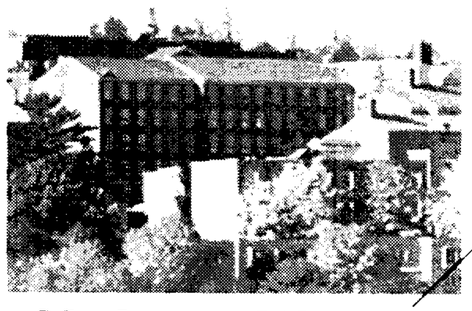
TELUS Bell

RIM COGECO VIDEOTRON

allstream SaskTel

US-CERT

International



Universities:

CUCCIO,ISSNet

TREND MICRO McAfee

symantec

Defence

shadowserver

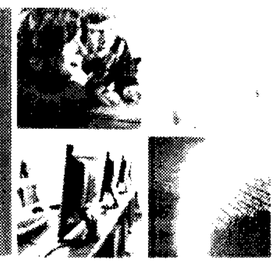
AV Vendors

CI Sectors:

Health	Food
Finance	Water
ICT	Safety
Energy and utilities	Manufacturing
Government	Transportation

Public Safety Canada / Sécurité publique Canada

CCIRC Upcoming Projects

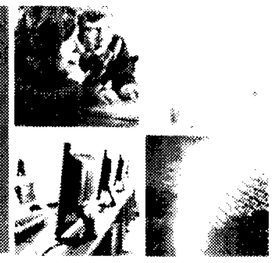


- **CCIRC Cyber Community Portal – C3P** (proposed for December 2011)
  - Government Incident Response Teams (P/T/M), Critical Infrastructure owners and operators, Critical Infrastructure associations
  - Features: Document libraries, Member directory (tentative), Forums, Wiki-like facility, Custom lists on request, Links to research, and response tools, Online incident reporting form (in development)

- **Cyber Situational Awareness** (December 2011)
  - Threat information and intelligence – including current and projected actions, doctrine, capability and intent.

- **SCADA Systems Test-bed Project** (March 2012)
  - Public Security Technical Program (PSTP) is a partnership led by DRDC Centre for Security Science (CSS).
  - Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) is the lead Federal department. Solana Networks is the lead industrial partner. Other project participants include Byres Security, Bell Canada and Exida
  - Purpose: To reduce the cyber risk to SCADA networks that manage Evaluate cyber threats, vulnerabilities and mitigations potentially impacting various SCADA systems and processes that support Canada's critical infrastructure sectors;

CCIRC's SCADA Systems Test-bed Project



- Part of a *Defence Research and Development Canada* (DRDC) research portfolio

- The goal is to fill the knowledge and capability gap concerning the construction and use of a SCADA test-bed for purposes of evaluating cyber security of SCADA networks managing Canada's critical infrastructure.

- The project objectives are:
  - Setting up a SCADA test bed in a protected laboratory environment and study how it can be applied to test out various network architectures;
  - Evaluate security technologies on the various architectures;
  - Develop best cyber security practices and recommendations.

- CCIRC is leading the project, in collaboration with Solana Networks as the industrial partner. Other project participants include Byres Security, Bell Canada and Exida.

Project Outcomes

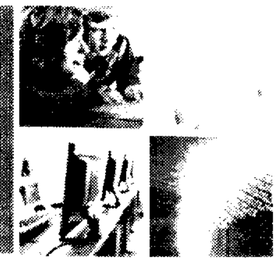
- Develop and setup of a model-based emulated SCADA test bed in CCIRC's cyber laboratory;

- Assess the vulnerability of two common architectures utilized in operational SCADA networks;

- Evaluate the effectiveness of two security technologies to detect/protect against SCADA cyber threats;

- Develop a best-practices manual for securing SCADA networks.

SCADA Security Workshops



SAFE RESILIENT CANADA

- The Government of Canada is hosting a series of regional workshops focused on control systems security
- Two-day 'no-fee' training and community building opportunity aimed at infrastructure owners and operators, including:
  - Presentations and training from control system security experts in industry and government
  - Opportunity to network with regional colleagues in the field
- Past regional workshops include Saskatchewan, BC, Ontario, and Newfoundland
- Workshops in Quebec and Alberta are scheduled for early 2012
  - For further information contact

    Tom Campbell, Public Safety Canada

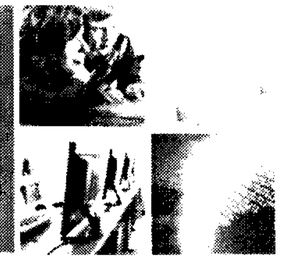
    (613) 990-3577 or @ tom.campbell@ps.gc.ca

Pillar 3 - Help Canadians to be secure online

Canadians need three things to be secure online:

1. Awareness of the need to act
2. Information about how to act
3. Protection from those who act criminally

Public Awareness Campaign, "GetCyberSafe"



Objectives of the public awareness campaign:

Knowledge Objectives

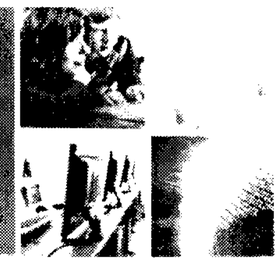
- Increase Canadians' awareness of what constitutes: an online threat; sensitive and or/or personal information; high-risk behaviour relating to cyber security
- Increase Canadians' awareness of cyber security practices and tools to protect themselves, their computer and their information

Attitude Objectives

- Increase the number of Canadians who believe (agree) that strengthening their cyber security is important

Behaviour Objectives

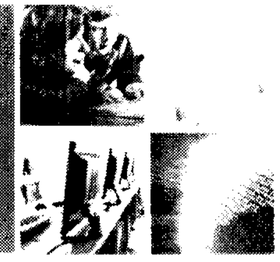
- Increase actions taken by Canadians at home, at work and in-between (mobile users) to secure their computers/mobile devices and protect their personal information



Goals of the study:

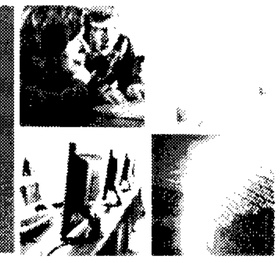
- To establish a quantitative baseline of the state of public opinion on the issue of cyber security, including knowledge level of the issue, beliefs, and behaviours
- To provide the data required to obtain a segmentation analysis (psychographic and demographic) of the online Canadian public 18 years of age or older
- To help identify target audiences - those most likely to take action as well as at-risk populations
- To segment population:
  - Youth
  - Adults (often breaking out messaging for parents and educators)
  - Seniors

Key Findings – Baseline Data



- Canadians are generally sophisticated users of Internet and understand its threats.
- They are aware of need to protect themselves, although some do not demonstrate the behaviours to back it up.
- Demand for information is high, including on how to recognize online threats and how to protect oneself.
- Most Canadians feel confident they can protect themselves given the right information.
- Trust in government to provide information is high.

Creative Concepts



- Banner
- Video
- Radio Ad

Creative concepts available through:

http://www.getcybersafe.gc.ca/abt/ads-eng.aspx

Des produits créatifs sont disponible à:

http://www.pensezcybersecurite.gc.ca/abt/ads-fra.aspx

[redacted]

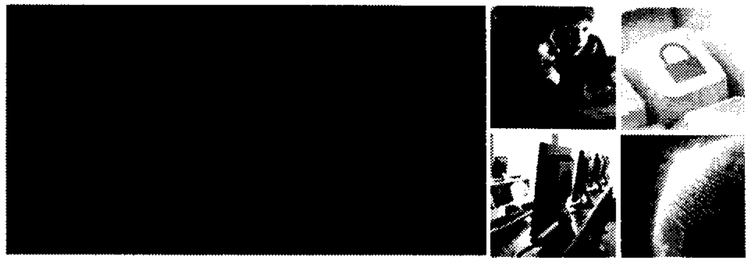
Government of Canada | Gouvernement du Canada

Canada

Get Cyber Safe

GetCyberSafe.ca

Français | Home | Contact Us | Help | Search | canada.gc.ca



BUILDING A **SAFE** AND **RESILIENT CANADA**

Home

Know the Risks
- Online Activities
- Common Threats
- Scams and Fraud

Protect Yourself
- Protect Your Identity
- Protect Your Money
- Protect Your Family

Protect Your Devices
- Computers, Laptops and Tablets
- Mobile Devices
- Home Networks
- Storage

Resources
- Public Safety Canada
- Canada's Cyber Security Strategy

About Us

Proactive Disclosure

GETCYBERSAFE

Make cyber safety a personal priority with tips and resources to help protect everything that's important to you.

Find out where the risks are

The first step to keeping yourself safe from online risks is knowing where they are.

Email | Banking & Finance | Social Networks | Mobile

Online Shopping & Auctions | Entertainment Games & Contests | Downloading & File Sharing | Voice Over Internet Protocol (VoIP)

Share | Email

Search

GetCyberSafe Video

See the Ad

It Happened to Me

Here's your chance to share your story and read about others' experiences. By passing along any helpful information you've learned, you may be able to help someone else protect themselves against cyber crime.

Cyber Security Awareness Month 2011

This month, take time to find out how to protect yourself online by learning how to create a stronger password, recognize a phishing scam, safeguard personal information, and more.

Take Our Quiz

You receive an email from your bank telling you to update your account information immediately, or the account will be closed within 48 hours. What do you do?

- Reply to the email asking for more details, including why they're sending me such an urgent request out of the blue.
- Call the customer relations at my bank and ask them if they sent the email.
- Reply to the email with the requested information, including my password.

Submit

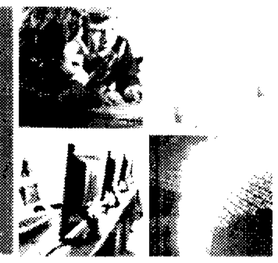
Last Updated: 2011-10-01

Top of Page

Important Notices

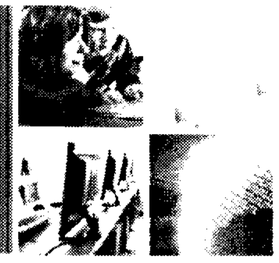
Public Safety Canada | Sécurité publique Canada

Next steps



- Explore potential opportunities with water sector
- Continue to develop partnerships and opportunities for collaboration with private sector
- Sustain the message and continue momentum
- Evaluate and monitor phase 1 of the campaign

Contact Information:



SAFE RESILIENT CANADA

Sebastien Labelle

Director, Engagement and Partnerships, National Cyber Security Directorate

613-990-2655, Sebastien.labelle@ps-sp.gc.ca

Robert Pitcher

Canadian Cyber Incident Response Centre (CCIRC)

613-949-8318, Robert.pitcher@ps-sp.gc.ca

Stéphanie Durand

Director General, Public Safety Communications

613-991-2799, stephanie.durand@ps-sp.gc.ca

Nov 2011

CCIRC JOINS NCSD

Key Messages:

As part of the implementation of *Canada's Cyber Security Strategy* and the ongoing efforts to enhance the Government of Canada's capacity to respond to cyber threats, Public Safety Canada is transferring the Canadian Cyber Incident Response Centre (CCIRC) from the Operations Directorate to the National Cyber Security Directorate (NCSD) under Robert Dick, Director General, effective November 14, 2011. This transfer will integrate the department's full range of cyber security policy and operational activities into a single organization.

This realignment is based on the functional benefits of integrating the policy and operational aspects of cyber security.

The almost daily reports of new and disturbing cyber attacks emphasize the importance of unifying Public Safety's cyber security activities and enabling CCIRC to fully deliver on its role as Canada's official national Computer Emergency Response Team (CERT).

The transfer will also help streamline our engagement with provinces and territories and critical infrastructure and private sector partners, while improving our collaboration efforts with Canada's international partners.

Recent global events have stressed the critical role played by national governments in the response to emergency events. This realignment will allow the Government Operations Centre to focus on its mission of supporting, on behalf of the Government of Canada, response coordination for events affecting the national interest.

REALIGNMENT OF CCIRC WITHIN NCSD
QUESTIONS AND ANSWERS

1. Why is CCIRC being realigned within NCSD?

   As part of the implementation of *Canada's Cyber Security Strategy,* this realignment will allow the department to unify its full range of cyber security policy and operational activities into a single organization.

2. When will this change be effective?

   The change will be effective as of Monday, November 14th, 2011.

3. Will current job classification levels be affected?

   No, we do not expect any impact on current job classification levels.

4. Will there be layoffs as a result of these changes?

   No, these changes will not affect our current complement of resources. In fact, with the combined salary dollars from CCIRC and NCSD, once fully staffed, we will have a complement of approximately 50 positions.

5. Will this change affect staffing actions currently underway?

   No, we expect all current actions to continue.

6. Will this change affect current acting assignments?

   No, we expect current acting situations to continue for the original period specified in the acting assignment.

7. Will this change involve physical relocations?

   For the foreseeable future, we will all remain in our current locations.

8. What is the impact on the Government Operations Centre (GOC)?

   There will be no impact to the Government Operations Centre.

9. How will internal partners and external clients be informed of this change?

   Notices will be developed to be sent to internal government partners and external clients.

10. Will this realignment affect our external clients?

    We are not expecting any immediate impacts on CCIRC clients. Over time however, we are hopeful that as CCIRC moves more fully into its role as Canada's official national CERT and as we better integrate CCIRC and NCSD activities, that services to clients will be even further enhanced.

11. Will CCIRC be renamed?

    Probably, but at a future date.

12. How will CCIRC be integrated within NCSD?

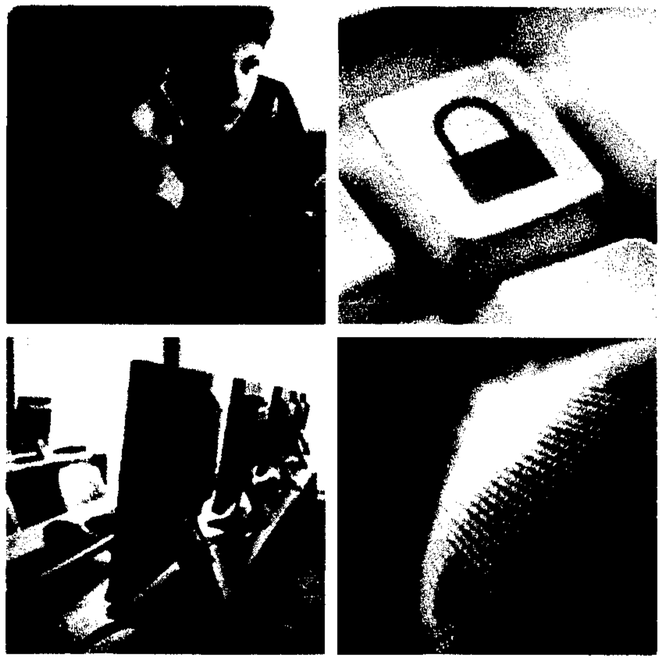
    The Director of CCIRC will report directly to the Director General, National Cyber Security. The Director of CCIRC will be part of the NCSD Management Team and as such will be part of its weekly management meetings. CCIRC will benefit from NCSD's central services, such as Finance, HR, ATIP, Accommodation and Travel coordination. CCIRC's Administrative Assistant will become a member of NCSD's Admin Working Group and will receive operational direction from the Director of CCIRC and functional guidance from NCSD's Office Manager.

13. How large is the new NCSD with the inclusion of CCIRC?

    CCIRC will be the largest Division within NCSD. The combined salary budgets will allow us to staff up to our full complement of approximately 50 FTEs.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

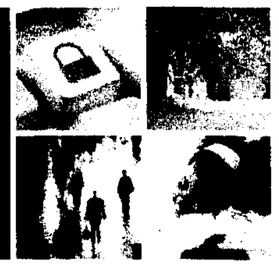


CCIRC Cyber Community Portal

November 2011

Canada

CCIRC Cyber Community Portal

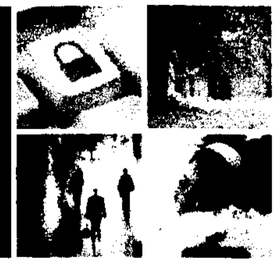


BUILDING A **SAFE** AND **RESILIENT** CANADA

- Moving to the Public Safety Canada's SharePoint platform will provide CCIRC's client community with a richer, full featured portal experience including:
  - Flexible file sharing;
  - Custom lists;
  - Report forms;
  - Workflow; and
  - Forums / blogs

- Will bring the CCIRC Portal inline with current technologies being deployed at Public Safety Canada.

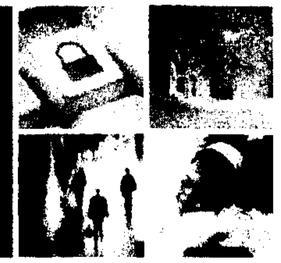
How it will work



BUILDING A **SAFE** AND **RESILIENT** CANADA

- The CCIRC Cyber Community Portal will be an operational portal:
  - The community will be made up of IT Security Coordinators, Departmental Security Officers, IT Security Analysts etc. from all levels of government and critical infrastructure.
  - CCIRC currently has over 300 member accounts on our legacy portal in the CCIRC lab where we make available our weekly "GovIRT" products. This number will increase as we continue our outreach to our CI Partners.
- Only registered members will get an account.
- Every portal member will have her/his own user ID and password which will allow access to all portals where they have been granted permissions.
- We will provide per-sector private areas on the portal:
  - Members who have access to both CIPD and CCIRC portals may have to re-authenticate as they move from one part of the portal to another.

Technical Specifications



BUILDING A **SAFE** AND **RESILIENT** CANADA

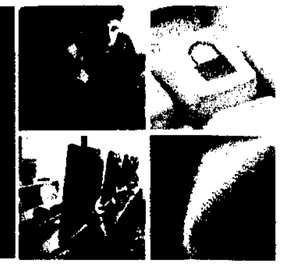
s.16(2)(c)

- [redacted]
- [redacted]
- [redacted]

[redacted]

Public Safety Canada / Sécurité publique Canada

Content Management



BUILDING A **SAFE** AND **RESILIENT CANADA**

- CCIRC will not post classified material on the community portal.

- CCIRC products will be posted as soon as they are finalized/approved. Many products are time sensitive (e.g. Cyber Flashes).

- CCIRC members may post additional content on a daily basis. (Documents, links to useful sites, contact information, etc).

- CCIRC may also post information live, during the weekly Webex teleconference.

- CCIRC is engaging IT to facilitate the generation of reports from the portal (e.g., business metrics).

Content Management (cont'd)

- Access to the portal will be subject to non-disclosure agreement or memorandum of understanding.

- CCIRC staff will have control over the content and membership in order to maintain trust.

- CCIRC will allow members to post indicators of compromise and other defensive information to benefit other members.

- Forums and blogs will be monitored and moderated, as the information that will be exchanged via the portal will likely be sensitive in nature and warrant timely review by knowledgeable individuals.

Canada

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

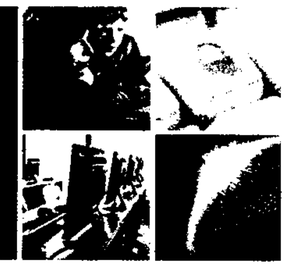
Canada's Cyber Security Strategy

Presented to the CA/US Emergency Preparedness Committee for Civil Transportation (EPCCT)

November 2, 2011
Ottawa, Canada

Canada

Government of Canada Initiatives

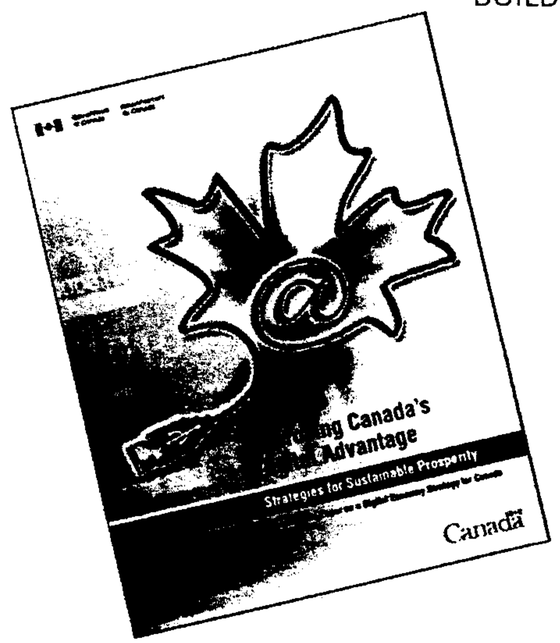


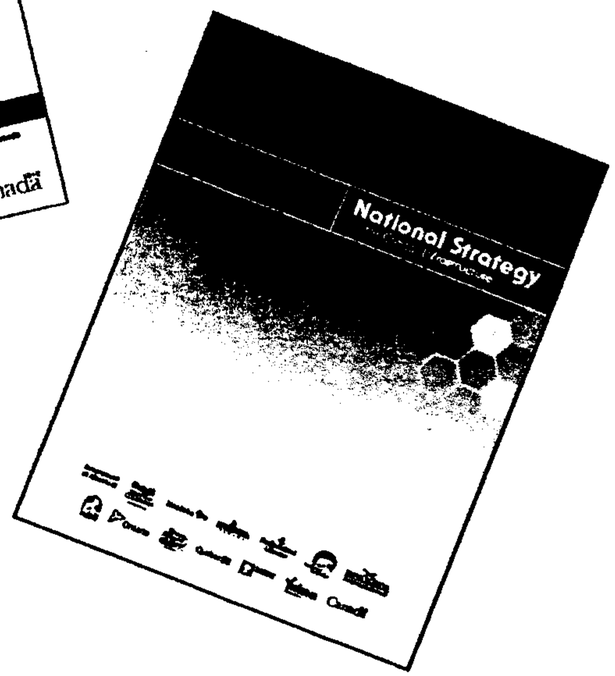
BUILDING A **SAFE** AND **RESILIENT CANADA**

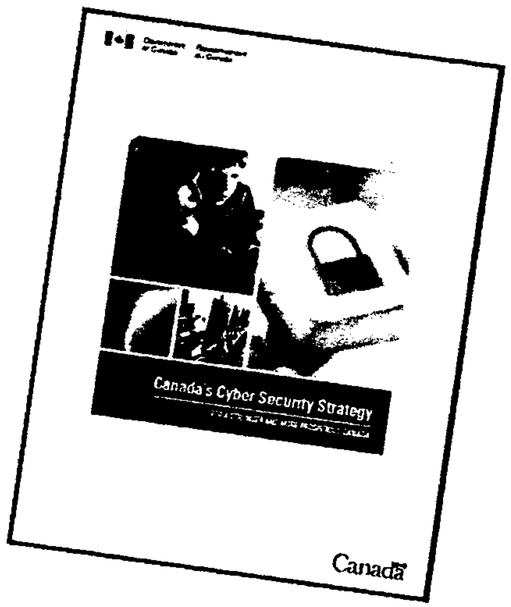
- *Consultation Paper on a Digital Economy Strategy for Canada* (May 2010).

- *National Strategy and Action Plan for Critical Infrastructure* (May 2010).

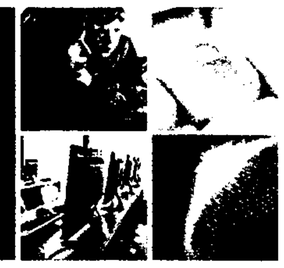
- *Canada's Cyber Security Strategy* (October 2010).







Canada's Cyber Security Strategy



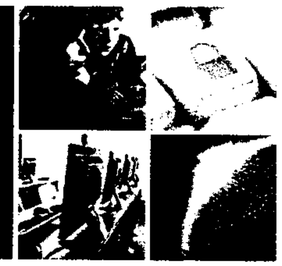
BUILDING A **SAFE** AND **RESILIENT CANADA**

- Signals cyber security as a priority investment for the Government of Canada.
- Coordinates and unifies domestic and international action.
- Built on three pillars:

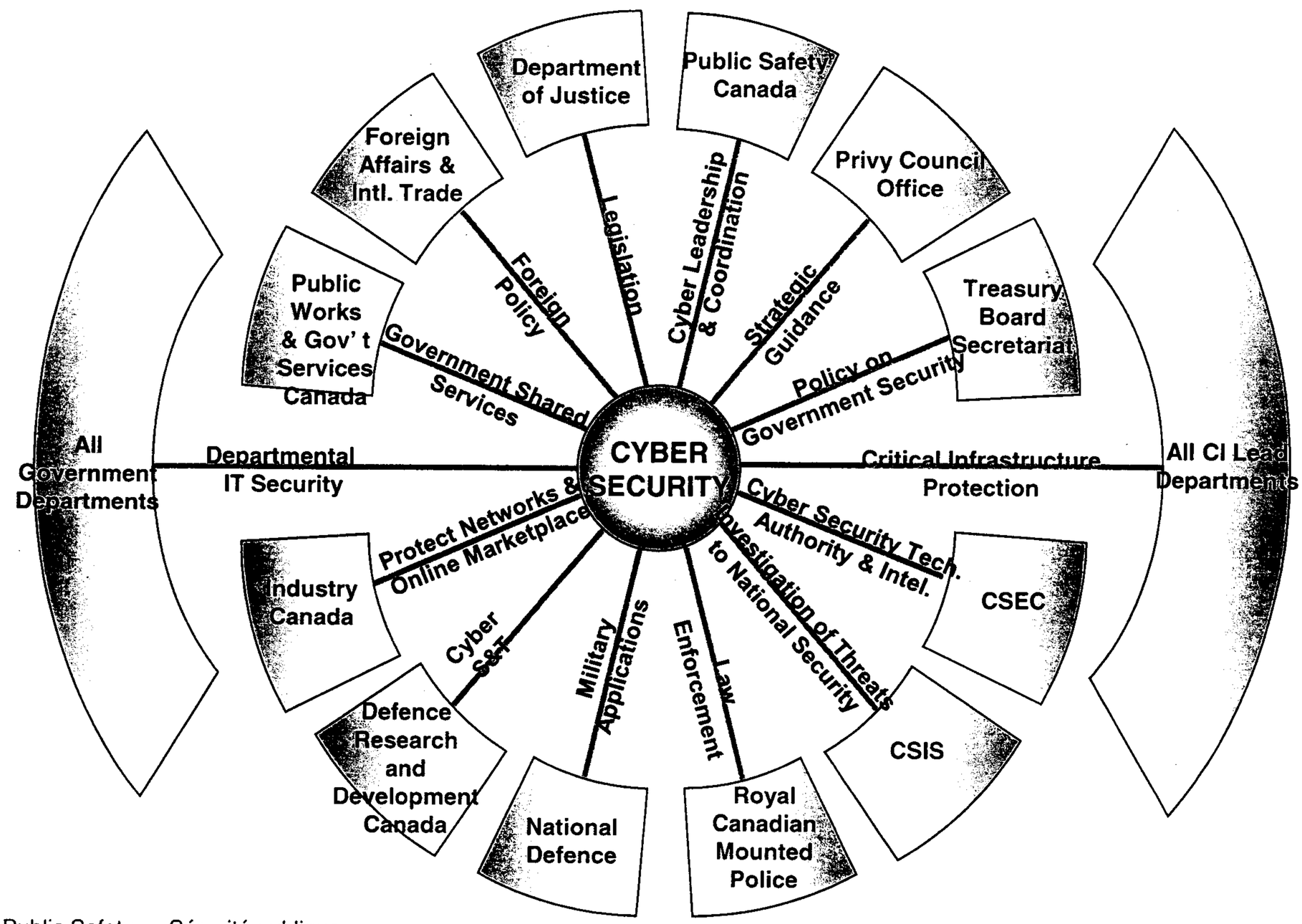
1. Secure Government systems.
2. Partner to secure systems outside the Government of Canada.
3. Help Canadians to be secure online.

UNCLASSIFIED

Cyber Security Roles and Responsibilities within the Government of Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**



Progress on Implementation and Upcoming Initiatives

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Streamlined and consolidated Government IT infrastructure, and created Shared Services Canada.
- Redefined the responsibilities for cyber security incidents affecting Canadian networks.
- Engaged provincial and territorial governments to shape a joint action plan to guide collaboration on cyber security matters.
- Created the National Cross-Sector Forum to build partnerships, improve information sharing, and address the physical and cyber vulnerabilities that span all critical infrastructure sectors.
- Updating laws to reflect the realities of the digital world.
- Developed cyber security public awareness campaign.
- Expanded Canada-U.S. cooperation on cyber security.

Shared Services Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

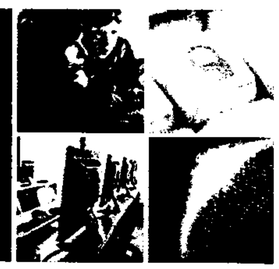
- Effective August 4, 2011, the Government streamlined and consolidated its IT architecture in the areas of email, data centres and networks.
- This will produce savings and reduce the Government's footprint; strengthen security and the safety of Government data to ensure Canadians are protected; and realize economies of scale and make it more cost-effective to modernize these IT services.
- All resources associated with the delivery of email, data centre and network services are being transferred from 44 of the more IT-intensive departments to a new entity called Shared Services Canada.

Division of Cyber Security Roles in Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

- On June 20, 2011, the responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the Cyber Threat Evaluation Centre, which is the computer emergency response team for federal departments and agencies.
  - CCIRC is now the national computer emergency response team for provinces, territories and critical infrastructure sectors.

Meetings with Provincial and Territorial Governments



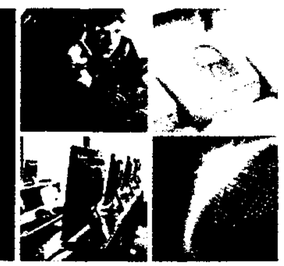
BUILDING A **SAFE** AND **RESILIENT CANADA**

- Initiated dialogue with provincial and territorial interlocutors to strengthen intergovernmental engagement on cyber security.
- Key objectives from a federal perspective:
  - clarify national operational roles and responsibilities;
  - improve information sharing;
  - engage critical infrastructure and private sectors;
  - ensure a better informed population by maximizing resources and leveraging provincial and territorial access to the public;
  - establish a forum for consultation on legislative and policy undertakings;
  - explore interest in the development of a national cyber incident response framework; and
  - ensure a cohesive front in regards to international efforts and pressures.

National Cross-Sector Forum

- Four priorities were identified at the inaugural meeting:
  - Develop a common understanding of critical infrastructure within and across sectors.
  - Establish an information sharing framework for sensitive information shared between public-private and private-private entities.
  - Identify key assets and critical systems.
  - Identify key interdependencies and vulnerabilities.
- Engaged with provincial and territorial departments of telecommunications, energy and natural resources.

Canadian Security Telecommunications Advisory Council



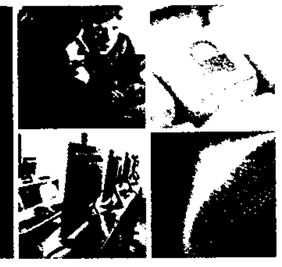
BUILDING A **SAFE** AND **RESILIENT CANADA**

- CSTAC is comprised of senior executives from the public and private sectors. It provides a forum to:
  - exchange information;
  - collaborate strategically on current and evolving issues that may affect the confidentiality, integrity or availability of the telecommunications infrastructure; and
  - provide advice on measures to address these issues.
- The Committee is focusing on several areas:
  - risks to the critical telecommunications infrastructure, including proactive and mitigating measures to address threats and vulnerabilities;
  - network monitoring;
  - interdependencies; and
  - emergency management and disaster recovery.

Legislation

- Passed two pieces of legislation to enhance cyber security.
  - Anti-Spam Bill:
    - Seeks to deter the most damaging and deceptive forms of spam from occurring in Canada.
    - Authorizes the creation of a spam reporting centre.
  - Bill S-4:
    - Amends the *Criminal Code* to create three new offences related to identity theft, with five-year maximum sentences.
    - Authorizes courts to order offenders to pay restitution to a victim of identity theft as part of their sentence.
- Examining ways to provide law enforcement with modernized investigative tools to address cyber crimes.

Get Cyber Safe.ca Campaign



BUILDING A **SAFE** AND **RESILIENT CANADA**

- Public Safety Canada's Communications Directorate has launched a national public awareness advertising campaign to deliver on the third pillar of *Canada's Cyber Security Strategy.*
- Provides Canadians with information on cyber threats in order for them to take action to protect themselves and their personal information.
- Includes advertising, a cyber-specific website, marketing partnerships and international coordination of messaging, as well as issues management in response to cyber incidents.
- Was launched in October to coincide with Cyber Security Awareness Month and the one-year anniversary of the Strategy.

Public Awareness Campaign

BUILDING A **SAFE** AND **RESILIENT CANADA**

Government of Canada / Gouvernement du Canada

Canada

Get Cyber Safe

GetCyberSafe.ca

Français | Home | Contact Us | Help | Search | canada.gc.ca

Home

Know the Risks
- Online Activities
- Common Threats
- Scams and Fraud

Protect Yourself
- Protect Your Identity
- Protect Your Money
- Protect Your Family

Protect Your Devices
- Computers, Laptops and Tablets
- Mobile Devices
- Home Networks
- Storage

Resources

Share Email

GETCYBERSAFE

Make cyber safety a personal priority with tips and resources to help protect everything that's important to you.

Search

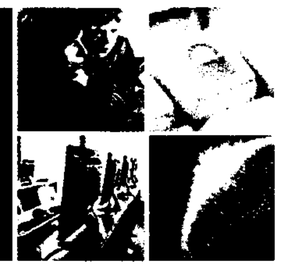
GetCyberSafe Video

See the Ad

It Happened to Me

Here's your chance to share your story and read about others' experiences. By passing along any helpful information you've

Canada-U.S. Cooperation

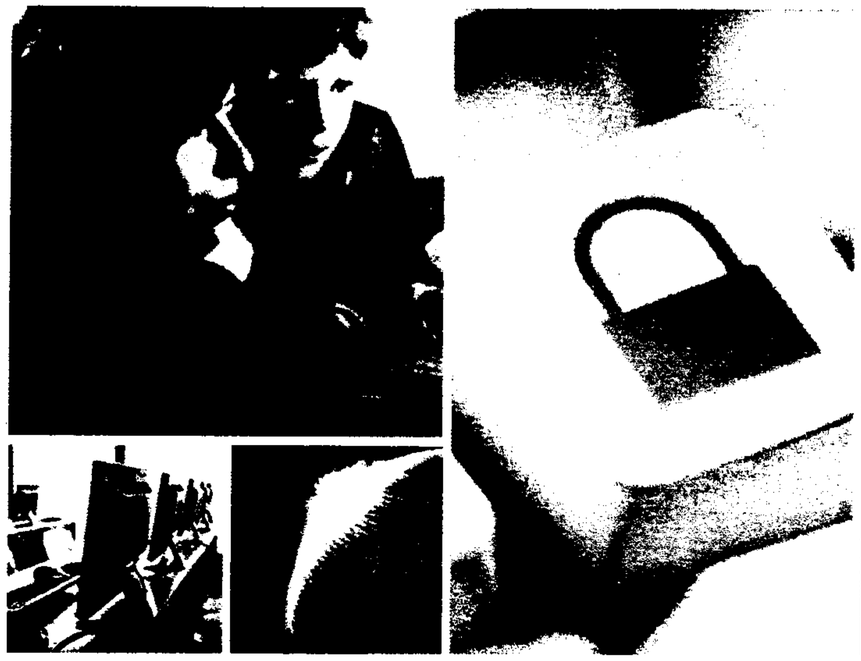


- Long history of bilateral cooperation on cyber security:
  - critical infrastructure protection;
  - operational cyber incident coordination (CERT to CERT);
  - bilateral and multi-national collaboration in exercises; and
  - intelligence and information sharing.

- Recent years have seen this accelerate and broaden through the Emergency Management Consultative Group and other mechanisms:
  - policy and program development;
  - Beyond the Border Perimeter Vision
    - collaboration through multinational fora
    - enhanced operations and private sector outreach;
  - 2+2 group of Deputies of Defence and Safety/Security; and
  - Council of Europe Convention on Cybercrime.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

Canada

Public Safety Canada | Sécurité publique Canada

Clarifying Cyber Security Roles and Responsibilities in Canada

DATE : TBD
RDIMS: 517283

Canada

Context

- Seeking clarity on the Government's roles and responsibilities in response to an existing or potential cyber security event

- Three cases:
  - Government departments responding to an event affecting Government systems (TBS lead – being revisited)
  - Government working with external partners to respond to a cyber event affecting the "whole of Canada" (PS lead – in progress)
  - Government departments jointly assisting an external entity (current question)

Roles and Responsibilities

- Roles and responsibilities of federal departments/agencies in providing external assistance are not clear
- Extent of what can be done varies with situation, malicious actors involved, and the intent of any assistance provided:
  - Addressing a threat to national security
  - Enforcing laws / pursuing an investigation
  - Preserving public safety
  - Advancing domestic economic interests
- Fact that assistance can be provided doesn't necessarily mean it is authorized or within the mandate of the department/agency involved
- Need greater clarity to inform policy on what Government's role should be

Proposed Way Forward

- PS, CSEC, CSIS, RCMP to identify and walk through various scenarios
  - Identify gaps and overlap in mandates, policies, resources
  - Clarify what gaps require policy versus legislative changes
- Scenario walkthrough / tabletop exercise

Step 2

- Walkthrough, tabletop exercises (similar to 2+2)
- Director then DG then ADM
  - Initial S&I and then broader community

Steps to Gain Clarity (Continued)

- Step 3
  - Invite P/T participation
  - Invite CI

- Considerations
  - US play and other allies
  - Information sharing
  - How would the GC handle a request for assistance from:
    - PT
    - CI
    - Industry/corporations
  - Lack of a national cyber incident response framework

UNCLASSIFIED

DATE: November 15, 2011

RDIMS No.: 517970

MEMORANDUM FOR THE DIRECTOR GENERAL

CANADIAN ELECTRICITY ASSOCIATION SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE

(For information)

ISSUE

To provide a list of discussion points to raise at the Canadian Electricity Association's (CEA) Security and Critical Infrastructure Protection (SCIP) Committee meeting. Proposed discussion points are attached at **TAB 1**.

BACKGOUND

The SCIP Committee meets quarterly in major Canadian cities to discuss common security issues affecting Canada's bulk electricity grid. Meetings are attended by Chief Security Officers (or equivalent) of utility owners and operators, and are chaired by Francis Bradley, Vice President of the CEA.

Federal officials and other external stakeholders are invited to attend a preliminary portion of the SCIP meeting to update on key areas of interest. Public Safety Canada has been engaging with the CEA in regards to critical infrastructure protection and cyber security. NCSD has been leveraging this partnership to discuss opportunities for collaboration and emerging issues, presenting at the most recent SCIP meeting on September 7, 2011 in Fredericton, NB. The report and deck are attached at **TAB 2.**

CONSIDERATIONS

NCSD participation at the September 2011 SCIP meeting was well received by Committee members, with many expressing support for a proposed 'incident response protocol.' Further, many spoke informally about a continued interest in cyber security and the desire to formalize an information sharing mechanism between the CEA and Public Safety.

As a first-step, the SCIP Committee is currently brokering the non-disclosure agreement (NDA) between the CEA and CCIRC, and will be looking to finalize the agreement at the

closed door portion of the meeting, scheduled for November 16, 2011. Robert Pitcher from CCIRC and Ben Blakely from the Independent Electricity Systems Operators (IESO) will provide an update on the NDA to the Energy and Utilities Sector Network (EUSN) on November 16, 2011. The presentation and draft NDA document are attached at **TAB 3**.

Further, Francis Bradley has been appointed the "Information Sharing Champion" for the EUSN. Through this role, Mr. Bradley has helped pen the *Critical Infrastructure Information Sharing Framework* being developed with Public Safety Canada's Critical Infrastructure Protection (CIP) Division. The sole identifiable difference with the CCIRC / CEA NDA relates to what constitutes 'shareable information,' however no contradictions are anticipated. The current version of the CI Framework is attached at **TAB 4**.

Finally, many SCIP committee members will participate in Grid-EX 2011 (notably the IESO) on November 15-17, 2011, including CCIRC, who will participate as an observer.

Sébastien Labelle
Director of Cyber Engagement and Partnerships

DISCUSSION POINT: *CCIRC Transition and Mandate Shift to Canada's National CERT.*

Given the private sector audience, this is an opportunity to highlight the transition of CCIRC from Operations to NCSD.

Speaking Points:

- I am pleased to formally announce that as part of the ongoing implementation of Canada's Cyber Security Strategy, Public Safety Canada is unifying the department's cyber security policy and operational activities into a single organization by transferring the Canadian Cyber Incident Response Centre (CCIRC) into the National Cyber Security Directorate (NCSD) effective November 14, 2011.

- This is an exciting and opportune time for this transfer to occur. CCIRC is re-focusing its activities on external stakeholders, while NCSD is leading efforts to engage at the strategic level with provinces, territories, and the private sector.

- Bringing CCIRC into NCSD will help facilitate coordination and prioritization across these activities, and will help streamline our engagement with the critical infrastructure and private sector partners, while improving our collaboration efforts with Canada's key international partners.

- This change will also allow the Government Operations Centre to focus on its mission of supporting, on behalf of the Government of Canada, response coordination of emerging and occurring events affecting the national interest such as the recent floods.

- It should be noted that your operational points of contact remain the same for both CCIRC and the Government Operations Centre, and CCIRC continues its operations as usual.

DISCUSSION POINT: *Non-Disclosure Agreement (NDA) with the Canadian Electricity Association (CEA) and the Canadian Cyber Incident Response Centre (CCIRC).*

Robert Pitcher from CCIRC, Ben Blakely from the Independent Electricity Systems Operators (IESO), and Francois Lemay from Hydro Quebec are leading the development of the NDA between CCIRC and the CEA.

s.23

The NDA has been a CCIRC operational deliverable for over a year and was scheduled to be finalized at the November 15, 2011 SCIP Committee Meeting. The NDA has been vetted [redacted]PS management in summer 2011. It meets CCIRC's overall information sharing objectives, and the initial exposure to the NDA has been met with positive feedback by CEA Members.

However, given the overlap with a *CI Information Sharing Framework* being developed by Francis Bradley (through his role as 'information sharing champion' of the Energy and Utilities Sector Network) and Public Safety's Critical Infrastructure Protection (CIP) Division (current version attached at **TAB 4**), the NDA is being revisted internally to promote consistency with other approaches and to ensure that it remains the most effective model for continued information sharing requirements, given CCIRC's refocused mandate.

It is anticipated that the current version of the NDA will likely be finalized as a 'pilot project' and to ensure continued working relationships with the CEA. However, Committee Members should understand that NCSD, CIP, CCIRC and the Department of Justice will explore options to develop a comprehensive "cyber annex" for the Information Sharing Framework.

Speaking Points:

- We are committed to facilitating information sharing between the Government our energy sector partners.
- We hope to have tools like the NDA in place in the near future.
- **(If appropriate):** We are hoping to develop a comprehensive, department-wide model that could be employed across a range of critical infrastructure sectors. It would employ similar structure and protection clauses, but would be suitable for use in a cross-sectoral context.

DISCUSSION POINT: OTHER

Development of a 'playbook' or 'incident response protocol' project with NCSD and the CEA; and improved Government of Canada information-flow to the United States / FERC.

1. *Incident Response Protocol / Point of Contact*

At the September 2011 SCIP Meeting in Fredericton, NB, NCSD presented the idea of an "incident response protocol" – or "playbook" – that was positively received by Committee Members. Many recognized the importance of having a formalized point of contact for key energy sector partners, yet expressed an unwillingness to assume a large portion of the work-load.

If this idea is revisited, NCSD could develop an informal 'questionnaire' for distribution to CEA SCIP Members that would include key organizational contact information. This could then be streamlined into a comprehensive document to be shared at the February 2012 SCIP Meeting in Calgary.

A product of this nature could contribute to the wider National Incident-Management Framework, while providing industry partners with an improved understanding of the roles and responsibilities across Government agencies and departments.

2. *Improved Government of Canada information-flow to the United States / FERC.*

The CEA has informally expressed a desire to better understand the Government of Canada's position regarding the Federal Energy Regulatory Commission (FERC).

The CEA often conducts messaging through informal channels in the US, and is hoping that Public Safety Canada or Natural Resources Canada would become the formal Government of Canada liaison to the US regarding electricity sector issues.

Summary:

1. On September 7th, 2011 NCSD attended the quarterly meeting of the Canadian Electricity Association's (CEA) Security and Infrastructure Protection (SIP) Committee in Fredericton, New Brunswick. Participants included representatives from the Canadian energy sector, Public Safety Canada (NCSD and CIPD – via teleconference) and the Integrated Terrorist Assessment Centre (ITAC).

2. Traditionally, the CEA reserves a portion of the SIP meeting for stakeholder engagement, where external partners are invited to brief committee members on priorities and other matters of interest to the electricity sector. NCSD, CIPD and ITAC each provided a brief update on Government priorities. NCSD's presentation included input from CIPD.

3. NCSD used the opportunity to profile progress under each pillar of the Cyber Security Strategy, including work with four priority sectors (telecommunications, banking, P/Ts, and energy). The presentation outlined the broad range of cybersecurity-related issues currently facing the electricity sector, but focused specifically on two areas: strengthening the incident response protocol and improving coordination and advocacy with the United States.

Report:

4. Participants were largely receptive to the proposed focus areas. Most recognized that an information-gap exists between government and industry partners, and steps should be taken to improve the relationship ("office to office rather than person to person") and develop a more advanced communication mechanism. Strong support was given for the proposed "playbook" – a document that outlines specific roles, responsibilities and contact information – as a means to improve information flow. Certain industry partners offered support in developing the document, yet recognized the challenges associated with the task. One participant noted that there was significant confusion regarding government departments and their respective mandates ("who does what?"), so a 'playbook' could be helpful to put information in context and to ensure it is being understood at the appropriate level. Many expressed a willingness to submit information in a confidential manner, provided there was a clear understanding how it would be catalogued. Participants supported suggestions to leverage existing working groups as a means to conduct "table-top" exercises in 2012.

5. However, some were curious how a strengthened incident response protocol would differ from the "information sharing" mechanism currently being developed by CCIRC and the CEA. Subsequent conversations in the margins helped clarify the difference (technical information versus incident response management), yet reinforced the need to streamline the flow of information. Participants expressed concern with "reporting fatigue", or a need to report similar information to a variety of mechanisms. There was a strong willingness to share information and improve relationships, but in a manner that was clear and consistent ("one gateway into government"), contributing to a document that would remain evergreen.

6. During the presentation, the CEA highlighted that the issue was dealt with extensively through existing F/P/T working groups. Subsequent conversations in the margins exposed a different understanding: while industry felt informed to discuss the issue internally, linking to a 'single-source' of information would be beneficial.

s.15(1) - Int'l

s.15(1) - Subv

[redacted]

7. For the most part, participants expressed a willingness to deepen the relationship between NCSD and the CEA. Many were willing to have continued government participation at the next SIP Committee meeting scheduled for November in Ottawa and offered support for the development of an 'incident response protocol'.

8. Overall, participation at the SIP Committee meeting was successful in signalling the Government's continued willingness to engage with the electricity sector on cyber security, while providing NCSD with additional insight into the Committee's perception of the subject.

Annex:

9. NCSD met with Claude Robichaud, Regional Director of Public Safety Canada's New Brunswick office. Mr. Robichaud highlighted his team's work [redacted] Mr. Robichaud indicated that his engagement with the province of New Brunswick on cybersecurity is premature; however, his [redacted] on the subject, where appropriate.

10. Industry participants at the CEA SIP Committee meeting included representatives from: NB Power, Hydro Quebec, Capital Power Corporation, Power Corporation of Canada, EPCOR, ENMAX, Ontario Power Generation, NTS Power, Sask Power, BC Hydro, IESO, and the CEA.

11. SIP Committee participants were interested in Public Safety Canada's "Cyber Awareness Month" campaign and were curious how to obtain additional information ahead of the October 1, 2011 launch-date. This request was communicated to Public Safety Canada's communications directorate.

12. PSC-CIPD provided a brief update on the National Cross Sector Forum (NCSF). The presentation highlighted the four priority areas – understanding of the issues; information-sharing mechanisms; identifying key assets and systems; and finally, recognizing interdependencies. It was noted that the NSCF can provide owners and operators with the tools required to identify critical infrastructure and key assets, and is working to establish a "portal" for CI industry to collaborate and share information.

13. Canada's Integrated Terrorist Assessment Centre (ITAC) gave a brief oral update on perceived threats to Canada's critical infrastructure. Participants expressed a desire to obtain more "sensitive" information than what is available on open source.

Public Safety Canada | Sécurité publique Canada

Public Safety Canada Cyber Security Priorities

September 6, 2011
Security and Critical Infrastructure Protection Committee
Canadian Electricity Association
Fredericton, NB

Canada

Canada's Cybersecurity Agenda:

Since the release of the Government of Canada's Cyber Security Strategy in 2010, Public Safety Canada has been working to implement the three pillars:

1. Secure Government systems
   - Shared Services Canada established to consolidate Government networks
   - Realigned the Government's cyber incident response coordination through the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre

2. Partner to secure systems outside the Government of Canada
   - Prioritized engagement with four key critical infrastructure sectors: energy (electricity), telecommunications, finance and P/Ts including the establishing of collaborative mechanisms and work-plans; raising awareness with the remaining six
   - Strengthened the Canadian Cyber Incident Response Centre's relationships and service offerings
   - Strengthening policy and operational partnerships with key allies

3. Help Canadians to be secure online
   - Preparing a nationwide communications campaign and developing partnerships for "Cyber Security Awareness Month" in October 2011

Status of Work with Four Key Sectors:

Telecommunications:

- Established the Canadian Security Telecommunications Advisory Committee (CSTAC)

Banking:

- Engaging with the Canadian banking and financial sector

P/Ts:

- Created a policy-level committee that meets semi-annually and bi-monthly via teleconference

Energy:

- Participating with the Energy and Utilities Sector Network
- Obtaining observer status to GridEX exercise
- Participate in regular Classified briefs with the energy sector
- Seeking to identify next steps

Cybersecurity and the Energy Sector

- There is a range of potential areas of collaboration with the energy sector on cybersecurity, including:
  - Information sharing and incident management
  - U.S. cyber security initiatives and legislation
  - FERC / NERC engagement
  - Control systems
  - Cyber exercises
  - Standards
  - Risk management

Existing Collaborations:

- Public Safety Canada has a strong collaborative history with Canada's energy sector
- A range of existing mechanisms at the federal, provincial / territorial and industry level are examining cybersecurity issues, such as:

Fed-Prov:

- FPT Electricity Working Group through Natural Resources Canada

Canada / US / International:

- Trilateral Meetings of P/T Regulators and P/T Energy Departments, including FERC and the US DOE (led by NRCan)

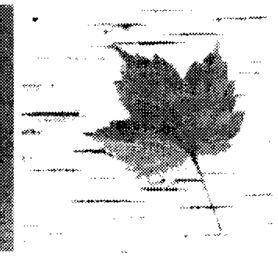
Energy and Utilities Sector:

- Energy and Utilities Sector Network (eg. CEA / CCIRC information sharing and mutual services)
- Classified Briefings to the Energy Sector

Canadian Electricity Association:

- Security and Critical Infrastructure Protection Committee
- Regulator Development Task Group
- Cyber Security Task Force / Smart Grid Task Force

Proposed Focus Areas:



Strengthen coordination and advocacy with the US:

- Share information on any proposed future US legislation or standards, e.g. the GRID Act, FERC standards/directives
- Collaborate to develop common positions and strategize on how to advance them

Strengthening Incident Response Protocol:

- Identify and conduct security and gap analyses
- Clarify roles, responsibilities and protocols to improve incident management and response to a cyber incident
- Create a "playbook," outlining responsibilities and contact information

Next Steps:

- For discussion today:
  - What:
    - Confirm whether these are the focus areas
  - How:
    - What is the ideal discussion forum?
  - Who:
    - Broad participation or specialized representation?
      - NRCan? P/Ts?
    - Secretariat, co-chairs, "champion"?
  - When:
    - Collectively, what can we accomplish by March 2012?
    - Can we conduct table-top exercises in 2012?

SECRET – with attachments

ADM Cyber

November 16, 2011
15:00 to 16:00

Boardroom 17B-2000
269 Laurier Avenue West

For your meeting with:
ADM Cyber
On:
November 16, 2011, 15:00-16:00

SECRET – with attachments

DATE:

File No.: 383300
RDIMS No.: Dragon 796

MEMORANDUM FOR THE ASSISTANT DEPUTY MINISTER

MEETING OF THE ASSISTANT DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

(Information only)

ISSUE

You will chair a meeting of the Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber) on November 16, 2011, from 15:00 to 16:00 in boardroom 17B-2000 at 269 Laurier Avenue West.

Melanie Mohammed, Policy Analyst, National Cyber Security Directorate (NCSD), will be present to take notes.

BACKGROUND

ADM Cyber last met in August 2010 prior to the October 2010 launch of *Canada's Cyber Security Strategy*. The Committee was then scheduled to meet in June 2011; however, due to schedule conflicts, the meeting was cancelled.

The November 16, 2011 meeting will provide an opportunity for departments and agencies to give an update on their progress achieved to date in terms of cyber security, and to discuss challenges and obstacles they have encountered.

Most importantly, however, you will be debriefing participants on the outcome of the November 8, 2011 meeting of the National Security Advisor with the Deputy Ministers of the Canadian Security Intelligence Service, the Communications Security Establishment Canada (CSEC), the Department of National Defence, and Public Safety. You will also speak to the creation of the Deputy Ministers Committee on Cyber Security (DM Cyber), which is currently scheduled to hold its inaugural meeting in early December 2011.

.../2

s.15(1) - Int'l

CURRENT STATUS

There are seven items on the agenda. s.15(1) - Subv

Item	1. Opening Remarks
Purpose	Information
Your role	Lead
Desired outcome	– Welcome members to the meeting. – Speak to the recent integration of the Canadian Cyber Incident Response Centre (CCIRC) with the National Cyber Security Directorate. – Inform that Windy Anderson is new Director, CCIRC.
Additional documents	– Proposed talking points (**TAB 1**)

Item	2. Quintet debrief
Purpose	Information
Your role	Turn to Don Piragoff, Senior Assistant Deputy Minister of the Policy Sector, Department of Justice Canada.
Desired outcome	– Debrief on July 2011 Quintet meeting. – [redacted]
Additional documents	– Proposed talking points and briefing note (**TAB 2**)

Item	3. London International Conference on Cyberspace [redacted]
Purpose	Information
Your role	Lead discussion
Desired outcome	– Debrief on London Conference. – Determine how to support Hungary next year. – Propose ways to increase participation, under Public Safety Canada lead. – [redacted]
Additional documents	– Proposed talking points (**TAB 3**) – Key Take Aways document, Chair's Statement, and Closing Remarks (**Annex to TAB 3**)

Item	4. Debrief of November 8, 2011 Deputies meeting
Purpose	Information
Your role	Lead
Desired outcome	– Debrief on Deputies meeting.
Additional documents	– Proposed talking points (**TAB 4**)

.../3

Item	5. Follow-up on November 8, 2011 Deputies meeting
Purpose	Information
Your role	Lead, except on Network hygiene item (Treasury Board Secretariat)
Desired outcome	– Determine how to address the three main issues raised by Deputies at the meeting: • Network hygiene – Treasury Board Secretariat lead. Seek a way forward on how best to advise Deputies; • Roles and responsibilities – Public Safety Canada lead. Directors General Committee on Cyber Security (DG Cyber) prepared a deck that shows mandates with respect to cyber security. **Determine if this can be used as a tool to provide clarity to Deputies**; and • Deputy Ministers Committee on Cyber Security (DM Cyber) – Public Safety Canada lead. Review and seek consensus on terms of reference and membership.
Additional documents	– Proposed talking points and briefing note, where applicable • Network hygiene (**TAB 5A**) • Roles and responsibilities (**TAB 5B**) • DM Cyber (**TAB 5C**) – [redacted] – DG Cyber roles and responsibilities deck (**Annex to TAB 5B**) – Draft Terms of Reference for DM Cyber (**Annex to TAB 5C**)

Item	6. Disclosure map
Purpose	Information
Your role	Introduce Robert Dick, Director General, National Cyber Security Directorate, as lead
Desired outcome	– [redacted]
Additional documents	– [redacted]

Item	7. Roundtable

.../4

Purpose	Information
Your role	Lead
Desired outcome	–
Additional documents	– Proposed talking points (**TAB 7**) – Briefing note (**Annex to TAB 7**)

CONCLUSION

You should close the meeting by noting that ADM Cyber will reconvene prior to the inaugural meeting of DM Cyber in December 2011, and will assume a regular monthly schedule in 2012.

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Melanie Mohammed, Policy Analyst, NCSD, at 613-991-2700.

Robert Dick
Director General
National Cyber Security Directorate

Enclosure: (1)

Public Safety Canada / Sécurité publique Canada

MEETING PARTICIPANTS - PS

PARTICIPANTS À LA RÉUNION - SP

DATE : ➲ **NOVEMBER 16, 2011 ADM CYBER**	**CONTACT PERSON - PERSONNE RESSOURCE :** ➲ **CARMEN VOGHEL OR RUBA PIASKO**
TIME - HEURE : ➲ **3:00**	**TELEPHONE No - N° DE TÉLÉPHONE :** ➲ **991-7025 OR 991-2901**
ROOM - SALLE : ➲ **17th floor, 17B2000**	**DIVISION & SECTION :** ➲ **NS**

	PASS NUMBER NUMÉRO DU LAISSEZ-PASSER	NAMES OF GUESTS LISTE DE NOMS DES INVITÉS	DEPARTMENT/COMPANY MINISTÈRE/ENTREPRISE
	✓	[redacted]	CSE
	✓		CSE
	✓		CSIS
	✓	**STEVEN NOONAN for J. TURNER**	DND
	✓	**JIM JUNKE for K. BUCK & K. CHRISTIE**	DFAIT
	✓	**ANDREW VALLERAND for M. FORTIN**	DRDC
	DECLINED	**CHRIS FORBES**	FIN
		HELEN McDONALD	IC
	✓	**MICHAEL DUFFY for D. THERRIEN**	JUSTICE
	✓	**LUCIE ANGERS for D. PIRAGOF**	JUSTICE
	✓	**RENNIE MARCOUX**	PCO
	DECLINED	**BARBARA GLOVER**	PWGSC
		JIRKA DANEK for M.CHÉNIER	PWGSC
	✓	**ANTOINE BABINSKY**	RCMP
	✓	**MICHEL POULIN for J. OSSOWSKI**	TBS
	DECLINED	**CORINNE CHARETTE**	TBS
	✓	**PIERRE BOUCHER**	TBS
	✓	**LYNDA CLAIRMONT**	
	✓	**ANDREW HANAN for S. DURAND**	
	✓	**ROBERT DICK**	
	✓	**BOB GORDON**	

SIGNATURE: ➲	Date:

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED
s.15(1) - Subv

ADM Cyber Meeting

November 16, 2011 – 15:00 to 16:00
Boardroom 17B-2000, 269 Laurier Avenue West

AGENDA

	Time		Presenter	Type of Document
1	15:00 *5 min*	Opening remarks	L. Clairmont, PS	N/A
2	15:05 *10 min*	Quintet debrief	D. Piragoff, JUS	N/A
3	15:15 *10 min*	London International Cyber Conference [redacted]	L. Clairmont, PS	Key Take Aways; Chair's Summary; and Closing Remarks included in meeting invitation
4	15:25 *5 min*	Debrief of November 8, 2011 Deputies meeting	L. Clairmont, PS	N/A
5	15:30 *10 min*	Follow-up on Deputies meeting a. Network hygiene b. Roles and responsibilities c. DM Cyber: Terms of Reference and membership	L.Clairmont, PS	Documents will be distributed at the meeting
6	15:40 *10 min*	[redacted]	L. Clairmont, PS	[redacted]
7	15:50 *10 min*	Roundtable	All	N/A

Dragon: PS-SP-#524339-v1-ADM_Cyber_-_2011-11-14_-_Agenda

Sécurité publique Canada | Public Safety Canada

NON-CLASSIFIÉ

s.15(1) - Int'l

s.15(1) - Subv

SMA sur la cybersécurité

Le 16 novembre 2011 – 15h00 à 16h00
Salle de conférence 17B-2000, 269, avenue Laurier ouest

ORDRE DU JOUR

		Sujet	Responsable	Documents connexes
1	15h00 *5 min*	Mot de bienvenue	L. Clairmont, SP	S/O
2	15h05 *10 min*	Compte rendu sur Quintet	D. Piragoff, JUS	S/O
3	15h15 *10 min*	Conférence internationale sur le cyberespace à Londres [redacted]	L. Clairmont, SP	Points clés; résumé du président; et observation finale joints dans l'invitation à la réunion
4	15h25 *5 min*	Compte rendu sur la réunion des sous-ministres du 8 novembre 2011	L. Clairmont, SP	S/O
5	15h30 *10 min*	Suivi de la réunion des sous-ministres a. Hygiène des réseaux b. Rôles et responsabilités c. SM sur la cybersécurité : mandat et participants	L. Clairmont, SP	Les documents nécessaires seront distribués à la réunion
6	15h40 *10 min*	[redacted]	L. Clairmont, SP	[redacted]
7	15h50 *10 min*	Tour de table	Tous/Toutes	S/O

Dragon: PS-SP-#524339-v1-ADM_Cyber_-_2011-11-14_-_Agenda

TAB 1

1. OPENING REMARKS

- Bonjour tout le monde, et bienvenue à la réunion.
  - *Good afternoon everyone, and welcome to the meeting.*

- We have several important items to discuss today, but only one hour in which to address them, so we will have to focus our discussion.

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

- The main purpose of today's meeting is to hear from colleagues at the Department of Justice Canada who are leading the upcoming Quintet meeting; debrief on the London Conference [redacted] and debrief and discuss next steps coming out of the November 8, 2011 Deputies meeting with the National Security Advisor.

- First, though, I would like to announce that the Canadian Cyber Incident Response Centre (CCIRC) has joined the National Cyber Security Directorate, unifying all Public Safety Canada cyber activities and allowing better leveraging of respective capabilities, and easing external engagement on cyber.

- Windy Anderson is the new Director of CCIRC.

s.14 •

TAB 2

s.15(1) - Int'l

s.15(1) - Subv

UNCLASSIFIED

2. QUINTET

PROPOSED TALKING POINTS

- Turn to Don Piragoff from the Department of Justice to speak to us regarding the July 2011 Quintet of Attorneys General meeting, as well as preparations that are currently underway for the 2012 Quintet, which is being hosted by Canada.

[redacted]

[redacted]

ISSUE

[redacted]

BACKGROUND

Canada will be hosting the next Quintet meeting in early 2012.

[redacted]

Prepared by: Melanie Mohammed

TAB 3

s.15(1) - Int'l

UNCLASSIFIED

s.15(1) - Subv

3. LONDON INTERNATIONAL CONFERENCE ON CYBERSPACE

PROPOSED TALKING POINTS

- The London International Conference on Cyberspace took place from November 1-2, 2011.

- I led the Canadian delegation, which included:
  - Lucie Angers, General Counsel in External Relations at the Department of Justice Canada;
  - Elissa Golberg, Ambassador and Permanent Representative to the United Nations and Conference on Disarmament;
  - Bob Gordon, my Special Advisor on Cyber Security;
  - Rennie Marcoux, Assistant Secretary to the Cabinet of Security and Intelligence at the Privy Council Office; and
  - Helen McDonald, Assistant Deputy Minister of Spectrum, Information Technology and Telecommunications at Industry Canada.

- 60 countries participated in the Conference.

- Southern Africa and southeastern Asia had limited to no participation.

- All sessions were televised, and will be uploaded to website of the United Kingdom Foreign Secretary.

- One to note is from Al-Jazeera Talk. The speaker provided a very different take on the Internet and the role of the government in governing cyberspace.

s.15(1) - Int'l

s.15(1) - Subv

UNCLASSIFIED

[redacted]

- The overall sentiment is that the Conference was a success. Canada's objectives were met.

- At the end of the Conference, the United Kingdom Foreign Secretary summarized the proceedings and highlighted that most, if not all, delegates seemed to agree on the following:
    - improving cyber security must not come at the expense of human rights;
    - cyberspace must remain open to innovation, the free flow of ideas, information, and expression;
    - governments must act proportionately in cyberspace, and should continue to comply with existing rules of international law and the traditional norms of behaviour that govern interstate relations;
    - actions unacceptable offline are unacceptable online; and
    - the multi-stakeholder model of cyberspace governance is critical to sustaining innovation and interoperability.

- Questions that were raised were mostly regarding the connection between governments and private sector.

- Hungary will chair 2012 conference, and South Korea will chair in 2013.

- We spoke a lot regarding next year's Conference. How do we support Hungary next year? How can we increase participation? How do we keep the momentum going post-London?

-

s.15(1) - Int'l

s.15(1) - Subv

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

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

- The dialogue presented an alternative way forward to counter proposals for creating an international treaty to govern cyberspace. [redacted]

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

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

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

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

more to prevent cyber crime for example through more secure devices, systems and services.

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

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

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

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

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

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

London Conference on Cyberspace: Chair's statement

02 November 2011

Full text of the Chair's statement from the London Conference on Cyberspace.

Governments, business and representatives of civil society met in London on 1-2 November 2011 to discuss the vital issues posed for us all by a networked world connected ever more closely together in cyberspace.

The advent and development of the Internet is transforming our world and revolutionising our everyday lives. The Internet can drive equitable and sustainable growth. It gives access to knowledge and the exchange of ideas. It nurtures innovation and investment. It improves opportunities for participation in social and economic activities for those on the margins. But the rise of the networked world has also produced significant challenges which could undermine these benefits and pose a serious threat to reaping the full potential of cyberspace. This affects us all. A secure, safe digital environment cannot be developed by governments alone. A safe and resilient cyberspace must be shaped by the interests of civil society, industry and governments across the globe. In tackling the threats, we must not allow improved security to come at the expense of fundamental human rights.

Earlier this year I proposed the following principles for governing behaviour in cyberspace, and called for a more focussed and inclusive dialogue between all those with a stake in the Internet – civil society and industry as well as governments - on how we might implement them:

1. The need for governments to act proportionately in cyberspace and in accordance with national and international law;
2. The need for everyone to have the ability – in terms of skills, technology, confidence and opportunity – to access cyberspace;
3. The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas;

4. Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and expression;
5. The need to respect individual rights of privacy and to provide proper protection to intellectual property;
6. The need for us all to work collectively to tackle the threat from criminals acting online; and
7. The promotion of a competitive environment which ensures a fair return on investment in network, services and content.

The London Conference on Cyberspace began this more focussed dialogue on principles and set out an agenda for further work. The success of this agenda will be founded on the set of partnerships we have explored at this Conference. Our starting point must build on existing work, including the Geneva and Tunis World Summits on the Information Society. Our partnerships must remain inclusive, co-operative and collaborative to make certain we can build a secure, resilient and trusted global digital environment. This work will now go forward over the next 24 months with conferences in 2012 and 2013, graciously hosted by Hungary and South Korea respectively, to take stock.

The Conference

The London Conference brought together Ministers, senior government officials, industry leaders, and representatives of the Internet technical community and civil society. In all, more than 700 participants from 60 countries took part.

Opening addresses were made by the Prime Minister of the United Kingdom, David Cameron; Vice President Joseph Biden of the United States; Carl Bildt, Foreign Minister of Sweden; Sachin Pilot, Communications Minister of India; Helen Clark, Administrator of the United Nations Development Programme; Jimmy Wales the founder of Wikipedia; Atiaf Alwazir, Yemeni activist and researcher; Lord (Richard) Allen of Facebook UK; and Eric Van der Kleij, CEO of Tech City UK.

President Toomas Ilves of Estonia spoke, and representatives from many other governments and the European Union. There were speakers from civil society and think tanks. The Conference heard from the information and communications industry and from many other companies. Altogether over 100 businesses were represented. International organisations such as the United Nations Development Programme (UNDP) and the International Telecommunications Union (ITU) also spoke. A full list of those who contributed is at Annex A.

Parallel to the main sessions, many workshops, fora, dynamic coalition meetings and breakout sessions were held. A youth conference ran alongside, bringing in the views of young people who are driving the digital revolution. The key conclusions of these London Cyber Youth sessions are captured in Annex B.

Meanwhile as is fitting in a conference on cyberspace, technology allowed not just those in the room to take part. Besides contributions from those present, input and views were gathered from citizens right across the world through the Web. Panellists took questions direct from the public through the Internet. The event was livestreamed and real-time updates put out through Twitter.

The Conference themes

The London Conference focussed on five topics:

- Economic growth and development, covering such questions as:

How to realise the benefits of a secure cyberspace for international economic growth and development?
Is Cyberspace a prosperity multiplier?
How to strike a balance between protection of intellectual property and access, innovation and creation of markets?
How to ensure transparency and predictability of regulatory and fiscal regimes, and their ability to adapt to fast-changing technologies?
Government regulation and industry self-regulation – what are the ways forward?
How can problems between states be prevented and managed?

- Social benefits, covering such issues as:

How can we maximise knowledge empowerment and the potential gains for government service delivery?
What more can be done to enhance democratic accountability and freedom of expression?
How can governments engage to best effect?
What more can be done to deal with the negative social aspects?

- Safe and reliable access, covering such questions as:

How to assure safe and reliable access to cyberspace?
How best to promote public risk-awareness and education in safe and secure online behaviour (particularly for vulnerable groups)?
How to ensure lawful access for individuals without discrimination or interference, while protecting against abuse?

- International security, covering such questions as:

How can problems between states be prevented and mitigated?
What lessons can be learned from other areas of international security and conflict prevention work?
How do we develop and apply appropriate principles of behaviour?
What are the most appropriate fora to take the debate forward?

- Cyber crime, covering such questions as:

What are the responsibilities for individuals, the private sector and government for preventing cybercrime?
How do we ensure that all countries have equivalent legislation to allow them to tackle cyber crime domestically, and support international working?
How do we secure the right level of investment in the right areas?
What more should Internet intermediaries do to address the spreading of malware and botnets over their networks?
How do we create the right incentives to build improved and cost-effective security into the design of devices, systems and services?
What role do industry standards have to play and what would they look like?

Questions were posed directly by members of the public to the Conference, while sessions were in progress, using Facebook and Twitter. Against each theme the following conclusions were reached and points made.

Economic growth and development

All delegates agreed that the Internet has a critical role to play as an engine and facilitator of economic growth, especially in the developing world.

The conference agreed that to achieve the broadest and deepest possible benefits to growth from cyberspace, access, in terms of both physical infrastructure and training and skills, must be broadened so the widest possible group of people can share what it has to offer.

Delegates agreed that cyberspace must be secure and reliable so that it is trusted as a medium for doing business, and innovators and content providers are confident their discoveries will be appropriately protected to encourage investment. There was strong support for the principle that in the cyber market we must promote a competitive environment which enables a fair return on investment in network, services and content.

At the same time speakers called for cyberspace to be free from government and commercial censorship, consistent with international legal obligations, so that the

free availability of information can drive strong incentives for the highest standards of accountability and national governance.

Delegates called for cyberspace itself to have the latitude to evolve and innovate naturally to create new opportunities and benefits in the future. This was also a strong theme of the online debate running alongside the Conference. There was general support for free and fair competition through transparent policy making, standards development and regulatory processes.

Delegates called for the removal of unnecessary barriers to trade in cyberspace. Only then will the full benefits of online cross border trade and globalisation be realised.

The Conference recognised existing work on the Internet and growth, such as the Organisation for Economic Co-operation and Development (OECD) Principles for Internet Policy Making agreed in June 2011 and work in the Council of Europe, ASEAN, APEC and other organisations, including private sector initiatives such as the development of principles for User Generated Content. Focus should be on building upon existing work, rather than revisiting discussions or creating new institutions.

The Conference strongly welcomed the role the Internet can play in giving the unheard a voice, improving access to education and healthcare, reducing poverty, and driving progress towards the Millennium Development Goals. Delegates called on developing countries, the private sector, donors and international development organisations to work together to ensure we harness the Internet's economic and social dividends.

The Conference called for global efforts to close the digital divide through the provision of development support on ICT. The goal must be to ensure the Internet is increasingly accessible, affordable, safe and reliable, so as to drive equitable and sustainable economic growth. Delegates expressed support for the objective of, and the work being taken forward by, the ITU/UNESCO Broadband Commission in seeking to increase access to broadband communication in the developing world. The key was promotion of open and competitive markets.

In developing existing work such as the OECD Principles, many delegates agreed it is critical that all those with an interest are engaged – business and civil society as well as governments, and from developing as well as developed countries. Only in this way will the interconnectedness of the Internet be properly reflected. The goal of further development of policy-making principles in this context should be to help promote and protect the global free flow of information, ideas and expression, to encourage investment and entrepreneurism, and help the development of cross border services.

Social benefits

On the theme of social benefits, all delegates reaffirmed the overwhelmingly positive and transformative benefits that the Internet has brought to citizens, societies and governments.

Many speakers in particular welcomed its contribution (especially through social media) to freedom of expression and association, and its ability to expose human rights abuses as they happen and give the unheard a voice. In bringing citizens and governments closer together, the Internet is a powerful engine for empowering citizens and driving government accountability.

Speakers emphasised the particular importance of engagement with the youth community, both in giving them a voice in the democratic process, and being more receptive to their ideas in the development of policy.

The conference agreed that efforts to improve cyber security must not be at the expense of human rights. There was overwhelming support for the principle that cyberspace must remain open to innovation and the free flow of ideas, information and expression. Many speakers affirmed their belief that rights to freedom of expression and association apply with equal force in cyber space, and stressed the imperative for governments to comply with their obligations and commitments in this area as set out in the Universal Declaration of Human Rights. Speakers stressed that capitalising on the full benefits of cyber space and protecting freedoms needs the participation of not just governments but also business and civil society. Given the speed of technological advance, speakers thought that the best foundation, and the one which best reflected the dynamic of the Internet itself, was a transparent and stable framework of self regulation.

There was strong support for the principle that users of cyberspace should show tolerance and respect for diversity of language, culture and ideas; but delegates said that protecting this principle must not be used as a cloak for attempts to subvert the right to freedom of expression and association, or become an excuse for fragmentation of the Internet. Speakers also expressed concern that some states may use notions of sovereignty as a guise to restrict access, block websites and censor Internet content.

Delegates (and many of those commenting as part of the online debate around the Conference) emphasised the need for transparent and interoperable approaches to handling privacy and data protection issues which recognise the requirement for global trade but also the importance of protecting personal information.

The Conference acknowledged the need to continue efforts to bridge the 'digital divide' and work towards the achievement of Millennium Development Goals. The work of the ITU/UNESCO Broadband Commission on capacity development and extending access was noted under this theme.

International Security

Government representatives discussed under this theme how best to prevent or mitigate potential problems between states on cyber issues.

All delegates underlined the importance of the principle that governments act proportionately in cyberspace and that states should continue to comply with existing rules of international law and the traditional norms of behaviour that govern interstate relations, the use of force and armed conflict, including the settlement by states of their international disputes by peaceful means in such a manner that international peace, security and justice are not endangered.

All speakers agreed that stronger co-operation and collaboration was needed to build confidence and to avoid misunderstandings.

All delegates agreed that the immediate next steps must be to take practical measures to develop shared understanding and agree common approaches and confidence-building measures through the UN Group of Government Experts and through the OSCE and other regional organisations. Some delegates noted the draft Code of Conduct circulated at the United Nations. There was no appetite at this stage to expend effort on legally-binding international instruments.

There was strong support for the recommendations of the 2010 UN Group of Government Experts on further dialogue among states to discuss norms pertaining to state use of information and communication technologies to reduce collective risk and protect critical national and international infrastructure.

Delegates welcomed the work the OSCE is also doing to develop specific confidence-building measures applicable in cyber space, and called on other regional organisations to develop their own work alongside the OSCE on this question.

Tackling cyber crime

The conference identified cyber crime as a significant threat to economic and social well-being, and one which requires a concerted and urgent international effort. As online criminals operate across national borders, all delegates strongly supported the principle that we must work collectively together to tackle the threat from cybercrime and ensure there are no safe havens for cyber criminals. There was strong support from delegates for the guiding principle that what is unacceptable offline is also unacceptable online. As was pointed out in the London Cyber Youth sessions, for young people the online and offline worlds are one place.

Many countries and regional bodies are already taking positive steps towards

implementing cyber crime legislation, but the need to ensure that these were compatible internationally was recognised.

There was general support for the principles for fighting online crime that are set out in the Budapest Convention on Cybercrime. Some delegates raised problems with the Convention. But there was little support for negotiating a new instrument. The Convention's usefulness as a framework on which nations could build to achieve better international co-operation was recognised by many speakers. Many delegates encouraged countries to look at whether they could sign up to the Budapest Convention, seeing the Convention as the best form of international agreement in this area. Some delegates expressed their support for the Commonwealth work on a cyber crime Model Law as a useful stepping stone.

Delegates noted that while having the right legislation in place was essential, this must also be supported by a willingness to act when called upon. In addition to legislation, countries were encouraged to ensure they have the forensic resources, processes and willingness to co-operate as necessary.

There was very strong support from many delegates for practical collaboration and capacity development on cross-border law enforcement, to take place at a rapid pace that reflects the reality of the networked world.

Speakers pointed to the network of law enforcement contact points known as the "24/7 Network" as the best means to make sure that when urgent assistance is required, partner countries are able to obtain it. Delegates called on all countries to join the 24/7 Network and to redouble efforts and commitment to make it a success.

As well as law enforcement and cross-border co-operation, the debate noted prevention as being central to tackling cyber crime. There was general agreement that all sectors - private companies and individuals as well as governments and law enforcement agencies – have responsibilities in preventing cyber crime.

Delegates in the room and those commenting online all thought government and industry had a shared responsibility to do more to prevent cyber crime, in industry's case for example through more secure devices, systems and services. Industry must be a part of the solution on prevention. There was general support for the view that the public and businesses should get more help to able to identify easily products that have good security. Delegates encouraged the private sector to lead development of improved Internet security products, systems, services and standards in cyberspace, and to make the market easier to navigate for consumers.

Speakers noted that all Governments are currently looking to place more services online, and that many are considering outsourcing to cloud computing. It was

agreed that governments need to lead by example, and that when governments procure and provide online services, security is one of the key criteria.

Ensuring safe and reliable access

There was general agreement that global interoperability and resilience underpin the economic and social benefits of the Internet and that governments, industry and civil society must work together to preserve and enhance them. In this context, there was recognition of the important role played by ICANN. There was a call for all those with an interest to get involved in the normal three-yearly ICANN public meetings.

There was also widespread support for the excellent work being taken forward by the Internet Governance Forum. Delegates pointed to the Forum as a demonstration of the clear value of involving participants from private sector and civil society in discussing issues of Internet public policy.

There was recognition of the private sector's central role in delivering the security, safety, resilience and reliability of cyberspace, through continued collaboration between all participants, and through the development of appropriate international standards in the appropriate international fora.

Delegates believed governments have a responsibility, working with the private sector, to ensure an open Internet that allows individuals access to content and services with only such restrictions as are permitted under international legal obligations, while protecting users (especially children) against abuse.

Speakers emphasised that the private sector is central to the roll-out of broadband. The necessary innovation and investment can be facilitated or inhibited by governments' actions. Delegates called on governments to take an appropriate and proportionate interest in improving the safety and reliability of cyberspace, while recognising that the expertise lies with industry partners.

Speakers emphasised that the private sector is central to the roll-out of broadband. The necessary innovation and investment can be facilitated or inhibited by governments' actions. Many speakers thought that governments should encourage self-regulatory mechanisms for the private sector, rather than start with legislation and regulation.

Service providers and suppliers talked of their commitment to ensuring their continued reliability and availability of systems. Delegates called on industry to lead the creation and maintenance of open standards being mindful of the challenges to information access. There was support for a strong private sector-led strand to the work which would now take place leading up to the next conference in Budapest in 2012.

There was general support for Computer Emergency Response Teams (CERTs) co-operating regionally and internationally and a call for these to cover public and private sector alike.

Delegates inside the room and those commenting as part of the online debate all agreed that the Internet must remain a single undivided network, with engagement from all to ensure that safe and reliable access is something on which we can all count.

Altogether, delegates welcomed the fact that debate at this London Conference had been wide-ranging, constructive, and based on partnership, with representatives from industry and civil society as well as governments participating. Delegates looked forward to continuing work on these issues, and to the next conference in Hungary in 2012, building on a shared vision of a safe, secure, resilient and open cyberspace.

Speakers at the London Conference on Cyberspace

Helen Clark, Administrator, United Nations Development Programme
Carl Bildt, Minister for Foreign Affairs, Sweden
Jimmy Wales, founder of Wikipedia
Atiaf Alwazir, Yemeni activist and researcher
Sachin Pilot, Minister of Communications, India
Lord Richard Allan, Director of Policy for Europe, Middle East and Africa, Facebook
Eric Van der Kleij, Chief Executive Officer, Tech City UK
Joseph Biden, Vice President of the United States of America
Igor Shchogolev, Minister of Communications and Mass Media, Russia
Dong-Seok Min, Vice Minister of Foreign Affairs, Republic of Korea
Sanjay Pradhan, Vice President World Bank Institute
Uri Rosenthal, Minister of Foreign Affairs, Netherlands
James Manyika, Director and Senior Partner, McKinsey & Company
Mikhail Yakushev, Chairman, Russian Association of Electronic Communications
Yu Zhou, Vice President, Tudou.com
President Toomas Ilves of Estonia
Neelie Kroes, Vice President and European Commissioner for the Digital Agenda, European Commission
Patrick Spence, Managing Director, Global Sales and Regional Marketing, Research in Motion
Helen Margetts, Director, Oxford Internet Institute
Speranza Ndege, Director of the Institute of Open, Distance and e-Learning, Kenyatta University
Cornelia Rogall-Grothe, State Secretary, Federal Ministry of the Interior and Federal Government Commissioner for Information Technology, Germany

Asoke Kumar Mukerji, Additional Secretary, Ministry of External Affairs, India
Andrei Krutskikh, Deputy Head, Department of New Threats and Challenges, Ministry of Foreign Affairs, Russian Federation
Patrick Pailloux, Director General, Network and Information Security Agency, France
Nils Melzer, Research Director of the Competence Centre for Human Rights, University of Zurich
Lee Hyun-Ju, Ambassador for International Security Affairs, Ministry of Foreign Affairs and Trade, Republic of Korea
Howard Schmidt, Cybersecurity Co-ordinator, White House, USA
Matthew Kirk, Group External Affairs Director, Vodafone
Erik Akerboom, National Coordinator Counter Terrorism and Security, Netherlands and President Cyber Security Council, Netherlands
Harry van Dorenmalen, Chief Executive Officer Europe, IBM, and member Cyber Security Council, Netherlands
Scott Charney, Corporate Vice President, Trustworthy Computing Group, Microsoft
Eugene Kaspersky, Chief Executive Officer, Kaspersky Lab
Athalia Molokomme, Attorney General for Botswana
Peter Davies,Chief Executive Officer, Child Exploitation and Online Protection Centre (CEOP)
Hyeon Yu, Cybercrime Investigation Professor, Korea Police Investigation Academy
Hamadoun Touré, Secretary General, International Telecommunication Union
Olivia Garfield, Chief Executive Officer, Openreach
Chen Lifang, Senior Corporate Vice President, Huawei
Roger Wilkins, Secretary General, Attorney General's Department, Government of Australia
Rod Beckstrom, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers (ICANN)

LondonCyber Interactive

Barbora Bukovská, Senior Director, Law and Policy, ARTICLE 19
John Kampfner, Chief Executive, Index on Censorship
Tom Ilube, Managing Director, Consumer Markets, CallCredit
Atiaf Alwazir, Yemeni activist and researcher
Hannan Ezzat, Regional Director for Marketing and Communications for Middle East and North Africa, British Council, Cairo
William Echikson, Head, Free Expression in Europe, Middle East and North Africa, Google
Marco Gercke, Cybercrime Research Institute, Cologne
Alexander Seger, Secretary, Cybercrime Convention Committee, Council of Europe, Strasbourg

Zahid Jamil, Legal Expert, Commonwealth Cyber Crime Initiative, Karachi
Barbara Stocking, Chief Executive, Oxfam
Sarah Jordan, Head, Digital Communications, Oxfam
Christèle Delbé, Head of Sustainability, Vodafone
Helen Clark, Administrator, United Nations Development Programme
Mark Graham, Research Fellow, Oxford Internet Institute
Charlie McMurdie, Detective Superintendent, Police Central eCrime Unit, Metropolitan Police Service
Simon Tee, Senior Performance Manager, Specialist Crime Directorate
Steve Mortimore, Assistant Chief Constable, Policing Policy and Practice Service
Director, National Policing Improvement Agency
Greg Day, EMEA Security, CTO and Director of Security Strategy, Symantec
Lee Miles, Cyber Head, Serious Organised Crime Agency (SOCA)
Peter Davies, Chief Executive Officer, Child Exploitation and Online Protection Centre (CEOP)
Sonia Livingstone, Professor of Social Psychology, LSE, and Director, EU Kids Online
Mike Galvin, Managing Director, Next Generation Access, Openreach
Andrew Flanagan, NSPCC
Niketa Sanderson, Ambassador, NSPCC
David Pollington, Director of International Security Relations, Microsoft
Robert Marcus, Chief Executive Officer, Quantumwave Capital
Jeff Peel, Managing Director, Quadra Consulting
Owen Pengelly, Office of Cyber Security and Information Assurance, Cabinet Office
Mark Harris, Global Vice President for Labs, Sophos Ltd
Andrew Rogoyski, Chair of the Intellect Cyber Group, Roke Manor
Kevin Jones, Director IS, ADS
William Beer, PriceWaterhouseCoopers UK
Thomas Buchanan, PriceWaterhouseCoopers UK
Ed Gibson, PriceWaterhouseCoopers USA

LONDON CYBER YOUTH

A diverse group of young people from different parts of the UK took part in the Youth Forum, a parallel series of debates intended to feed into the conference debates and conclusions.

The Youth Forum covered the following issues:

The Future of Technology and Development opportunities

Young people at the LondonCyber Youth Forum were asked to think about the next generation of the internet and associated technology. Their future gazing covered:

The use of cloud technology to make access to information more democratic and more affordable for developing countries
The continued development of the social network into a hub that collects the best of the web, safely and supported.
Increased coming together of different devices and the use of smart tech to merge virtual and real life closer together
TV becoming more interactive and using internet technology to make TV watching more social

Economic growth and development

Young people recognise that the digital world is central to economic growth and can be a driver of economies in developing countries but that it is overlaid with social factors which need to be learnt from an early age in school. They believe the internet should be an intrinsic part of citizenship skills so that you learn that everything from safety to privacy at an early age.

- Some of us who have visited developing countries have Seen the power of the internet in changing the lives of communities but we all have a responsibilities to help them afford the new technologies. We think of the internet as a global phenomenon but large parts of the world still don't have access to the digital revolution

- It seems that the newspaper industry is dying but this creates issues of reliability of information as it is much harder to know what we are reading is true and we are concerned about the power of governments to close down internet access. There is a human right to assembly in the real world and this should exist online as well.

- Young people are drivers of the economy and yet there is no consistency in what you can have access to at different ages. Being able to access to material is not just about age its about emotional maturity and conversations about age verification should take this into account.

- All companies operating in the digital world need to remember that yp are their most important present and future audience and continue to engage with us at the earliest possible stage

Hopes and Fears

The Youth Forum hopes were that:

Their voice is not just a space but is acted upon
Adults recognise young people are driving the digital world

There is a balance between the excitement and opportunity of cyberspace, with keeping young people safe
We come together and show although we are from different places we have a common vision to get YP better understood by the adult world

Their fears were that:

Young people's views could get lost in international political ideology
Fast moving world prevents opportunity
Young people could become more vulnerable
Their participation could be seen as tokenistic

Child Safety

Age verification: social networking sites should risk-assess emotional competence to overcome age verification, e.g. a set of questions to assess and answer before given an account
Safe access: greater education directed at young people but with parents involved
Parental controls: need to be young people led but assessed by their competence and in partnership with parents to develop a trusted relationship
You can put up danger signs at the swimming pool but it is no substitute for teaching a child how to swim

In conclusion

The Conference recognized that young people have a critical stake in cyberspace and will be instrumental in its development over the coming years.

Their involvement going forward should never be tokenistic and the voice of young people should be an integral part of the international dialogue going forward to Budapest and Seoul.

Further information

Full coverage of the London Conference on Cyberspace

Images from the conference on Flickr

Follow us on Twitter: @londoncyber & @fcohumanrights

1

2

Foreign Secretary's closing remarks at the London Conference on Cyberspace

02 November 2011

Foreign Secretary William Hague spoke at the end of the London Conference on Cyberspace on 2 November.

Speaker **Foreign Secretary William Hague**
Event **London Conference on Cyberspace**

CHECK AGAINST DELIVERY

"Thank you all very much for coming to this conference. I hope you have enjoyed it, and found it rewarding and thought-provoking.

Earlier this year I proposed principles to govern behaviour in cyberspace, and called for a focussed and inclusive dialogue between all those with a stake in the Internet – civil society and industry as well as governments - on how we might implement them:

The need for governments to act proportionately in cyberspace and in accordance with national and international law;
The need for everyone to have the ability to access cyberspace and the skills, technology, confidence and opportunity to do so;
The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas;
Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and expression;
The need to respect individual rights of privacy and to provide proper protection to intellectual property;
The need for us all to work collectively to tackle the threat from criminals acting online; and

The promotion of a competitive environment which ensures a fair return on investment in network, services and content.

Our Conference began this dialogue on principles and set out an agenda for further work to build a secure, resilient and trusted global digital environment.

Over the next 24 months there will be two follow-on conferences, the first in 2012 hosted by Hungary, and the second in 2013 hosted by South Korea.

I thank the governments of both countries for the leadership and vision they have shown by offering to host the next stages of our work to build a new consensus about the future of cyberspace.

More than 700 participants from 60 countries have taken part in the conference – including Ministers, industry leaders, the internet technical community, civil society and our Youth Forum. I am extremely grateful to you all for your participation. We also heard from citizens across the world. Our panellists took questions direct from the public through the Internet, the event was livestreamed and debated on social media in China, Pakistan, India and the Middle East.

As Conference Chairman, it falls to me to draw together the points that were debated, and to offer my own thoughts about the significance of what we have achieved.

We focussed on five topics: economic growth and development, social benefits of cyberspace, safe and reliable access, international security and cyber crime. I will make a few remarks on each.

On economic growth and development, all delegates agreed that the Internet is a critical engine of economic growth, especially in the developing world, helping to improve access to education and healthcare, reducing poverty, and driving progress on the Millennium Development Goals. To achieve the broadest and deepest possible benefits to growth from cyberspace we must increase access to broadband communication in the developing world and promote the continued global investment and competition in high speed networks and services.

It was also agreed that cyberspace must be secure and reliable so that it is trusted as a medium for doing business, and innovators are confident their discoveries will be appropriately protected.

There was strong support for the principle that we must promote a competitive environment which enables a fair return on investment in network, services and content.

At the same time many speakers called for cyberspace to be free from government and commercial censorship, consistent with international legal obligations, so that

the free availability of information provides incentives for the highest standards of accountability and national governance.

Delegates called for cyberspace itself to have the latitude to evolve and innovate naturally to create new opportunities and benefits in the future.

Delegates called for the removal of unnecessary barriers to trade in cyberspace. Only then will the full benefits of online cross-border trade and globalisation be realised.

On the social benefits and safe and reliable access, all delegates reaffirmed the overwhelmingly positive and transformative benefits of the Internet. Many welcomed its contribution to freedom of expression and association, and its ability to expose human rights abuses as they happen. The Internet is a powerful engine for empowering citizens and driving government accountability.

The conference agreed that efforts to improve cyber security must not be at the expense of human rights.

There was overwhelming support for the principle that cyberspace must remain open to innovation and the free flow of ideas, information and expression.

Many supported the principle that rights to freedom of expression and association apply with equal force in cyber space.

Capitalising on the benefits of cyber space and protecting freedoms is best achieved through inclusive participation of governments, business and civil society, according to many of our delegates. Speakers thought that the best foundation, and the one which best reflected the dynamic of the Internet itself, was a transparent and stable framework of self regulation.

There was strong support for the principle that users of cyberspace should show tolerance and respect for diversity of language, culture and ideas; but protecting this principle must not be used as a cloak for attempts to subvert the right to freedom of expression and association. Speakers also expressed concern that some states may use notions of sovereignty to restrict access, block websites and censor internet content.

Delegates emphasised the need for transparent and interoperable approaches to handling privacy and data protection issues, which recognise the requirement for global trade but also the importance of protecting personal information.

On international security, all delegates agreed with the principle that governments must act proportionately in cyberspace and that states should continue to comply with existing rules of international law and the traditional norms of behaviour that govern interstate relations, the use of force and armed conflict, including that states must settle their international disputes by peaceful means in such a manner that international peace, security and justice are not endangered.

All speakers agreed that stronger co-operation and collaboration was needed to build confidence and to avoid misunderstandings.

All delegates agreed that the immediate next steps must be to take practical measures to develop shared understanding and agree common approaches and confidence-building measures. There was no appetite at this stage to expend effort on new legally-binding international instruments.

There was strong support for the recommendations of the 2010 UN Group of Government Experts on further dialogue among states to discuss norms pertaining to state use of information and communication technologies to reduce collective risk and protect critical national and international infrastructure.

Delegates welcomed the work the OSCE is also doing to develop specific confidence-building measures applicable in cyber space, and called on other regional organisations such as the ASEAN Regional Forum to develop their own work alongside the OSCE on this question.

And on the fifth and final theme, the conference identified cyber crime as a significant threat to economic and social well-being, and one which requires a concerted and urgent international effort.

All delegates strongly supported the principle that we must work collectively together to tackle the threat from cybercrime and ensure there are no safe havens for cyber criminals. There was strong support from delegates for the guiding principle that what is unacceptable offline is also unacceptable online. As was pointed out in the Youth Sessions, for young people the online and offline worlds are one place.

Many countries and regional bodies are already taking positive steps towards implementing cyber crime legislation, but it was recognised that these need to be compatible internationally. In addition to legislation, countries were encouraged to ensure they have the forensic resources, processes and willingness to co-operate as necessary.

There was general support for the principles for fighting online crime that are set out in the Budapest Convention on Cybercrime and little appetite for negotiating a new instrument. Many delegates encouraged countries to look at whether they could sign up to the Budapest Convention, seeing the Convention as the best form of international agreement in this area. Some delegates called on the UK to promote the Convention during its forthcoming chairmanship of the Council of Europe, a recommendation that the UK intends to take forward. Some delegates also expressed their support for the Commonwealth work on a cyber crime Model Law as a useful stepping stone.

As well as law enforcement and cross-border co-operation, the debate noted prevention as being central to tackling cyber crime. There was general agreement that all sectors - private companies and individuals as well as governments and law enforcement agencies – have responsibilities in preventing cyber crime.

Delegates thought government and industry had a shared responsibility to do more to prevent cyber crime, in industry's case for example through more secure devices, systems and services. Industry must be a part of the solution on prevention. There was general support for the view that the public and businesses should get more help to able to identify easily products that have good security. Delegates encouraged the private sector to lead development of improved Internet security products, systems, services and standards in cyberspace, and to make the market easier to navigate for consumers.

Speakers noted that all Governments are currently looking to place more services online. It was agreed that governments need to lead by example, and that when governments procure and provide online services, security is one of the key criteria.

Delegates believed governments have a responsibility to ensure an open Internet that allows individuals access to content and services with only such restrictions as are permitted under international legal obligations, while protecting users against abuse, especially children.

There was agreement that government should have an underpinning legal framework to protect the integrity of online transactions that can provide recourse, for example in the event of fraud. Beyond that many speakers thought that governments should encourage self-regulatory mechanisms for the private sector, rather than start with legislation and regulation.

Delegates called on governments to take an appropriate and proportionate interest in improving the safety and reliability of cyberspace, while recognising that the expertise lies with industry partners. Delegates called on industry to lead the creation and maintenance of open standards being mindful of the challenges to information access. Speakers called on service providers and suppliers to redouble their commitment to ensuring the reliability and availability of systems.

These and other findings of the Conference will be published in a document available to you all shortly.

I wish to add my own three reflections the significance of the London Conference on Cyberspace and some views on the messages it sends.

The first reflection is that the conference has shown that there is a real hunger to address the need for a safe and secure future in cyberspace. It is striking that

every country represented here perceives itself to be at the receiving end of threats in cyberspace.

The demand for a safe digital environment is rising as more and more of our lives are lived on the internet. All Governments need to respond to this demand; not just some governments in some regions of the world, but across the globe.

My second reflection is that we have established conclusively that governments cannot determine the future of the internet and digital networks alone.

In fact, when governments do discuss this subject we are at risk of adopting wrong or dangerous conclusions, or of being out of touch and out of date the minute we sit down. It is vital that we understand our limitations in this area.

The founder of Wikipedia described how that organisation bases its moderation of online content on the principle of 'assuming good faith'. This is an inspiring model that Governments could not have devised and which could not be enforced by them either. The involvement of industry, civil society and internet experts is absolutely essential and any attempt to move forward without their participation will fail.

The third reflection I offer is that we must now accelerate the international debate on cyberspace and move it onto a permanent and continuous footing. Until now, it has not sufficient intensity to match either the exponential rise in threats or the booming nature of the opportunity.

So this has been a hopeful and immensely inspiring conference. We have succeeded in galvanising the international debate about the future of cyberspace. We have achieved our central objective and identified the ground that will need to be covered on the way to agreement about norms of behaviour in cyberspace.

The London Conference will lead to concrete action across its themes, building on the foundations laid in organisations such as the UN, OECD, Council of Europe, and APEC, as well as on private sector initiatives such as the development of principles for User Generated Content and the Global Network Initiative. Just a few examples include:

Working to bridge the digital divide through support to the ITU/UNESCO Broadband Commission;
Considering further the recommendations of the 2010 UN Group of Government Experts on norms of behaviour;
And expanding support for the Budapest Convention on cyber crime;

In my view there are clear messages from this conference for governments, the private sector and individuals.

For governments there are four messages: whatever country you represent the rapid rise of cyber crime is a growing threat to your citizens. Our occasional talking together on this subject needs to become a permanent activity, and just because no one person in most governments is responsible for this area does not mean it can be ignored any longer.

The second message for governments is do not treat cyberspace as if it belongs to you. We will only be capable of tackling the issues we have discussed at this conference about the future of the internet by using the ideas and ingenuity of people outside government.

The third message for governments is that state sponsored attacks are not in the interests of any country long term, and that those governments that perpetrate them need to bring them under control.

The fourth message for governments is while working together to defeat threats in cyberspace you should not imagine for an instant that you can resist the growing force of the tide now flowing for transparency, open information and the free exchange of ideas. Those governments that try to do so are bound to fail.

The message to entrepreneurs and companies is keep your ideas flowing. You need to work with your government to safeguard intellectual property and prevent cyber crime, while continuing to pursue the innovation and ideas that created cyberspace in the first place.

And the message for individuals is this is your debate. Large numbers of people have followed this conference online. You must be our allies in ensuring that the future global consideration of cyberspace, like this conference, remains true to its own nature and allows for a vast diversity of opinion and individual expression.

In taking forward this work no one country can go it alone. Just as forty years ago discussion of Cooperation and Security in Europe evolved to establish a range of agreements that promote co-operation while ensuring security, we can now look forward with optimism that in London we began the collective endeavour of enhancing and protecting the internet for future generations.

We do not underestimate the difficulties ahead. There are still divides to be bridged and difficulties to be overcome. Achieving the broad, international consensus will take time. But this is one of the great challenges of our time and in London the world has made clear that we will not leave it to chance. We will pursue it with the intensity it demands and deserves.

I thank all those who have taken part in the London Conference and look forward to working together to build a secure, resilient and trusted global digital environment which will benefit us all for generations to come.

More information

Read the Chair's statement

Full coverage of the London Conference on Cyberspace

Images from the conference on Flickr

Follow us on Twitter: @londoncyber & @fcohumanrights

TAB 4

4. DEBRIEF OF NOVEMBER 8, 2011 DEPUTIES MEETING

PROPOSED TALKING POINTS

- As a result of the November 8, 2011 Deputies meeting was the establishment of a new governance structure for cyber security.

- This called for the creation of the Deputy Ministers (DMs) Committee on Cyber Security, which will meet quarterly. We will discuss the terms of reference for this Committee shortly.

- As a result of increased meeting frequency, Assistant Deputy Ministers (ADMs) could meet as often as monthly.

- Membership of the DM/ADM Cyber could be looked at to streamline membership to core and non-core members. This would facilitate decision-making and alleviate the meeting burden on departments such as Industry Canada.

- Deputies have varying degrees of familiarity with the cyber file.

- Let's first discuss how best to brief Deputies on network hygiene, and roles and responsibilities.

TAB 5

ANNEX

SECRET

5a. FOLLOW-UP ON DEPUTIES MEETING: NETWORK HYGIENE

PROPOSED TALKING POINTS

- Deputy Ministers have expressed interest in learning more about network hygiene and how best to advance it in Government.
- [redacted]
- We need to identify what key messages we should be giving Deputies, and how best to equip them to advance this issue. Pierre (Boucher), perhaps as lead, you could propose an approach to briefing Deputies?

ISSUE

You will introduce this agenda item. Treasury Board Secretariat will lead the discussion as security of Government systems falls under their responsibilities. The Communications Security Establishment Canada (CSEC) is expected to speak in support.

BACKGROUND

Network hygiene refers to regularly performing the "bread and butter" activities of network and information technology (IT) security, such as keeping firewalls and anti-virus products up to date, regularly applying software patches from vendors, regularly updating which users have access to which data, and maintaining good records of the configuration of the network and what computers are permitted to connect to what.

Security organizations have published lists of the most important network hygiene activities [redacted] as it is well recognized that disciplined network hygiene makes a significant difference in security. Network hygiene can also be onerous, time-consuming for IT staff, and in conflict with operational priorities that demand that systems not be taken down for maintenance.

CURRENT STATUS

[redacted]

The *Policy on Government Security* IT security standard contains numerous clauses that speak to good network hygiene. For example, departments and agencies must have "a systematic, documented patch management process to ensure they apply security-related patches in a timely manner."

[redacted]

Shared Services Canada will centralize the governance of Government IT, which should make network hygiene easier. This transition will evolve over years, during which time discipline will still be required across the decentralized IT infrastructure.

[redacted]

Prepared by: Adam Hatfield

Pages 135 to / à 150

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

ANNEX

5b. FOLLOW-UP ON DEPUTIES MEETING: ROLES AND RESPONSIBILITIES

PROPOSED TALKING POINTS

- Deputy Ministers want a clearer understanding of the respective roles and responsibilities of departments with respect to cyber security, and how they can be leveraged to improve Canada's cyber security posture.

- Our Directors General have contributed to a deck that was distributed at the beginning of this meeting, which shows the respective roles and responsibilities of our departments with respect to cyber security.

- It was updated very quickly by all our teams, so I encourage you to take it back and provide final input by the end of the week. We should also discuss how best to brief up in advance of the DM Cyber meeting.

ISSUE

You will lead a discussion regarding cyber security roles and responsibilities.

Deputy Ministers have expressed interest in the respective roles and responsibilities of departments with respect to cyber security, and how they can be leveraged to improve Canada's cyber security posture.

A copy of a roles and responsibilities deck that was populated with input from member departments of the Directors General Interdepartmental Committee on Cyber Security (DG Cyber) was distributed to participants in advance of this meeting, and is **attached** for your ease of reference.

There is concern that more time is needed to ensure the slides reflect current activities, and due to outstanding issues between the Treasury Board Secretariat and Shared Services Canada.

BACKGROUND

August 2011 saw the creation of Shared Services Canada (SSC), an agency that will consolidate the Government email system, reduce the overall number of data centres, and streamline electronic networks within and between Government departments.

s.21(1)(a)

UNCLASSIFIED

s.21(1)(b)

[redacted]

CURRENT STATUS

[redacted]

At the December 2010 DG Cyber retreat, departments were asked to provide a snapshot of their mandate as it relates to cyber security with a view to providing clarity on the issue and to avoid duplication of efforts. Following the Deputy-level meeting, departments were asked to update their snapshot. Departmental input has been incorporated into a deck for the purpose of this meeting.

You may wish to use this opportunity to present the deck to participants, informing them that they may review the contents and provide any changes within the week.

Prepared by: Melanie Mohammed
Approved by: Corey Dvorkin

SECRET

Public Safety Canada / Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

Departmental Roles and Responsibilities with respect to Cyber Security

Canada

SECRET

Canadian Security Intelligence Service

- Responsible for conducting national security investigations, reporting to and advising the Government of Canada of activities constituting a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act*.

- Investigates cyber incidents or related activity assessed as constituting a threat to the security of Canada; and assist in the Government's cyber incident response capability through the *Government of Canada Information Technology Incident Management Plan*.

- Provides analysis that will assist the Government of Canada in understanding cyber threats, the actors behind those threats, and overall situational awareness enabling the Government of Canada to better identify cyber vulnerabilities and to take action to secure critical infrastructure, prevent cyber espionage or other related cyber threat activity.

Canada

1

SECRET

Communications Security Establishment Canada

- Provides advice, guidance and services to help protect electronic information and systems of importance to the Government of Canada.

- For the sole purpose of protecting computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, and with authorization from the Minister of National Defence, may intercept private communications (i.e., full monitoring/sensoring).

- Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the Five Eyes cryptologic community.

- Key player in the *Government of Canada Information Technology (IT) Incident Management Plan*

Canada

2

SECRET

Defence Research and Development Canada

- Leads the development of military cyber security science and technology (S&T) in support of the Canadian Forces.

- Leads domestic Public Safety Canada cyber security S&T efforts not specifically assigned to another department or agency through DRDC Centre for Security Science support to Public Safety Canada and domestic security partners in the Public Security Technical Program. This is delivered in partnership between Government, industry, academia and allies.

Canada

3

SECRET

Department of Foreign Affairs and International Trade

- Supports international bodies in mitigating cyber threats and assisting foreign governments in improving their cyber security profile and capabilities.
- Contributes to diplomatic engagement in order to help shape the multilateral regulatory space that is emerging with respect to cyber security. Enables the GC to better position Canada on the international stage to defend and promote its foreign policy and cyber security-related interests.
- Cyber security policy program will be aimed at gaining situational awareness of cyber security development in the international arena and ensure Canadian intervention as required in the key fora where cyber security policy is being debated.
- In addition to strengthening the GC's knowledge and capabilities on cyber security in the international sphere, the cyber security program will bolster Canada's credibility with allies and major partners.

Canada

4

SECRET

Department of National Defence / Canadian Forces

- Responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process.
- Contributes to Government of Canada situational awareness during the monitoring and analysis, mitigation, and response phases of the *Government of Canada Information Technology (IT) Incident Management Plan* by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

Canada

5

SECRET

Department of Justice Canada

- The primary mandate of the Department of Justice Canada is to support the initiatives of client departments and agencies through the provision of legal advice on matters relating to cyber policy and law.

- In respect of certain matters, especially those relating to criminal law policy and information sharing, Justice plays a leading role.

Canada

6

SECRET

Industry Canada

- Responsible for spectrum management in Canada and for fostering a robust and reliable telecommunications system.

- Responsible for ensuring a safe and secure online marketplace.

- Helps to ensure the continuity of telecommunications during an emergency.

Canada

7

SECRET

Privy Council Office

- Provides non-partisan advice to the Prime Minister, other ministers in his portfolio, Cabinet and the chairs of Cabinet committees on questions of national, intergovernmental and international importance, including cyber security.

- PCO houses and provides support to the National Security Advisor (NSA) to the Prime Minister.
  - Provides advice and support for Cabinet discussions on national security and intelligence matters, including cyber security.
  - Coordinates activities among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to national security issues.
  - Is the Deputy Minister of the Communications Security Establishment.
  - Maintains relationships with allies by acting as the senior Canadian representative on national security matters.

Canada

8

SECRET

Public Safety Canada

- Leads and coordinates the implementation of the Strategy and the design of a whole-of-Government approach to performance measurement and reporting.

- Leads engagement with provinces and territories, critical infrastructure, and international allies on strategic cyber security policy issues and national cyber incident management

- The Canadian Cyber Incident Response Centre (CCIRC) acts as Canada's national CERT (Computer Emergency Response Team) in providing assistance and mitigation advice to domestic partners and coordinating the national response to any cyber security incident; is also a key player in the *Government of Canada Information Technology Incident Management Plan*

- Public Safety Canada is also leading public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace.

Canada

9

SECRET

Public Works and Government Services Canada

- Provider of shared and common services. As part of its Industrial Security Program activity, ensures security in contracts awarded by the Department or when requested by other Government departments.

- Ensures the protection of foreign and NATO classified information within the private sector in Canada.

- The Industrial Security Sector maintains relationships with allies and negotiates Memoranda of Understanding on industrial security matters, including cyber security, in contracting.

Canada

10

SECRET

Royal Canadian Mounted Police

- Canadian national police service and an agency of Public Safety Canada.

- Leads the criminal investigative response to suspected criminal cyber incidents involving critical information infrastructure (i.e., unauthorized use of computer and mischief in relation to data). Leads the investigative response to suspected criminal national security cyber incidents.

- Assists domestic and international partners with advice and guidance on cyber crime threats.

- Key player in the *Government of Canada Information Technology (IT) Incident Management Plan*

Canada

11

SECRET

Shared Services Canada

- Responsible for streamlining and consolidating information communication technologies in the areas of email, data centres and networks.
- Provides common information technology (IT) security services and other solutions to enable departments to exchange information with citizens, businesses and employees.
- Responsible for ensuring the confidentiality, integrity and availability of common IT services provided to departments.
- Gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to common IT services and Government IT critical infrastructure managed by Shared Services Canada, and communicates the information to CCIRC and, as authorized, to departments and cyber security partners.
- Key player in the *Government of Canada Information Technology (IT) Incident Management Plan*

Canada

12

SECRET

Treasury Board of Canada Secretariat

- Establishes and oversees a whole-of-government approach to cyber security, including:
  - setting government-wide direction and establishing priorities for securing government information technology (IT) systems and networks;
  - providing direction and advice to lead security agencies on the approach and implementation of measures for managing IT security incidents; and
  - providing oversight of IT incident management, including post-mortem reviews and lessons learned.

Canada

13

ANNEX

5c. FOLLOW-UP ON DEPUTIES MEETING: DM CYBER

PROPOSED TALKING POINTS

- Deputies are keen to engage more on cyber and have indicated that quarterly meetings would be appropriate.

- They've asked us to propose terms of reference and membership, and a document reflecting each has been circulated.

- A first meeting would be convened mid-December 2011.

- Base don this discussion, it seems they want to be more engaged in monitoring progress, setting priorities, shaping policy, and de-conflicting issues that may arise. A smaller group, that could be expanded when necessary, seems best suited to this mandate and the proposed meeting frequency.

- I would invite your comments first on the proposed terms of reference, then on the membership.

- We will then have to consider our own membership and appropriate meeting frequency.

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED
DRAFT

Deputy Ministers' Committee on Cyber Security

Terms of Reference
November 2011

Purpose

The purpose of the Deputy Ministers' Cyber Security Interdepartmental Committee (DM Cyber) is to ensure an open and coordinated approach to:

- priority-setting;
- monitoring progress on the implementation of *Canada's Cyber Security Strategy*;
- the consideration and validation of threat assessments;
- issue de-confliction between departments and agencies;
- the consideration of key cyber policy issues, including those within and outside the Strategy's scopy.

Membership

- Chair and Secretariat:
  - Deputy Minister, Public Safety Canada

- Core members:
  - National Security Advisor, Privy Council Office
  - Director, Canadian Security Intelligence Service
  - Chief, Communications Security Establishment Canada
  - Deputy Minister, Department of National Defence
  - Chief of Defence Staff, Canadian Forces
  - Commissioner, Royal Canadian Mounted Police

Governance / Relationship to other working groups and committees

DM Cyber is supported by the Assistant Deputy Ministers' Committee on Cyber Security, which is supported by the Directors General Committee on Cyber Security.

Meeting frequency

DM Cyber will meet quarterly, with *ad hoc* meetings called by the Chair as required.

TAB 6

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

[redacted]

PROPOSED TALKING POINTS

[redacted]

- I will turn to the Director General of NCSD to speak to this endeavour.

ISSUE

Robert Dick, Director General, National Cyber Security Directorate (NCSD), [redacted]

[redacted]

BACKGROUND

[redacted]

CONSIDERATIONS

[redacted]

UNCLASSIFIED

[redacted]

CURRENT STATUS

[redacted]

NEXT STEPS

[redacted]

Prepared by: Ian Anderson
Approved by: Corey Dvorkin

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

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

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

[redacted]

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

[redacted]

TAB 7

s.15(1) - Int'l

s.15(1) - Subv

s.13(1)(a)

SECRET

6. ROUNDTABLE

CURRENT STATUS

During the roundtable, you will have one item to contribute:

[redacted]

Pages 174 to / à 176

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Subv, 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

Critical Information Infrastructure Protection and Cyber Security

Canada's Cyber Security Strategy – One Year Later

November 22-23, 2011

Atlantic Provinces Control Systems Security Workshop

Canada

Government of Canada Initiatives

BUILDING A **SAFE** AND **RESILIENT CANADA**

- *Consultation Paper on a Digital Economy Strategy for Canada* (May 2010).

- *National Strategy and Action Plan for Critical Infrastructure* (May 2010).

- *Canada's Cyber Security Strategy* (October 2010).

Canada's Cyber Security Strategy

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Signals cyber security as a priority investment for the Government of Canada.

- Coordinates and unifies domestic and international action.

- Built on three pillars:

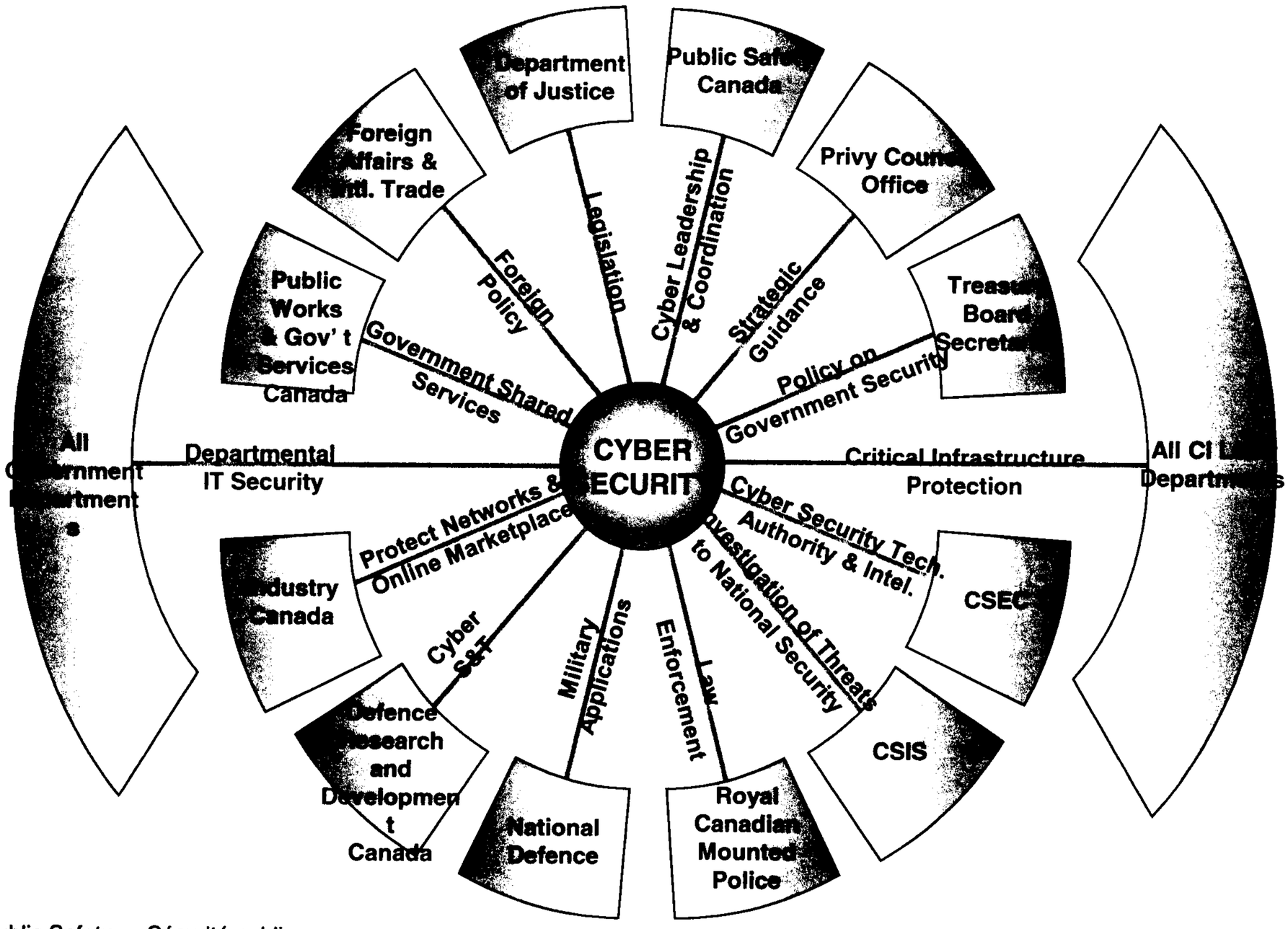
1. Secure Government systems.

2. Partner to secure systems outside the Government of Canada.

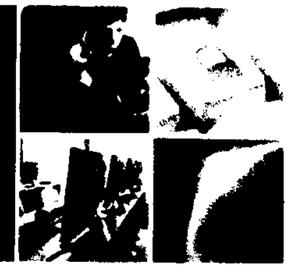
3. Help Canadians to be secure online.

Cyber Security Roles and Responsibilities within the Government of Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



Progress on Implementation and Upcoming Initiatives



BUILDING A **SAFE** AND **RESILIENT CANADA**

- Updating laws to reflect the realities of the digital world.
- Developed cyber security public awareness campaign.
- Redefined the responsibilities for cyber security incidents affecting Canadian networks.
- Streamlined and consolidated Government IT infrastructure, and created Shared Services Canada.

s.14(a)

- Created the National Cross-Sector Forum to build partnerships, improve information sharing, and address the physical and cyber vulnerabilities that span all critical infrastructure sectors.

Legislation

- Passed two pieces of legislation to enhance cyber security.
  - Anti-Spam Bill:
    - Seeks to deter the most damaging and deceptive forms of spam from occurring in Canada.
    - Authorizes the creation of a spam reporting centre.
  - Bill S-4:
    - Amends the *Criminal Code* to create three new offences related to identity theft, with five-year maximum sentences.
    - Authorizes courts to order offenders to pay restitution to a victim of identity theft as part of their sentence.
- Examining ways to provide law enforcement with modernized investigative tools to address cyber crimes.

Get Cyber Safe.ca Campaign

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Public Safety Canada's Communications Directorate has launched a national public awareness advertising campaign to deliver on the third pillar of *Canada's Cyber Security Strategy.*
- Provides Canadians with information on cyber threats in order for them to take action to protect themselves and their personal information.
- Includes advertising, a cyber-specific website, marketing partnerships and international coordination of messaging, as well as issues management in response to cyber incidents.
- Was launched in October to coincide with Cyber Security Awareness Month and the one-year anniversary of the Strategy.

Public Awareness Campaign

BUILDING A **SAFE** AND **RESILIENT CANADA**

Government of Canada / Gouvernement du Canada

Canada

Get Cyber Safe

GetCyberSafe.ca

Français | Home | Contact Us | Help | Search | Canada.gc.ca

Home

Know the Risks
- Online Activities
- Common Threats
- Scams and Fraud

Protect Yourself
- Protect Your Identity
- Protect Your Money
- Protect Your Family

Protect Your Devices
- Computers, Laptops and Tablets
- Mobile Devices
- Home Networks
- Storage

Resources

GETCYBERSAFE

Make cyber safety a personal priority with tips and resources to help protect everything that's important to you.

Share | Email

Search

GetCyberSafe Video

See the Ad

It Happened to Me

Here's your chance to share your story and read about others' experiences. By passing along any helpful information you've

Public Safety Canada / Sécurité publique Canada

Division of Cyber Security Roles in Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

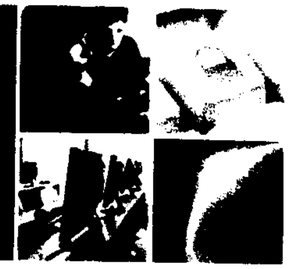
- On June 20, 2011, the responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the Cyber Threat Evaluation Centre, which is the computer emergency response team for federal departments and agencies.
  - CCIRC is now the national computer emergency response team for provinces, territories and critical infrastructure sectors.

Shared Services Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

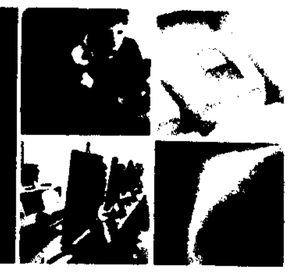
- Effective August 4, 2011, the Government streamlined and consolidated its IT architecture in the areas of email, data centres and networks.
- This will produce savings and reduce the Government's footprint; strengthen security and the safety of Government data to ensure Canadians are protected; and realize economies of scale and make it more cost-effective to modernize these IT services.
- All resources associated with the delivery of email, data centre and network services are being transferred from 44 of the more IT-intensive departments to a new entity called Shared Services Canada.

Meetings with Provincial and Territorial Governments



- Initiated dialogue with provincial and territorial interlocutors to strengthen intergovernmental engagement on cyber security.
- Key objectives from a federal perspective:
  - clarify national operational roles and responsibilities;
  - improve information sharing;
  - engage critical infrastructure and private sectors;
  - ensure a better informed population by maximizing resources and leveraging provincial and territorial access to the public;
  - establish a forum for consultation on legislative and policy undertakings;
  - explore interest in the development of a national cyber incident response framework; and
  - ensure a cohesive front in regards to international efforts and pressures.

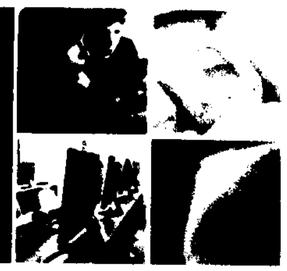
National Cross-Sector Forum



BUILDING A **SAFE** AND **RESILIENT CANADA**

- Four priorities were identified at the inaugural meeting:
  - Develop a common understanding of critical infrastructure within and across sectors.
  - Establish an information sharing framework for sensitive information shared between public-private and private-private entities.
    - Identify key assets and critical systems.
    - Identify key interdependencies and vulnerabilities.
- Engaged with provincial and territorial departments of telecommunications, energy and natural resources.

Canadian Security Telecommunications Advisory Council



BUILDING A **SAFE** AND **RESILIENT CANADA**

- CSTAC is comprised of senior executives from the public and private sectors. It provides a forum to:
  - exchange information;
  - collaborate strategically on current and evolving issues that may affect the confidentiality, integrity or availability of the telecommunications infrastructure; and
  - provide advice on measures to address these issues.
- The Committee is focusing on several areas:
  - risks to the critical telecommunications infrastructure, including proactive and mitigating measures to address threats and vulnerabilities;
  - network monitoring;
  - interdependencies; and
  - emergency management and disaster recovery.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

www.publicsafety.gc.ca/cyber

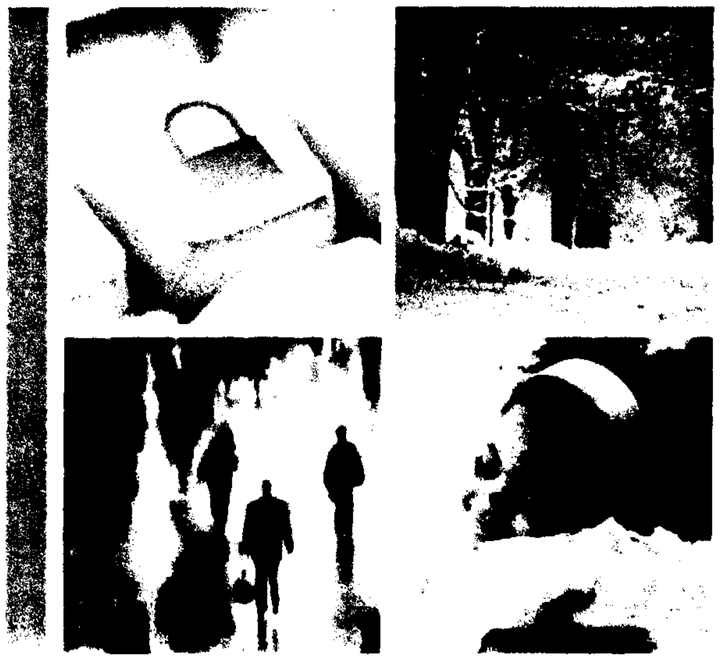
www.publicsafety.gc.ca/ci

Canada

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

BUILDING A SAFE AND RESILIENT CANADA



Control Systems Security Workshop

Post Workshop Report

St. John's, NL
November 22-23, 2011

Canada

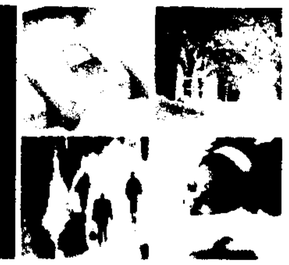
Highlights

- Very positive feedback from all participants
  - Provided valuable tools and knowledge
  - Strengthened Federal-Provincial-critical infrastructure relations
  - Growing appetite for additional events

- 60 Participants – all levels of government, critical infrastructure owners and operators and academia

- Presentations from recognized experts and federal Government on control systems and cyber security

Workshop Overview



- Two-day training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators better secure their most critical control system and information technology assets.
- Recognized experts along with representatives from the federal Government provided briefs on the latest threats and steps that can be taken to increase the security of control systems.
- Goals:
  - provide a greater awareness of the threats and what resources are available to assist in mitigating them;
  - provide a trusted forum where control systems owners and operators can exchange information and ideas to help improve their security posture; and
  - help develop a trusted relationship between the federal, provincial and territorial governments; and control systems owners and operators.

Participants

- Total – 60 participants
- Federal Government
  - Public Safety Canada, RCMP, CSIS, DRDC, DFO, PWGSC, Environment Canada and Nav Canada
- Provincial Government
  - Newfoundland and Labrador, New Brunswick and Nova Scotia
- Municipal Government
  - St. John's
- Academia
  - Memorial University
- Critical Infrastructure Sectors (8/10)
  - Energy and utilities, Transportation, Government, Information and communication technology, Health, Water, Safety, Manufacturing

Agenda

SAFE RESILIENT CANADA

RCMP GRC

2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

Tuesday, November 22, 2011

08:30 – 09:00	**Registration** (identification required)
09:00 – 10:15	**State of Control Systems Cyber Security** [redacted] Department of Homeland Security
10:15 – 10:30	**Health break**
10:30 – 11:15	**Exercising Security: A look inside the NERC Cyber Risk Preparedness Assessment Program** Mark Fabro, Lofty Perch
11:15 – 12:00	**Evaluating the Safety and Security of Automation Products & Systems** John Cusimano, Exida
12:00 – 13:30	**Lunch break**
13:30 – 14:15	**SCADA security in the oil and gas sector** Mark Fabro, Lofty Perch
14:15 – 15:00	**Control Systems Security Program (CSSP) cyber security products and services for owners and operators of Control Systems** [redacted] Department of Homeland Security
15:00 – 15:15	**Health break**
15:15 – 16:00	**Canadian Cyber Incident Response Centre (CCIRC)** Luc Beaudoin, Canadian Cyber Incident Response Centre
16:00 – 16:45	**Intrusion Detection/Prevention in Critical Networks** Frank Marcus, Wurldtech
16:45 – 17:00	**Closing remarks**

RCMP GRC

2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

Wednesday, November 23, 2011

08:45 – 09:00	**Registration** (identification required)
09:00 – 09:30	**Canada's Cyber Security Strategy** Tom Campbell, Public Safety Canada
09:30 – 10:15	**Cybercrime and Critical Infrastructure Protection** Jacques Boucher, Royal Canadian Mounted Police
10:15 – 10:30	**Health break**
10:30 – 11:15	**Cyber Security Evaluation Tool (CSET)** [redacted] Department of Homeland Security
11:15 – 12:00	**Smart Grid and Advanced Metering Infrastructure Security Research Activities** Mark Fabro, Lofty Perch
12:00 – 13:30	**Lunch break**
13:30 – 14:15	**Government of Canada Control Systems Security Research** Rodney Howes, Defence Research and Development Canada
14:15 – 15:00	**Briefing** [redacted] Canadian Security Intelligence Service
15:00 – 15:15	**Health break**
15:15 – 16:00	**Control Systems Cyber Security Training Opportunities** [redacted] Department of Homeland Security
16:00 – 16:45	**Break-out Session**
16:45 – 17:00	**Closing remarks**

Organizers

- Organizers:
  - National Cyber Security Directorate (NCSD) and Critical Infrastructure and Strategic Coordination Directorate (CISCD) of PS.

- Supporting Organizations:
  - RCMP Tech Crime Branch
  - Regional offices of both PS and the RCMP
  - Canadian Security Intelligence Service
  - Defence Research and Development Canada

Speakers

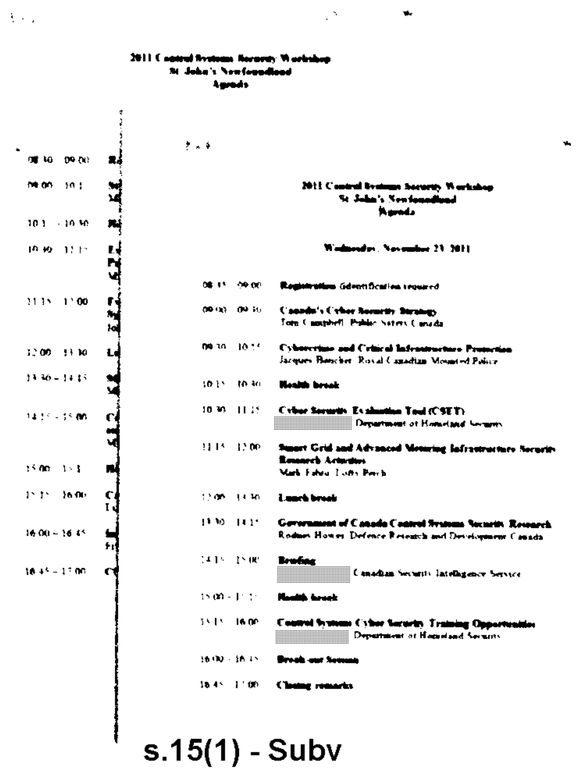
- [redacted] DHS Control Systems Security Program
- Mark Fabro, Lofty Perch
- John Cusimano, Exida
- Luc Beaudoin, CCIRC
- Frank Marcus, Wurldtech
- Tom Campbell, Public Safety
- Jacques Boucher, RCMP
- Rodney Howes, DRDC
- [redacted] CSIS

s.15(1) - Subv

s.19(1)

Topics

- State of Control Systems Cyber Security
- Exercising Security: A look inside the NERC Cyber Risk Preparedness Assessment Program
- Evaluating the Safety and Security of Automation Products & Systems
- SCADA security in the oil and gas sector
- Control Systems Security Program (CSSP) cyber security products and services for owners and operators of Control Systems
- Canadian Cyber Incident Response Centre (CCIRC)
- Intrusion Detection/Prevention in Critical Networks
- Canada's Cyber Security Strategy
- Cybercrime and Critical Infrastructure Protection
- Cyber Security Evaluation Tool (CSET)
- Smart Grid and Advanced Metering Infrastructure Security Research Activities
- Government of Canada Control Systems Security Research
- CSIS Briefing
- Control Systems Cyber Security Training Opportunities



2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

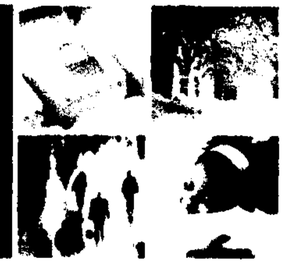
2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

Wednesday, November 23, 2011

08:15	09:00	Registration (Identification required)
09:00	09:10	Canada's Cyber Security Strategy Tom Campbell, Public Safety Canada
09:10	10:15	Cybercrime and Critical Infrastructure Protection Jacques Bourcier, Royal Canadian Mounted Police
10:15	10:30	Health break
10:30	11:15	Cyber Security Evaluation Tool (CSET) [redacted] Department of Homeland Security
11:15	12:00	Smart Grid and Advanced Metering Infrastructure Security Research Activities Mark Fabro, Lofty Perch
12:00	13:30	Lunch break
13:30	14:15	Government of Canada Control Systems Security Research Rodney Howes, Defence Research and Development Canada
14:15	15:00	Briefing [redacted] Canadian Security Intelligence Service
15:00	15:15	Health break
15:15	16:00	Control Systems Cyber Security Training Opportunities [redacted] Department of Homeland Security
16:00	16:15	Break out Session
16:45	17:00	Closing remarks

s.15(1) - Subv
s.19(1)

Lessons Learned



- The workshops are viewed as:
  - Good forum for exchanging information
  - Helpful in strengthening Federal-Provincial-critical infrastructure relations
  - Important communication mechanism
  - Useful in provide valuable tools and knowledge

- There is opportunity to build upon the workshops to include:
  - Classified executive briefings
  - Hands-on technical training

Next Steps

- Short-Term
  - Planning underway for next workshops:
    - Montreal Jan 31 – Feb 1 2012
    - Calgary mid-March
  - Looking to integrate:
    - Hands-on technical training (starting in Montreal)
    - Classified executive briefings (starting in Calgary)

- Long-Term
  - Conduct review of workshop series and determine approach for their future

Page 201

is withheld pursuant to sections

est retenue en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Cyber Security Working Group (CSWG)

Presentation to the Emergency Management Consultative Group

October 20, 2011

Ottawa, Canada

Cyber Security Working Group Mandate

- Serves as a Federal level forum for:
  - the bilateral exchange of information on cyber security strategies, initiatives and projects; and
  - coordination of initiatives and projects with bilateral interest or implications.

- Areas of Focus:
  - Policy, Programs, and Capabilities Development;
  - CERT Collaboration;
  - Cyber Incident Management;
  - Exercise Collaboration; and
  - Collaboration through Multinational Fora.

Key Accomplishments in 2011

- Bilateral Information sharing
  - February 8-9 – Working level meeting between DHS, PS and DND
  - April 12 – Senior level bilateral meeting between DHS and PS
  - April 13 – MS-ISAC tour
  - Ongoing collaboration between Canadian Cyber Incident Response Centre (CCIRC) and US-CERT

- 2+2 Cyber Engagement
  - Feb 10 – Staff level planning conference
  - Apr 4-6 – Deputy Assistant Secretary and Director General meeting
  - Oct 5 – Deputy Secretary and Deputy Minister-level meeting

- Program collaboration
  - April 12-13 – British Columbia Control Systems Security Workshop

- Perimeter Vision and Action Plan development

- Collaboration through multinational fora

  [redacted]

  Usual Five - Jun 29-Jul 1, 2011 in London, England

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

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

2+2 Cyber Engagement

- On October 5, 2011, the Deputy Secretaries and Deputy Ministers from DHS, DOD, PS and DND discussed:

- The next steps identified during the meeting include:

Beyond the Borders Perimeter Vision

- Initiative 29 commits to improving bi-national coordination between respective national cyber operations centres.

- Designed to build on lessons learned through **Usual 5** and IWWN collaboration, Cyberstorm exercise series, and the 2+2 tabletop exercise.

- Canada and the U.S. will improve processes for dealing with:
  - bi-national information sharing;
  - providing information or assistance to the private sector; and
  - public affairs communications (steady-state and incident response).

Looking Forward

- Implementation of Beyond the Border Perimeter Vision
- Exploring opportunities for bilateral and multi-national collaboration in cyber exercises
- Sharing lessons learned on creation of National Cyber Incident Response Plan
- Upcoming meetings:
  - Meridian Conference – October 24-26, 2011 in Doha, Qatar;
  - London Conference on Norms and Values in Cyberspace – Nov 1-2, 2011 in London, England;
  - [redacted]
  - Usual Five – January 2012 in New Zealand.

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

- Questions? Please contact NCSDInternationalAffairs2@hq.dhs.gov or Adam.Hatfield@ps-sp.gc.ca

Minister of Public Safety | Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

s.19(1)

NOV 2 3 2011

[redacted]

Thank you for your correspondence dated October 4, 2011 regarding *Canada's Cyber Security Strategy,* and digital rights management.

I can assure you that the Government takes all threats to Canada's cyberspace seriously and is committed to keeping cyber infrastructure secure and resilient. Canadian citizens, businesses, and governments are embracing the many advantages that cyberspace offers, and our economy and quality of life are the better for it. This is why the Government launched *Canada's Cyber Security Strategy* in October 2010. The Strategy is our plan for meeting the cyber threat while ensuring Canadians can continue to enjoy the benefits of cyberspace. The Government is working hard with our partners, including the provinces, territories and industry, to protect our digital infrastructure.

Bill C-11, the *Copyright Modernization Act,* is an important step towards preparing Canada for the digital economy of today and tomorrow. We believe that protecting information and the rights of intellectual property holders is important to Canadians and further exemplifies the efforts of the Government of Canada to strengthen and secure our economic prosperity.

Regarding the technologies used by the Government of Canada for its own systems, as a matter of policy we do not comment on the specifics of our information technology infrastructure. I can assure you that we use technology from many different sources to meet our technological needs in the most effective and secure means possible.

Thank you again for writing on this important issue.

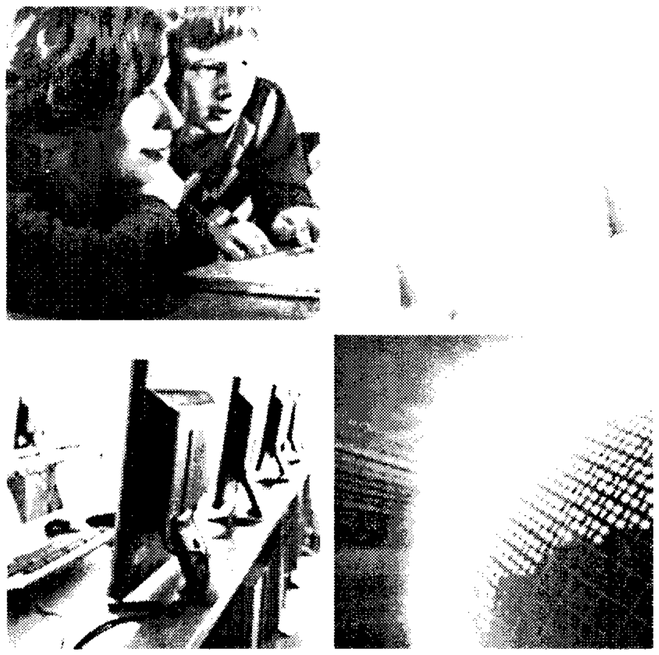
Yours sincerely,

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

Canada

Public Safety Canada | Sécurite publique Canada

SAFE RESILIENT CANADA



Update on Canada's Cyber Security Strategy

The Canadian Electricity Association, Regulatory Development Task Group
23 November 2011

Canada

Outline

1. Progress towards the implementation of Canada's *Cyber Security Strategy*

2. Update on the Canadian Cyber Incident Response Centre's (CCIRC) refocused mandate

3. Development of a cross-sectoral non-disclosure agreement (NDA) for improved information sharing

Progress in Implementation

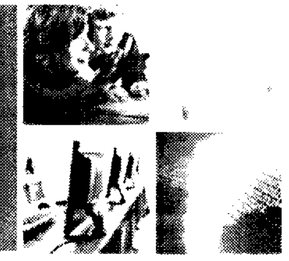
Since the release of the Government of Canada's Cyber Security Strategy in 2010, Public Safety Canada has been working to implement the **three** pillars:

1. **Secure Government systems**
   - Shared Services Canada established to consolidate Government networks
   - Realigned the Government's cyber incident response coordination through the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre

2. **Partner to secure systems outside the Government of Canada**
   - Engaging with critical infrastructure sectors to establish collaborative mechanisms and work-plans, including the development of *Information Sharing arrangements*
   - Strengthening the Canadian Cyber Incident Response Centre's relationships and service offerings
   - Further developing policy and operational partnerships with key allies

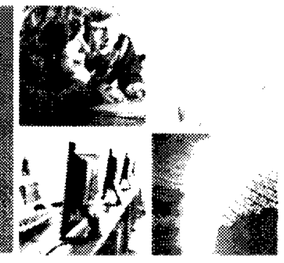
3. **Help Canadians to be secure online**
   - Prepared a nationwide communications campaign "*Get Cyber Safe*" to coincide with Cyber Security Awareness Month in October 2011

Refocusing Canada's Cyber Response



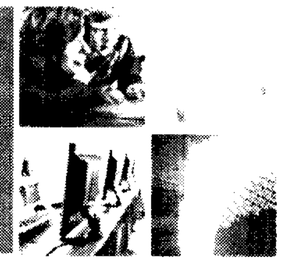
- In mid 2011, responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the *Cyber Threat Evaluation Centre*: the computer emergency response team for federal departments and agencies, charged with protecting government systems
  - CCIRC is now the national computer emergency response team (CERT) for provinces, territories and critical infrastructure sectors.
  - CCIRC is now the designated entity within the Government of Canada entrusted with coordinating the response to cyber security incidents of national interest and protecting critical infrastructure.

CCIRC Services



- **Incident Coordination** between national and international cyber security stakeholders;
- Dissemination of **Cyber Awareness** Products;
- **Notifying** domestic **stakeholders** of compromised systems;
- Malicious sites **takedown**;
- **Analysis** of malicious software;
- **Repatriation** of stolen data;
- Vulnerability **disclosure coordination;**
- **Facilitate** Information **sharing**.

Improved Information Sharing

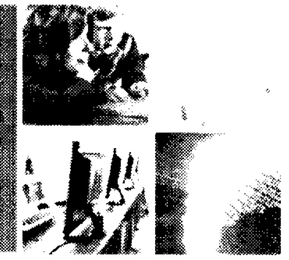


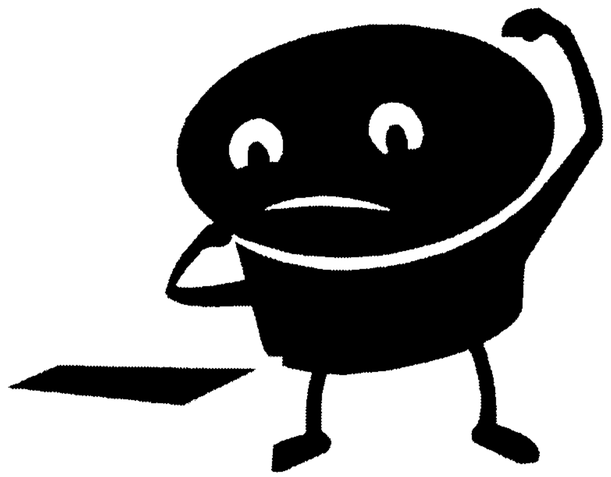
- CEA / CCIRC Non-Disclosure Agreement (NDA) currently being finalized

- NCSD will develop a cross-sectoral (electricity, oil and gas, telecommunications, water, etc.) non-disclosure agreement to facilitate information sharing and strengthen public-private collaboration on cyber security

- Proposed information sharing arrangement will leverage existing products being developed through the National Cross Sector Forum in partnership with the CEA and Public Safety Canada's Critical Infrastructure Protection Division

Questions?





Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

Seen by the DM
Vu par le SM

NOV 28 2011

SECRET/CEO

DATE: NOV 25 2011

File No.: 384125

Thanks

UK seems to be taking this seriously

B.

MEMORANDUM FOR THE DEPUTY MINISTER

THE UNITED KINGDOM'S UPDATED CYBER SECURITY STRATEGY

(Information only)

ISSUE

The United Kingdom (U.K.) has released an updated version of its *Cyber Security Strategy* (The Strategy) today, November 25, 2011. A copy of the Strategy is attached for your reference (**TAB A**).

BACKGROUND

As a reflection of the level of political engagement and visibility accorded to cyber security within the U.K. government, the new governing Conservative – Liberal Democrat Coalition has issued an updated cyber strategy.

Unsurprisingly perhaps, there is a great degree of commonality between the new Strategy and that issued in June 2009 by the previous Labour government. It builds on the U.K.'s October 2010 *National Security Strategy*, which identified cyber as a "tier 1" threat. The updated version commits no new funds to cyber security, other than the £650 million (approximately CAD $1 billion) *National Cyber Security Programme* that is already in place.

The Strategy sets out four high-level goals that the U.K. will seek to achieve by 2015:

- to be one of the most secure places in the world to do business in cyberspace;
- to be more resilient to cyber attacks and better able to protect U.K. interest in cyberspace;
- to help shape an open, stable and vibrant cyberspace that supports open societies; and
- to have the cross-cutting knowledge, skills and capabilities to support the U.K.'s cyber security objectives.

Of note, the new Strategy includes a vision outlining roles for the government, private sector and individuals to play with respect to cyber security. It sets out ambitious objectives for improving information sharing with the private sector within six months, building on the U.K.'s May 2011 *National Incident Response Plan.*

The Strategy makes reference to maintaining and strengthening the U.K.'s ability to anticipate, prepare for and disrupt hostile acts in cyberspace through "proactive defence" disruption activities.

The U.K. will establish a Defence Cyber Operations Group (the Group) within the Ministry of Defence, an interim version of which will be in place by April 2012. Full operational capability of the Group is expected by April 2014. This is an approach similar to that underway within the U.S. and the creation of its Cyber Command.

The Strategy also speaks to the creation, by 2013, of a dedicated cyber crime unit within the National Crime Agency now being stood up. It is believed that this unit will be able to direct even more attention to cyber crime while also better leveraging available resources. With the U.K. having suddenly ratified its signature to the Council of Europe Convention on Cybercrime in May 2011, they may be looking to take a leadership position in this area.

CONCLUSION

It is notable that cyber security is considered significant enough that the new U.K. government wishes to put its own political stamp on a new Strategy. This level of political engagement was also demonstrated at the October 2011 London Conference on Cyberspace, where seven sitting U.K. Cabinet Ministers hosted panels.

The British approach to cyber security remains fundamentally unchanged and continues to align extremely well with Canada's own efforts. The added emphasis given by the U.K. to the economic and national prosperity dimensions of cyber security closely echo Canadian policy discussions, and suggest several opportunities for further cooperation.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

for Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure: (1)

Prepared by: Melanie Mohammed

Protecting and promoting the UK in a digital world

November 2011

Introduction by the Rt Hon Francis Maude MP, Minister for the Cabinet Office 5

Executive summary 7

1. Cyberspace: Driving growth and strengthening society 11

2. Changing threats 15

3. Our vision for 2015 21

4. Action: Meeting threats, taking opportunities 25

Annex A: Implementation 35

- Objective 1: Tackling cyber crime and making the UK one of the most secure places in the world to do business in cyberspace. 36
- Objective 2: Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace. 39
- Objective 3: Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies. 40
- Objective 4: Building the UK's cross-cutting knowledge, skills and capability to underpin all our cyber security objectives. 42

References 43

The growth of the internet has been the biggest social and technological change of my lifetime. It is a massive force for good in the world in the way it drives growth, reduces barriers to trade, and allows people across the world to communicate and co-operate. As we saw this spring in the Arab world, it can help give the unheard a voice and hold governments to account. It will have a huge role to play in supporting sustainable development in poorer countries.

At the same time our increasing dependence on cyberspace has brought new risks, risks that key data and systems on which we now rely can be compromised or damaged, in ways that are hard to detect or defend against.

The UK Government takes these risks seriously. That is why the 2010 National Security Strategy rated cyber attacks as a 'Tier 1' threat and why, despite a tight fiscal situation, we set £650 million aside over four years to develop our response.

We are determined to tackle the threats, but in a way which balances security with respect for privacy and fundamental rights. At home and internationally the UK Government will continue to work to ensure that cyberspace remains an open space – open to innovation and the free flow of ideas, information and expression.

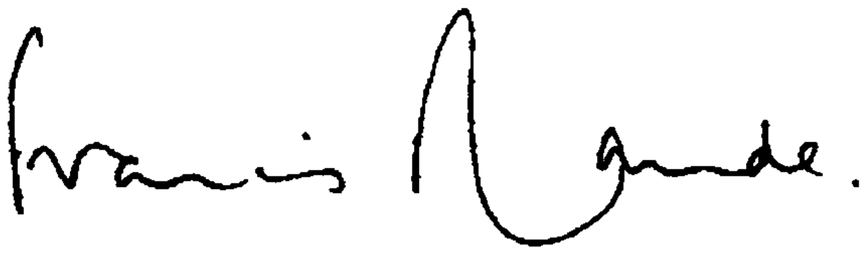
This strategy sets out the actions we will take to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals:

If you are in business this strategy sets out what we will do to help ensure protection of your company; to promote the UK as a good place to do business online; and to foster opportunities for UK cyber security firms to leverage strength at home to sell their products overseas.

If you are an individual concerned about your own personal security from crime, fraud and identity theft this strategy outlines what we will do to tackle these threats and ensure you have the support needed to protect yourself.

In a domain where technology and change are fast-moving, responding effectively will require a consistent and extensive effort. By 2015, the aspiration is that the measures outlined in this strategy will mean the UK is in a position where: law enforcement is tackling cyber criminals; citizens know what to do to protect themselves; effective cyber security is seen as a positive for UK business; a thriving cyber security sector has been established; public services online are secure and resilient; and the threats to our national infrastructure and national security have been confronted.

We will report back next year on progress; in the meantime I would welcome your feedback on this strategy and the plan it sets out. Please send your comments care of the Office of Cyber Security and Information Assurance in the Cabinet Office (ocsia@cabinet-office.x.gsi.gov.uk).



The Rt Hon Francis Maude MP
Minister for the Cabinet Office and Paymaster General

The internet is revolutionising our society by driving economic growth and giving people new ways to connect and co-operate with one another. Falling costs mean accessing the internet will become cheaper and easier, allowing more people in the UK and around the world to use it, 'democratising' the use of technology and feeding the flow of innovation and productivity. This will drive the expansion of cyberspace further and as it grows, so will the value of using it. Chapter 1 describes the background to the growth of the networked world and the immense social and economic benefits it is unlocking.

As with most change, increasing our reliance on cyberspace brings new opportunities but also new threats. While cyberspace fosters open markets and open societies, this very openness can also make us more vulnerable to those – criminals, hackers, foreign intelligence services – who want to harm us by compromising or damaging our critical data and systems. Chapter 2 describes these threats. The impacts are already being felt and will grow as our reliance on cyberspace grows.

The networks on which we now rely for our daily lives transcend organisational and national boundaries. Events in cyberspace can happen at immense speed, outstripping traditional responses (for example, the exploitation of cyberspace can mean crimes such as fraud can be committed remotely, and on an industrial scale). Although we have ways of managing risks in cyberspace, they do not match this complex and dynamic environment. So we need a new and transformative programme to improve our game domestically, as well as continuing to work with other countries on an international response.

Chapter 3 sets out where we want to end up – with the Government's vision for UK cyber security in 2015.

Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.

To achieve this vision by 2015 we want:

Objective 1:

The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace

Objective 2:

The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace

Objective 3:

The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies

Objective 4:

The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives

That means a UK where:

Individuals know how to protect themselves from crime online.

Businesses are aware of the threats they face, their own vulnerabilities and are working with Government, trade associations, and business partners to tackle them. We want to see UK companies building on our strengths to create a thriving and vibrant market in cyber security services around the world. In the current economic climate the UK needs more than ever to identify and exploit areas of international competitive strength to drive growth. We believe that being able to show the UK is a safe place to do business in cyberspace can be one such strength.

Government has: sharpened the law enforcement response to cyber crime; helped the UK take opportunities to provide the cyber security services that will be needed across the world; encouraged business to operate securely in cyberspace; bolstered defences in our critical national infrastructure against cyber attack; strengthened our capabilities to detect and defeat attacks in cyberspace; enhanced education and skills; and established and strengthened working relationships with other countries, business and organisations around the world to help shape an open and vibrant cyberspace that supports strong societies here and across the globe.

To achieve this we have set aside £650 million of public funding for a four-year, National Cyber Security Programme. Chapter 4 sets out what

Government will do, in partnership with the private sector and other countries, to deliver the vision.

As part of this action plan Government will:

Continue to build up in GCHQ and MOD our sovereign UK capability to detect and defeat high-end threats.

Pursue the agenda defined at the recent London Conference on Cyberspace to establish internationally-agreed 'rules of the road' on the use of cyberspace.

Work with the companies that own and manage our critical infrastructure to ensure key data and systems continue to be safe and resilient.

Establish a new operational partnership with the private sector to share information on threats in cyberspace.

Encourage industry-led standards and guidance that are readily used and understood, and that help companies who are good at security make that a selling point.

Help consumers and small firms navigate the market by encouraging the development of clear indicators of good cyber security products.

Hold a strategic summit with professional business services, including insurers, auditors, and lawyers to determine the role they might play in promoting the better management of cyber risks.

Bring together existing specialist law enforcement capability on cyber crime into the new National Crime Agency (NCA). Encourage the use of 'cyber-specials' to make more use of those with specialist skills to help the police.

Build an effective and easy-to-use single point for reporting cyber fraud and improve the police response at a local level for those who are victims of cyber crime.

Work with other countries to make sure that we can co-operate on cross-border law enforcement and deny safe havens to cyber criminals.

Encourage the courts in the UK to use existing powers to impose appropriate online sanctions for online offences.

Seek agreement with Internet Service Providers (ISPs) on the support they might offer to internet users to help them identify, address, and protect themselves from malicious activity on their systems.

Help consumers respond to the cyber threats that will be the 'new normal' by using social media to warn people about scams or other online threats.

Encourage, support, and develop education at all levels, crucial key skills and R&D.

Build a single authoritative point of advice for the public and small businesses to help them stay safe online.

Foster a vibrant and innovative cyber security sector in the UK, including exploring new partnerships between GCHQ and business to capitalise on unique Government expertise.

Because of its links to intelligence and national security, some of the activity the Government has set in train is necessarily classified. The full range of unclassified actions is set out in Annex A.

[redacted]

1. Cyberspace: Driving growth and strengthening society in the UK and around the world

A networked world...

1.1 The internet and digital technologies are transforming our society by driving economic growth, connecting people and providing new ways to communicate and co-operate with one another. The World Wide Web only began in 1991, but today 2 billion people are online[1] – almost a third of the world's population. Billions more are set to join them over the next decade. There are over 5 billion internet-connected devices.[2] $8 trillion changed hands last year in online commerce.[3]

1.2 The internet is already having a profound impact on the way we live our lives. This social change will only grow and gather pace as the number of users increases. Already it looks like it will be on the scale of the very biggest shifts in human history, such as the coming of the railways, or even learning to smelt metals.

Real GDP per capita has risen by $500 over the last 15 years in mature countries enabled by the internet. By comparison, it took 50 years for the industrial revolution to have the same effect.

McKinsey Global Institute, Internet Matters, 2011

...which feeds growth....

1.3 It is easy to see why the growth of the internet has been so dramatic. Cyberspace is transforming business, making it more efficient and effective. It is opening up markets, allowing commerce to take place at lower cost and enabling people to do business on the move. It has promoted fresh thinking, innovative business models and new sources of growth. It enables companies to provide better, cheaper and more convenient service to customers. And it helps individuals to shop around, compare prices and find what they want.

Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services. Digital networks already underpin the supply of electricity and water to our homes, help organise the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK. And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances.

1.4 Developing countries in particular stand to benefit as increasing interconnectivity makes commerce easier and allows access to information, knowledge and education, enabling people to innovate, collaborate and compete in global marketplaces.

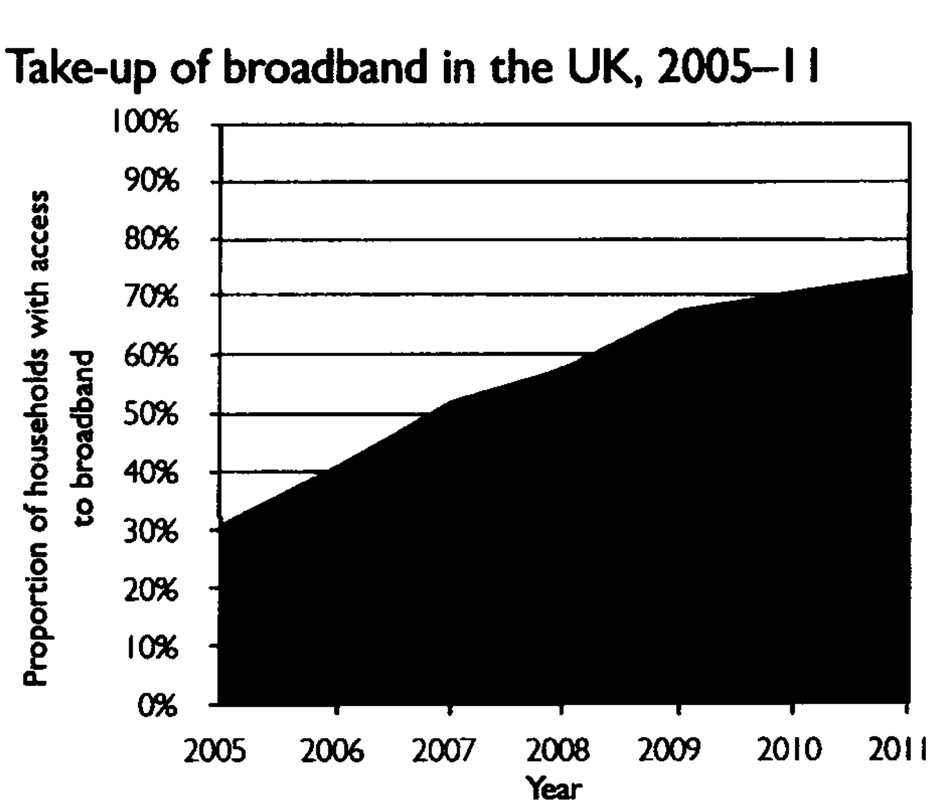
Some 52% of UK consumers with access to broadband use online shopping as an opportunity to save money.

Ofcom, *Communications Market Report*, 2010

1.5 The UK has positively adopted cyberspace as a means of doing business. In 2009, 608 million card payments were made online, with a total spend of £47.2 billion,[4] and in 2011 around 74% of UK

homes had access to broadband, as shown in the graph below (this compares to an EU average of 60.8% in 2010[5]).

Take-up of broadband in the UK, 2005–11



Source: Ofcom

1.6 Recent research suggests that the internet contributes an average of 3.4% of GDP in a range of developed countries[6]. In the UK, the internet accounts for around 6% of GDP: if it were a sector in itself it would be larger than either utilities or agriculture.

1.7 The same research shows that the internet has also played a vital role in driving prosperity, accounting for 21% of GDP *growth* in the last five years in 'mature' countries. Often, small businesses and traditional industries draw the biggest benefits. This study also shows that overall moving trade online has resulted in gains: for every job lost, 2.6 jobs have been created.

1.8 As it has developed, cyberspace has enabled the automation and optimisation of the infrastructure that supports many businesses; for example, the SCADA[7] systems that automatically control and regulate industrial processes such as manufacturing, water distribution, refining and power generation.

1.9 Cost savings for governments resulting from using online services instead of telephone or face-to-face services are substantial.

The creation of a common ICT infrastructure for Government will save £460 million in 2014/15.

Government ICT strategic implementation plan 2011

Universal Credit will provide support to around 19 million citizens across 8.5 million households, and will include provision of online access to benefit-related services and information. Online delivery and greater automation of processes will contribute towards £500 million savings in costs, per year, once Universal Credit is fully operational.

Department for Work and Pensions

... supports open, strong societies...

1.10 Cyberspace also strengthens open societies. It acts as a vast repository for many forms of knowledge. It allows individuals to connect with one another, share ideas and express views, and take new approaches to shared problems. It provides new and more effective ways to participate, allowing larger numbers of people to solve problems, support each other and get involved in the issues they care about. As more people connect to the internet the flow of new and innovative ideas increases. With a reach that continues to expand, cyberspace is becoming 'democratised' and can now enable social change. It is now being used to empower people by making governments more transparent, accountable[8] and efficient in the way they provide public services.[9]

93% of children aged 12-15 now use the internet at home. This group are more likely to say they would miss the internet than television.

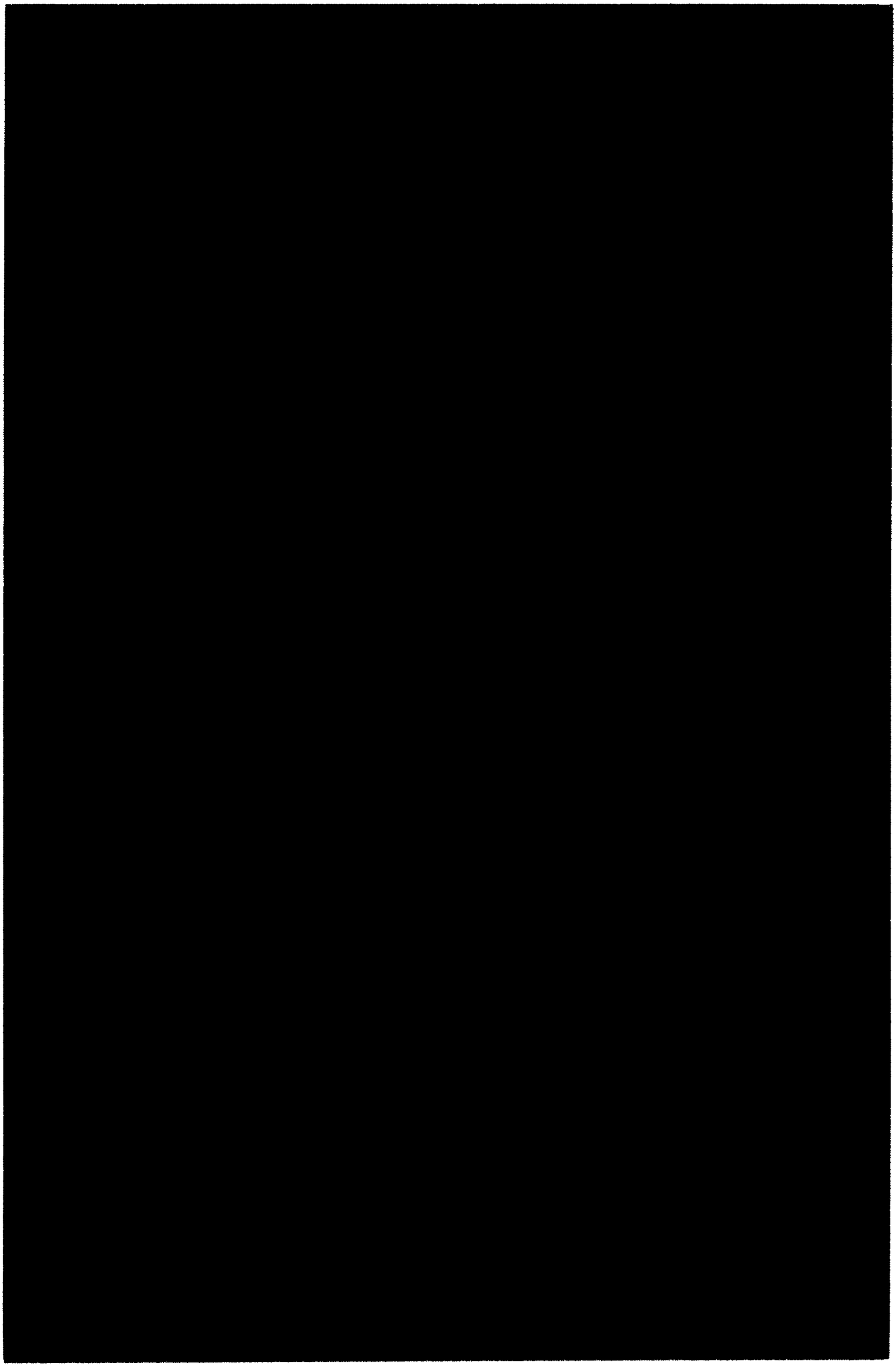
Ofcom, *Children and Parents: Media use report 2011*

...and which will continue to grow

1.11 Since the 1970s, we have witnessed remarkable transformational change that has helped drive the growth of cyberspace. The amount of information created or replicated using

digital technology continues to grow. In 2010 it was estimated to be 1.2 zetabytes and by 2011 it is predicted to grow to 1.8 zetabytes[10] (enough information to fill 380 billion DVDs). A zetabyte is a staggeringly large number – a *billion* terabytes – where a terabyte is typically the largest hard disk available for home computers in 2011.

1.12 But in many ways the most exciting developments in cyberspace are still to come. As more people and organisations around the world connect, it becomes more and more useful in a variety of new and often unexpected ways. The introduction of cloud computing and smart-grids, the continued growth of mobile working and the growth in the number of users of cyberspace each demonstrate that the pace of change will not let up: cyberspace will become increasingly valuable and important to the UK, and to countries across the world.



2. Changing threats

2.1 The internet will become increasingly central to our economy and our society. But the growing role of cyberspace has also opened up new threats as well as new opportunities – we have no choice but to find ways to confront and overcome these threats if the UK is to flourish in an increasingly competitive and globalised world.

2.2 The digital architecture on which we now rely was built to be efficient and interoperable. When the internet first started to grow, security was less of a consideration. However, as we put more of our lives online, this matters more and more. People want to be confident that the networks that support our national security, our economic prosperity, and our own private lives as individuals are safe and resilient.

2.3 Unfortunately a growing number of adversaries are looking to use cyberspace to steal, compromise or destroy critical data. The scale of our dependence means that our prosperity, our key infrastructure, our places of work and our homes can all be affected. For this reason the Government's 2010 National Security Strategy identified cyber attacks on the UK as a 'Tier 1' threat – that is, as one of our highest priorities for action.

What are the threats?

2.4 **Criminals** from all corners of the globe are already exploiting the internet to target the UK in a variety of ways. There are crimes that only exist in the digital world, in particular those that target the integrity of computer networks and online services. But cyberspace is also being used as a platform for committing crimes such as fraud, and on an industrial scale. Identity theft and fraud online now dwarf their offline equivalents. The internet has provided new opportunities for those who seek to exploit children and the vulnerable. Cyberspace allows criminals to target the UK from other jurisdictions across the world, making it harder to enforce the law. As businesses and government services move more of their operations online, the scope of potential targets will continue to grow.

2.5 Some of the most sophisticated threats to the UK in cyberspace come from other **states** which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes. 'Patriotic' hackers can act upon states' behalf, to spread disinformation, disrupt critical services or seek advantage during times of increased tension. In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home.

2.6 Cyberspace is already used by **terrorists** to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile physical attacks, the threat that they might also use cyberspace to facilitate or to mount attacks against the UK is growing. We judge that it will continue to do so, especially if terrorists believe that our national infrastructure may be vulnerable (the recently published CONTEST[11] strategy sets out our approach to terrorism).

2.7 The threat to the UK from politically-motivated activist groups operating in cyberspace is real. Attacks on public and private sector websites and online services in the UK orchestrated by **'hacktivists'** are becoming more common, aimed at causing disruption, reputational and financial damage, and gaining publicity.

2.8 All these different groups – criminals, terrorists, foreign intelligence services and militaries – are active today against the UK's interests in cyberspace. But with the borderless and anonymous nature of the internet, precise attribution is often difficult and the distinction between adversaries is increasingly blurred.

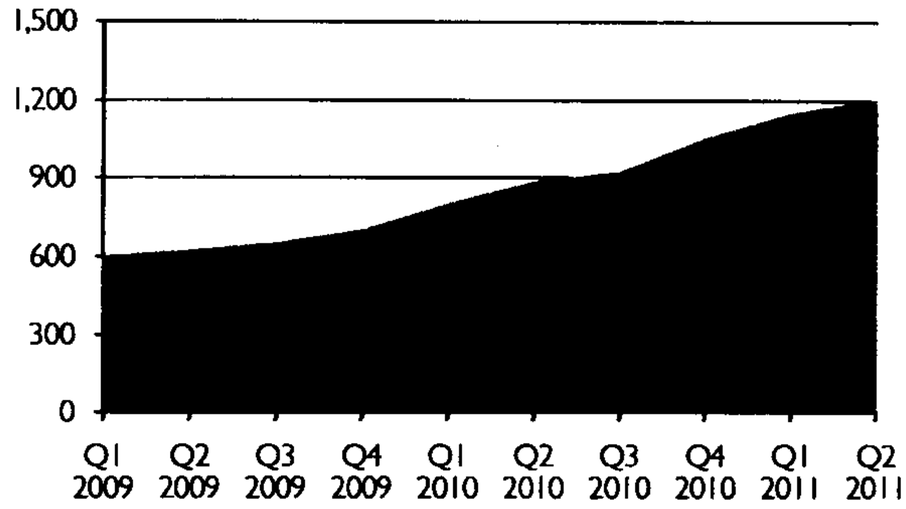
Affecting businesses

2.9 Organisations are not always aware of the new vulnerabilities that dependence on cyberspace can bring. Intellectual property and other commercially sensitive information (for example, business strategies) can be attractive targets. This risks undermining the strengths of the UK's research base and intellectual property as important drivers of growth. Services relying on, or delivered via, cyberspace can be taken offline by criminals or others, damaging revenue and reputations.

In the spring of 2011, Sony announced that criminals had successfully targeted the PlayStation network, compromising the personal details of up to 100 million customers and resulting in the network shutting down for several weeks. The costs to Sony are expected to total $171 million.

2.10 As the digital connections between organisations and individuals proliferate (for example through shared or sub-contracted services), incidents can affect larger numbers of individuals and organisations. Recent research suggests that the costs to the UK of cyber crime could be in the order of £27 billion per year[12]. A truly robust estimate will probably never be established, but it is clear the costs are high and rising. Cyber criminals have demonstrated their ability to adjust quickly to new developments like smart-phones (see graph above). The collective impact of this threat now has the potential to cause significant damage to online economies.

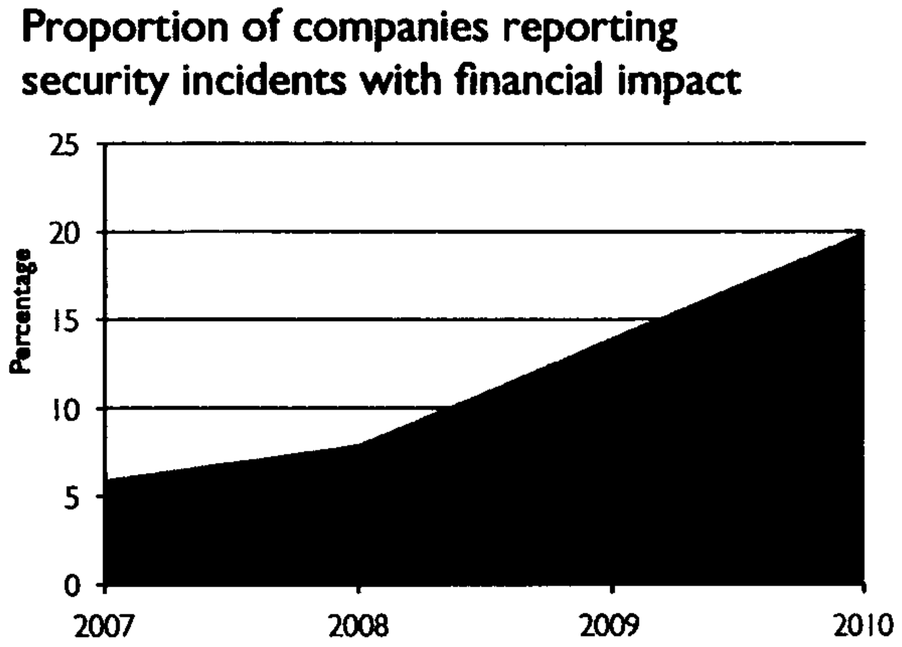
Total number of malware variants targeting smart phones



Source: data from McAfee, as cited in *The Economist, October 2011.*

2.11 The chart below demonstrates the growing impact of information security incidents on businesses worldwide. Maintaining confidence in e-commerce as a viable way of doing business is crucial. Investors, businesses, government and particularly customers each need to be confident that networks are safe to use if the UK is to realise its full potential for growth.

Proportion of companies reporting security incidents with financial impact



Source: *Pricewaterhouse Coopers. Global state of information security survey, 2011*

2.12 But staying secure in cyberspace can seem complex, difficult and expensive. Without a clear and shared understanding of the nature and scale of threats and vulnerabilities, the case for investing in protection and prevention can be undermined.

Affecting national security

2.13 Cyberspace has now grown to become a domain where strategic advantage – industrial or military – can be won or lost. It underpins the complex systems used by commerce (for example, banking, the delivery of food and the provision of utilities such as power and water) and the military. The growing use of cyberspace means that its disruption can affect nations' ability to function effectively in a crisis.

Nearly two-thirds of critical infrastructure companies report regularly finding malware designed to sabotage their systems.

McAfee, Critical infrastructure protection report, March 2011

2.14 Some states regard cyberspace as providing a way to commit hostile acts 'deniably'. Alongside our existing defence and security capabilities, the UK must be capable of protecting our national interests in cyberspace.

"There are over 20,000 malicious emails on government networks each month, 1,000 of which are deliberately targeting them."

Iain Lobban, Director of Government Communications Headquarters, 2010

These kinds of attack are increasing; the number of emails with malicious content detected by government networks in the whole of 2010 was double the number seen in 2009.

Cabinet Office, 2011

Affecting individuals and societies

2.15 In order to get the most from the internet, it is important that people feel confident that it can be used safely. As all of us make more use of the internet in our work and private lives it makes for a more attractive target for criminals or others. Any reduction in trust towards online communications can now cause serious economic and social harm to the UK.

2.16 Beyond the impact on individuals, the scale of the use of cyberspace means that it can now also affect society more broadly. We have a strong tradition in the UK of protecting our citizens in ways that are guided by core values of liberty, fairness, transparency and the rule of law. These values help define who we are, what we do and what it means to be British. The interconnected nature of cyberspace and its expansion mean that it has developed to promote many of these values.

2.17 The conventions and norms covering conduct within the cyber domain are still developing. While this helps make it the vibrant domain that it is today, it can also cause instability and uncertainty about accountability. The blurring of boundaries in cyberspace increases the risk of actions affecting larger numbers of people and organisations unintentionally. At its most serious, this leads to the potential for unpredictable and large-scale shocks.

2.18 Actions to strengthen our national security must also be consistent with our obligations, such as those concerning freedom of expression; the right to seek, receive and impart ideas; and the right to privacy. Defending security should be consistent with our commitment to uphold civil liberties. Of course, these are well-established and ongoing debates, but cyberspace can bring them into focus in new ways, and more quickly than in other areas.

2.19 These changes do not affect the UK alone. We believe that the global reach of the internet and digital technologies can provide an important means for the spread of ideas, with profound implications for societies. But like any communications medium, cyberspace can also potentially be used to restrict liberty and undermine freedoms. Some states and organisations are already seeking to control and restrict the future development of the cyber domain. These attempts are ultimately doomed to fail. But for as long as they last they are holding back progress and reducing social benefit. The UK will continue to work with like-minded states around the world to maximise the extent to which the world can fully realise and enjoy the benefits that cyberspace will offer.

A complex problem

2.20 The growing adoption of the internet and new uses of digitally connected technologies make for a fast moving and complex environment, which brings its own challenges:

- Cyberspace is largely commercially owned and driven, and global in nature.
- The systems that form cyberspace contain a vast array of components, sourced from a global and diverse range of suppliers. Multiple sub-contractors produce, test, package and assemble these components.
- Predicting and understanding how cyberspace will be used in future is difficult given the rate of innovation and change.
- New vulnerabilities and risks will emerge suddenly.
- The pace of events can make existing defences and responses look slow and inadequate. Along with the complexity of cyberspace, this makes attributing hostile actions difficult.
- The covert nature of the threat means that the public and businesses can underestimate the risks.

Existing capacity to meet the challenge

2.21 In tackling these problems we are not starting from scratch. The UK is well placed to respond to many of the challenges that cyberspace presents. Our private sector, key government agencies, and academia all have world-leading strengths in cyberspace; we must bring these together to capitalise on the opportunities and get the most for the UK:

- The UK has strong international alliances based on shared values and common interests.
- Our sound domestic legal framework and regulatory environment mean that the UK has the basis to respond to cyber crime and similar threats to the UK. We need to promote a similar environment internationally.
- The UK already has ways to exchange information with the private sector on the risks emerging from cyberspace, and to tackle cyber crime.
- Some of the specific technical and specialist expertise needed to help us achieve our cyber security objectives already exists in the UK.
- In particular GCHQ, the Government's signals intelligence agency, has some world-class skills at its disposal.
- We already have some businesses with strengths in cyber security.
- Information assurance already plays an important role in reducing our vulnerabilities in cyberspace.

2.22 But *government* capacity, though it includes these real strengths, is not sufficient or sufficiently scaled to meet the growing security challenges of the digital age. Although government already provides advice to organisations that run our infrastructure on how to manage the risks in cyberspace, the adoption of this approach needs to be broader. Our current capacity to enforce the law is too distributed, meaning that criminals still regard exploiting cyberspace as a profitable and low-risk option.

2.23 As for *business*, some firms recognise the growing scale and impact of the risks. However, some sectors of the economy, particularly small and medium sized businesses, do not have access to the skills and knowledge to protect themselves online. We need to improve our understanding of the threat across the board and manage it more effectively. This can mean relying upon skills and knowledge, not often found in the same place.

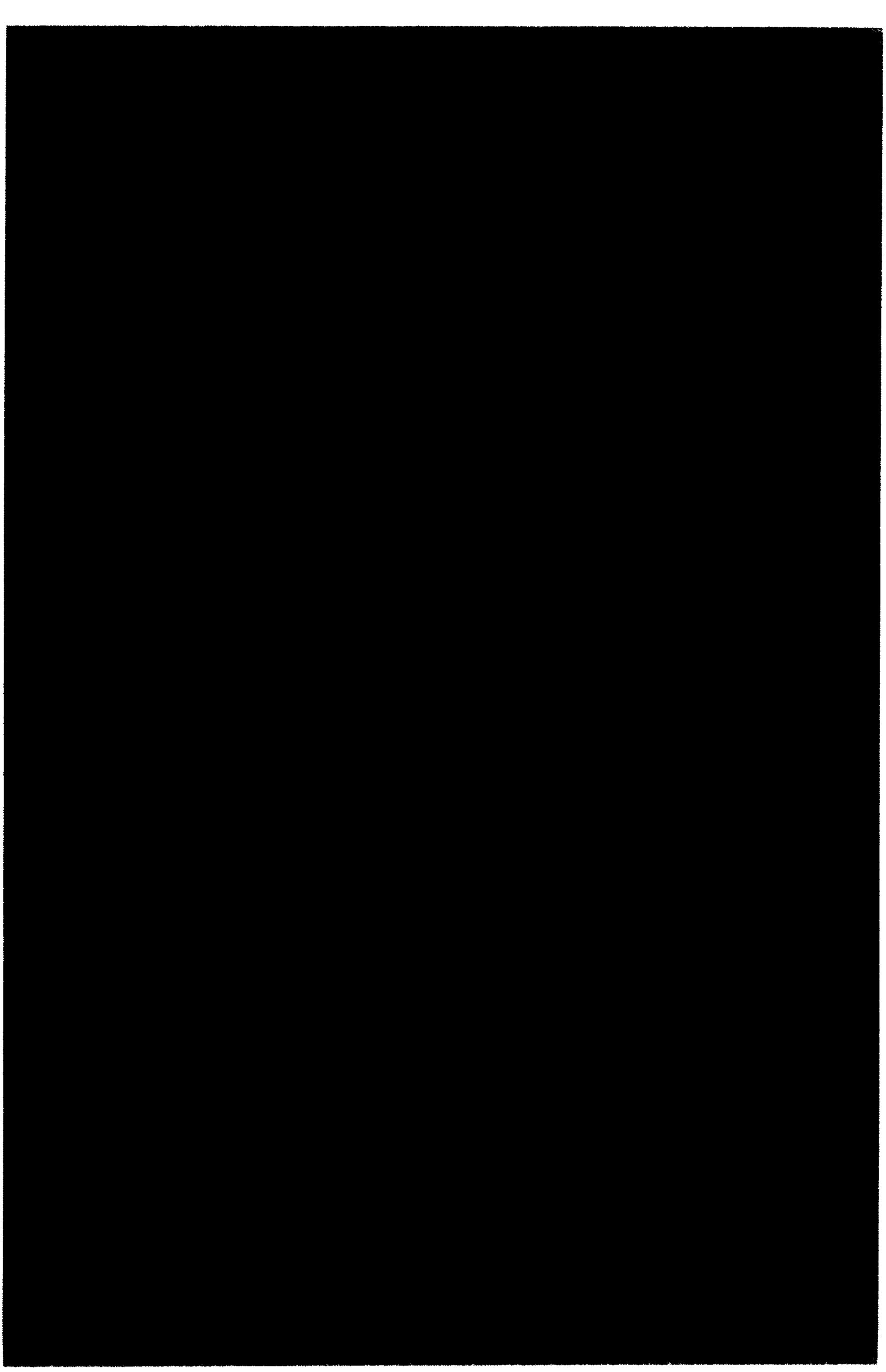
2.24 We also recognise that there are challenges in ensuring that the *public* has access to the information and skills they require in order to understand the threat and take actions to operate safely online. More needs to be done to ensure that the current provision of information is coordinated across Government, and with the private sector.

2.25 We do have a body of internationally agreed principles, behaviour and law which applies to cyberspace. The International Covenant on Civil and Political Rights sets out some of the key obligations. But there remains more to be done

with *other countries* to establish the practical implications of applying existing principles to cyberspace. At a practical level, not all countries have appropriate legislation to allow them to work together to tackle threats from crime in cyberspace.

2.26 The technical capabilities that enable a wide range of actions to protect the UK need strengthening. But it is clear that our approach to the risks in cyberspace must not rely on technical measures alone. Changes in attitudes and behaviours will also be crucial to operating safely in cyberspace.

2.27 It is clear that cyberspace is changing the world. The huge benefit that this brings also means new vulnerabilities. This dynamic and changing profile of risk demands a new approach.



3. A vision for UK cyber security in 2015

3.1 In order to secure the vast economic and social benefits that cyberspace will offer the UK we will transform our approach to cyber security. This section sets out our vision for the UK in 2015 and identifies the principles that will shape our work. The next chapter shows how we will use our existing strengths and the new National Cyber Security Programme to achieve our goals.

Our vision

Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.

Our objectives

Our objectives are for:

Objective 1:

The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace

Objective 2:

The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace

Objective 3:

The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies

Objective 4:

The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives

Our principles

A risk based approach

3.2 In a globalised world where all networked systems are potentially vulnerable and where cyber attacks are difficult to detect, there can be no such thing as absolute security. We will therefore apply a risk-based approach to prioritising our response.

Working in partnership

3.3 Though the scale of the challenge requires strong national leadership, Government cannot act alone. It must recognise the limits of its competence in cyberspace. Much of the infrastructure we need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business-driven.

3.4 Similarly, though we can improve our defences domestically, the internet is fundamentally transnational. Threats are cross-border. Not all the infrastructure on which we rely is UK-based. So the UK cannot make all the progress it needs to on its own. We will seek partnership with other countries that share our views, and reach out where we can to those who do not.

Balancing security with freedom and privacy

3.5 At home we will pursue cyber security policies that enhance individual and collective security while preserving UK citizens' right to privacy and other fundamental values and freedoms.

3.6 Internationally the UK will continue to pursue the development of norms of acceptable behaviour in cyberspace. We start from the belief that behaviour which is unacceptable offline should also be unacceptable online. Our position will be guided by the principles proposed by the Foreign Secretary in February 2011 and reiterated at the London Conference on Cyberspace this November:

- The need for governments to act proportionately in cyberspace and in accordance with national and international law.
- The need for everyone to have the ability – in terms of skills, technology, confidence and opportunity – to access cyberspace.
- The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas.
- The need to ensure that cyberspace remains open to innovation and the free flow of ideas, information and expression.
- The need to respect individual rights of privacy and to provide proper protection to intellectual property.
- The need for us all to work collectively to tackle the threat from criminals acting online.
- The promotion of a competitive environment which ensures a fair return on investment in network, services and content.

Roles and responsibilities

3.7 Achieving this vision will require everybody, the private sector, individuals and government to work together. Just as we all benefit from the use of cyberspace, so we all have a responsibility to help protect it.

Individuals

3.8 Ordinary people have an important role to play in keeping cyberspace as a safe place to do business and live our lives. By 2015 we want a UK where:

- People know how to get themselves a basic level of protection against threats online. They have access to accurate and up to date information on the online threats that they face, and the techniques and practices they can employ to guard against them.
- Individuals are careful about putting personal or sensitive information on the internet; are wary of email attachments or links from unrecognised senders; and are cautious about downloading files from websites they know little about.
- Everyone, at home and at work, can help identify threats in cyberspace and report them – for example, identifying fraudulent websites.
- Individuals play their part in transacting safely with businesses and Government, protecting passwords, understanding the importance

Pages 239 to / à 248

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

Canada's Cyber Security Strategy – One Year Later

December 1, 2011

National Cross Sector Forum

Canada

Canada's Cyber Security Strategy: setting broad objectives

Goals of resource allocation	*Canada's Cyber Security Strategy*	Support national priorities
Strengthen capability	**Pillar 1**: Secure Government systems	National security
Build credibility	**Pillar 2**: Partner to secure vital cyber systems outside the Government of Canada	Economic prosperity
Promote awareness	**Pillar 3**: Help Canadians to be secure online	Quality of life

Progress on Pillar 1: Secure Government systems

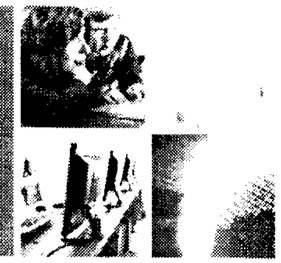
Strengthen security of federal information and systems

- Limited increase to investigative and analytical capability
- Consolidated internet access points
- Division of cyber security roles
  - Communications Security Establishment Canada established the Cyber Threat Evaluation Centre as the Government of Canada computer emergency response team
  - The Canadian Cyber Incident Response Centre (CCIRC) is now the national computer emergency response team for provinces, territories and critical infrastructure sectors

Establish policy capacity

- Public Safety Canada established National Cyber Security Directorate
- Creation of a governance structure to provide strategic guidance

Progress on Pillar 1: Secure Government systems – cont'd



Strengthen international cyber security activities

- Directly supports domestic objectives and progress being made
- Valued partner on furthering cyber policy issues (e.g., London Conference on Cyberspace)
- Deep engagement with the United States (U.S.) on Perimeter Vision and working with the Department of Homeland Security (DHS) on shared briefings to critical infrastructure sectors

Shared Services Canada

- Effective August 4, 2011, the Government streamlined and consolidated its information technology (IT) architecture in the areas of email, data centres and networks
- Will produce savings and reduce the Government's footprint; strengthen security and the safety of Government data to ensure Canadians are protected; and realize economies of scale and make it more cost-effective to modernize these IT services

Progress on Pillar 2: Partner to secure vital cyber systems outside the Government of Canada

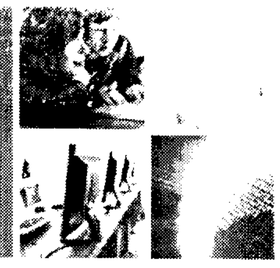
Partner with private sector and critical infrastructure

- Progress is being made
  - cross-sector briefings, regional workshops on industrial control systems, developing information sharing frameworks
  - initial focus: telecommunications, energy transmission, financial

Develop leading-edge science and technology

- Defence Research and Development Canada continues to pursue several research and development projects, and is currently developing a Memorandum of Understanding with DHS on cyber research and development initiatives

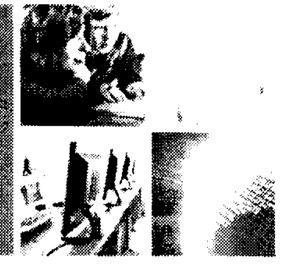
Progress on Pillar 2: Partner to secure vital cyber systems outside the Government of Canada – cont'd



Meetings with Provincial and Territorial Governments

- Initiated dialogue to strengthen intergovernmental engagement on cyber security.
- Key objectives from a federal perspective:
  - clarify national operational roles and responsibilities;
  - improve information sharing;
  - engage critical infrastructure and private sectors;
  - ensure a better informed population by maximizing resources and leveraging provincial and territorial access to the public;
  - establish a forum for consultation on legislative and policy undertakings; and
  - explore interest in the development of a national cyber incident response framework

Progress on Pillar 2: Partner to secure vital cyber systems outside the Government of Canada – cont'd



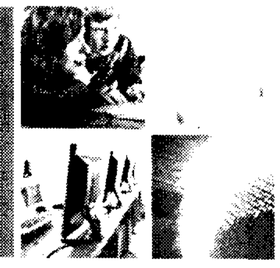
Canadian Security Telecommunications Advisory Council

- CSTAC is comprised of senior executives from the public and private sectors. It provides a forum to:
  - exchange information;
  - collaborate strategically on current and evolving issues that may affect the confidentiality, integrity or availability of the telecommunications infrastructure; and
  - provide advice on measures to address these issues

Financial Sector

- Ongoing discussions with Finance Canada on an engagement strategy for the financial sector
- Initial presentation provided to the Canadian Financial Institution – Computer Incident Response Team, Executive Meeting with the objective of initiating a dialogue leading to a permanent relationship

Progress on Pillar 2: Partner to secure vital cyber systems outside the Government of Canada – cont'd

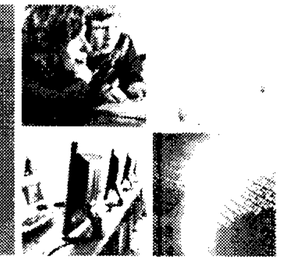


Energy Sector

- Coordinating engagement with U.S. agencies with Natural Resources Canada, such as the North American Electric Reliability Corporation and the Federal electric Reliability Corporation, to ensure Canadian views on cyber security in the energy production sector are transmitted to the U.S. government
- Developing a work plan with the Canadian Electricity Association and their members to facilitate the exchange of information with CCIRC

National Cross-Sector Forum

Progress on Pillar 3: Help Canadians to be secure online



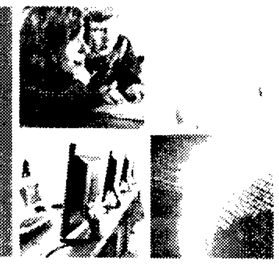
Promote public awareness, education and engagement

- Public awareness campaign launched by Public Safety Canada
  - baseline public opinion research undertaken, brand developed, and campaign launched
  - **getcybersafe.ca** launched with practical information for Canadians
  - expanded partnerships being pursued with provinces and territories, industry, and international allies
- Government-wide incident communications protocol being developed
- Communications working groups established with international partners and at the federal, provincial, and territorial level
  - Will consider both public awareness and incident communications

Cyber Crime

- The Royal Canadian Mounted Police has established Cyber Fusion Centre to improve statistics on cyber crime

Progress on Pillar 3: Help Canadians to be secure online – cont'd



Legislation

- Passed two pieces of legislation to enhance cyber security
  - Anti-Spam Bill:
    - Seeks to deter the most damaging and deceptive forms of spam from occurring in Canada
    - Authorizes the creation of a spam reporting centre
  - Bill S-4:
    - Amends the *Criminal Code* to create three new offences related to identity theft, with five-year maximum sentences
    - Authorizes courts to order offenders to pay restitution to a victim of identity theft as part of their sentence
- Examining ways to provide law enforcement with modernized investigative tools to address cyber crimes

BUILDING A **SAFE** AND **RESILIENT CANADA**

Government of Canada / Gouvernement du Canada

Canada

Get Cyber Safe

GetCyberSafe.ca

Français | Home | Contact Us | Help | Search | Canada.gc.ca

Home

- **Know the Risks**
  - Online Activities
  - Common Threats
  - Scams and Fraud
- **Protect Yourself**
  - Protect Your Identity
  - Protect Your Money
  - Protect Your Family
- **Protect Your Devices**
  - Computers, Laptops and Tablets
  - Mobile Devices
  - Home Networks
  - Storage
- **Resources**

GETCYBERSAFE

Make cyber safety a personal priority with tips and resources to help protect everything that's important to you.

Share | Email

Search

GetCyberSafe Video

See the Ad

It Happened to Me

Here's your chance to share your story and read about others' experiences. By passing along any helpful information you've

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

Canada's Cyber Security Strategy

The North American Cyberspace: Strengthening Cross-border Cyber Infrastructure

December 1, 2011

Polytechnic Institute of NYU, New York, U.S.A.

Canada

Government of Canada Initiatives

BUILDING A **SAFE** AND **RESILIENT CANADA**

- *Consultation Paper on a Digital Economy Strategy for Canada* (May 2010)

- *National Strategy and Action Plan for Critical Infrastructure* (May 2010)

- *Canada's Cyber Security Strategy* (October 2010)

Canada's Cyber Security Strategy

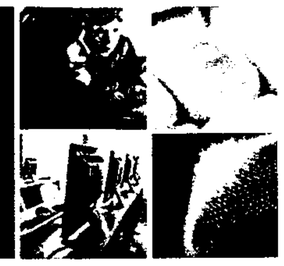
BUILDING A **SAFE** AND **RESILIENT CANADA**

- Signals cyber security as a priority investment for the Government of Canada

- Coordinates and unifies domestic and international action

- Built on three pillars:
  1. Secure Government systems
  2. Partner to secure systems outside the Government of Canada
  3. Help Canadians to be secure online

Progress on Implementation - Highlights



BUILDING A **SAFE** AND **RESILIENT CANADA**

- Consolidating Government IT infrastructure
- Strengthening relationships with critical infrastructure and industry
- Engaging international allies and domestic partners
- Updating laws to reflect the realities of the digital world
- Cyber security public awareness campaign

Public Awareness Campaign

BUILDING A **SAFE** AND **RESILIENT CANADA**

Government of Canada | Gouvernement du Canada

Canada

Get Cyber Safe

GetCyberSafe.ca

Know the Risks

Online Activities

Common Threats

Scams and Fraud

Protect Yourself

Protect Your Identity

Protect Your Money

Protect Your Family

Protect Your Devices

Computers, Laptops and Tablets

Mobile Devices

Home Networks

Storage

Resources

GETCYBERSAFE

Make cyber safety a personal priority with tips and resources to help protect everything that's important to you.

GetCyberSafe Video

See the Ad

It Happened to Me

Here's your chance to share your story and read about others' experiences. By passing along any helpful information you've

Canada-U.S. Cooperation

BUILDING A **SAFE** AND **RESILIENT CANADA**

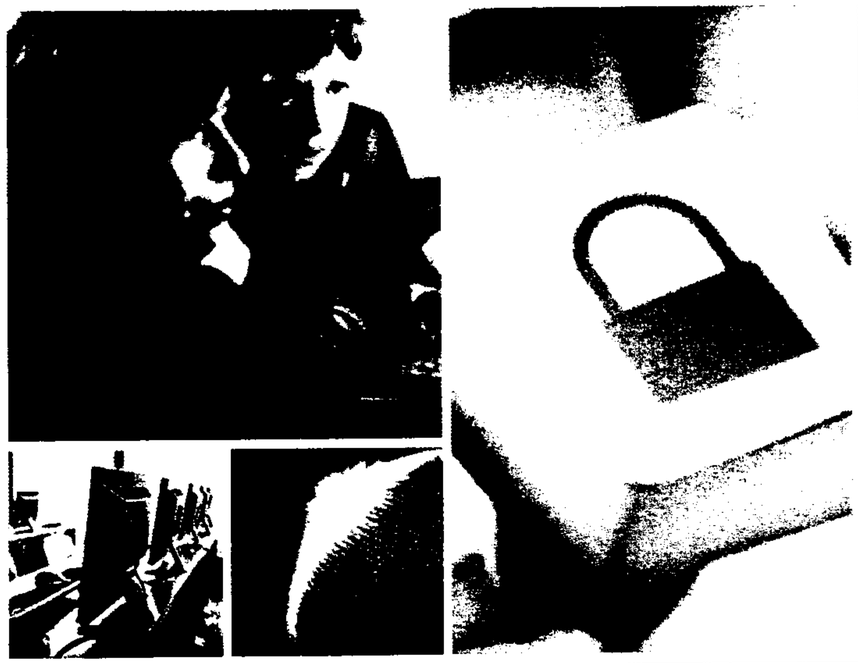
- Long history of bilateral cooperation on cyber security and critical infrastructure protection

- Crosses long-standing joint activities in public safety, law enforcement, military, intelligence, and diplomatic domains

- Cyber issues are drawing increasing attention and have accelerated bilateral work across many domains

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

Canada

Pages 267 to / à 273

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Dec 09 2011

Public Safety Canada / Sécurité publique Canada

Assistant Deputy Minister / Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

s.14(a)

DATE:

File No.: 382294
RDIMS No.: 484388

MEMORANDUM FOR THE DEPUTY MINISTER
c.c.: Paul MacKinnon, Assistant Deputy Minister, SPB

[redacted]

Canada

.../2

Page 275

is withheld pursuant to section

est retenue en vertu de l'article

14(a)

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

I approve:

_____
William V. Baker

Prepared by: Semira Selman

Pages 277 to / à 281

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Pages 282 to / à 288

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

International Approaches to Cyber Governance

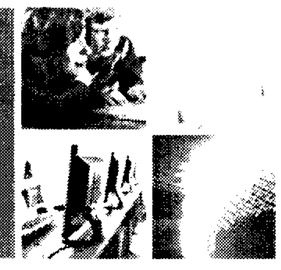
Public Safety Canada

January 2011

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

Canada

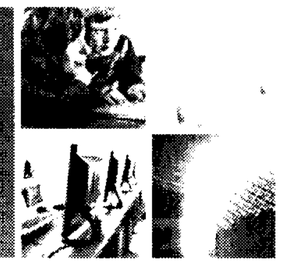
International Approaches to Cyber Governance



How Canada Views Cyberspace

- Cyber security and economic prosperity
- Cyberspace as a fundamental societal building block
- Similarities and contrasts with allies
  - Cyber security drivers
  - Cyber leadership: civilian vs. military

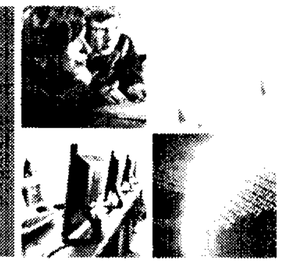
International Approaches to Cyber Governance



The Strategy and International Priorities, Engagement

- International efforts link to domestic objectives
- Activity in international cyber governance fora: ITU; IGF; ICANN; and others.

International Approaches to Cyber Governance

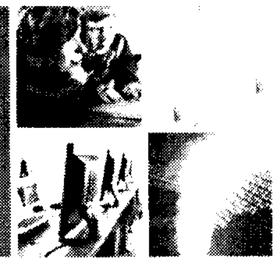


Specific Initiatives Canada Advances

- Norms
- Internet Governance
- Openness to new ideas, initiatives

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

International Approaches to Cyber Governance



- Cyber crime
- Intellectual Property
- Norms
- Critical Infrastructure

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

Pages 294 to / à 299

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Page 300

is withheld pursuant to sections

est retenue en vertu des articles

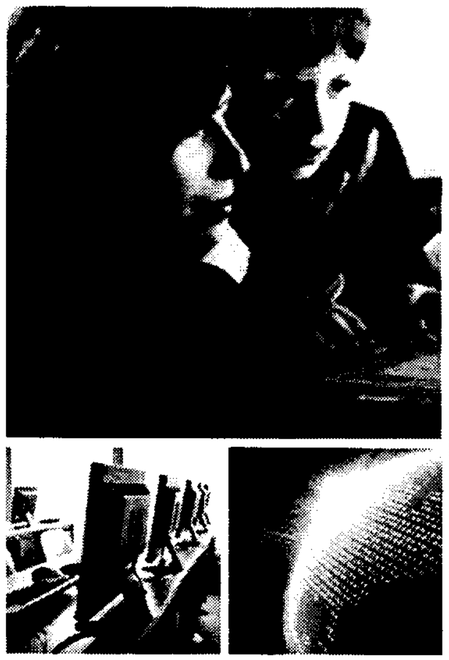
15(1) - Subv, 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



Cyber Security in Canada

Federal Roles and Responsibilities

January 2012

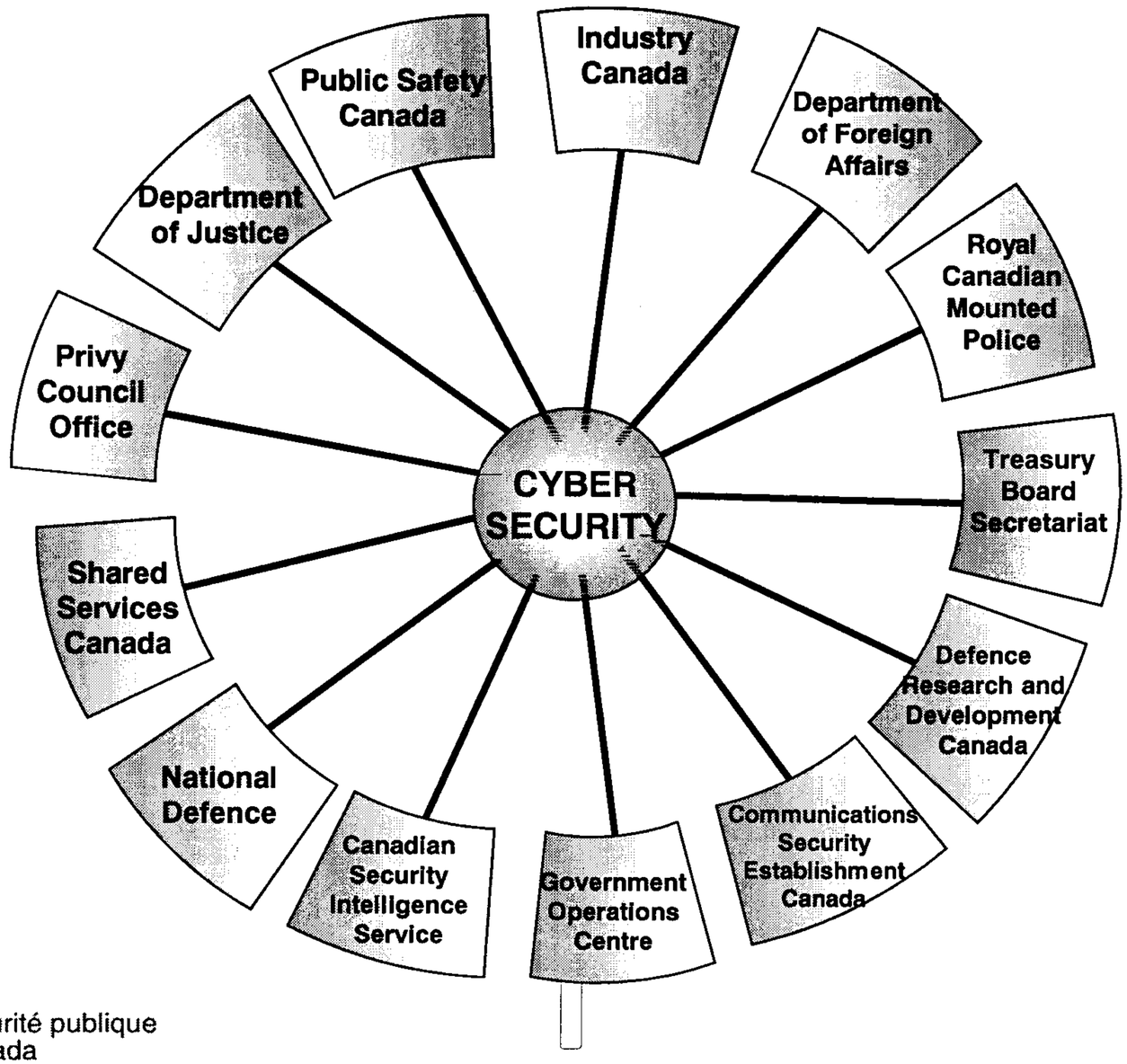
s.15(1) - Int'l

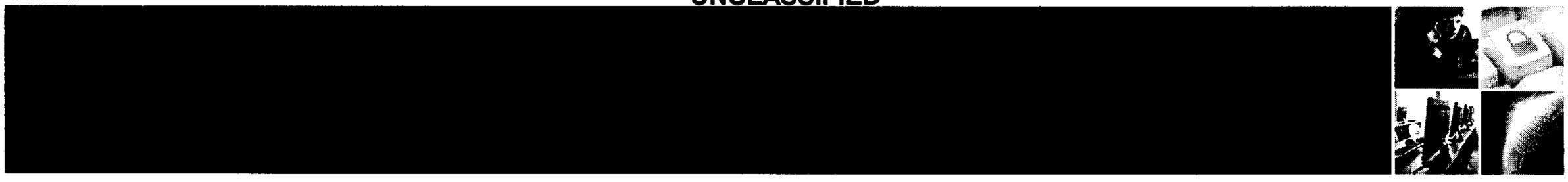
s.15(1) - Subv

Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

Cabinet





- Sets Government of Canada policy and provides political direction on issues requiring their attention.

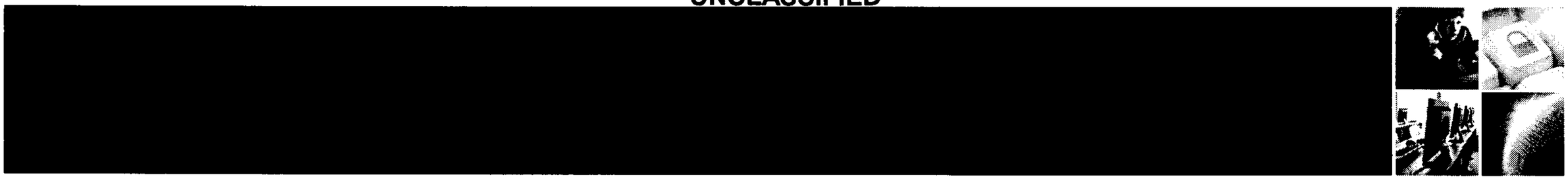
- Two Cabinet Committees specifically address cyber security:

Cabinet Committee on National Security

- Chaired by the Prime Minister.
- Provides broad strategic direction for security and foreign policy related to Canada's national interest.
- Oversees Canada's national security response activities.

Cabinet Committee on Foreign Affairs and Defence

- Chaired by the Minister of National Defence.
- Considers foreign affairs, international development, public and national security, and defence policy issues.



- Leads and coordinates the implementation of *Canada's Cyber Security Strategy*.

- Leads the Canadian Cyber Incident Response Center (CCIRC).
  - Canada's national Computer Emergency Response Team
  - Provides assistance and mitigation advice to the provinces, territories, and critical infrastructure.

- Leads the cyber security public awareness campaign.

BUILDING A **SAFE** AND **RESILIENT CANADA**

GOC-COG

ROLE: On behalf of the Government of Canada, supports response coordination of events affecting the national interest

- Strategic, whole-of-government
- All-hazards including cyber
- Works to support PMO, PCO, Deputy Ministers (DM) and departments and agencies
- Principle tool of DM and ADMs to coordinate government response
- Harmonizes collective actions in response to events
- Monitoring, triage, assessment, planning, response coordination

- Responsible for spectrum management and ensuring a robust telecommunications system.
  - Helps industry to secure their networks and ensure continuity of communications during an emergency.

- Responsible for ensuring a safe and secure online marketplace.
  - Maintains policy oversight for Canada's privacy protection and anti-spam legislation.

- Chairs the Canadian Security Telecommunications Advisory Committee.
  - Committee the federal government uses to engage the telecommunications industry on cyber security.

- Represents Canada at international Internet and telecommunications fora (e.g. Internet Governance Forum, International Telecommunication Union).

- Provides legal advice to Departments and agencies on cyber-related policy and law.

- Provides policy leadership on criminal law and information sharing matters, including cyber crime.

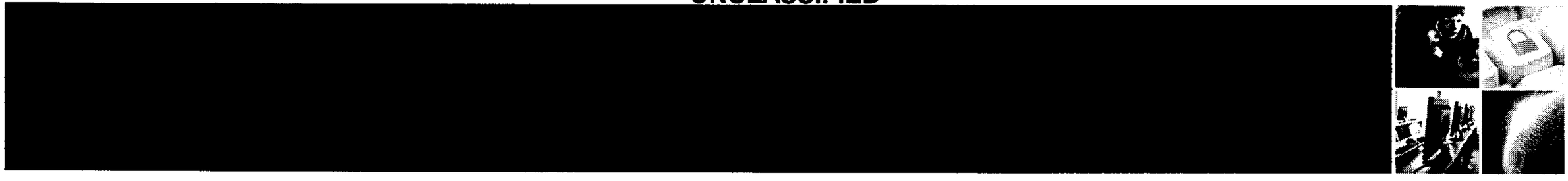
BUILDING A **SAFE** AND **RESILIENT CANADA**

- Canada's national police service and an agency of the Public Safety portfolio.

- Leads investigations into suspected cyber crime activity in Canada.

- Operates the Cyber Crime Fusion Center.

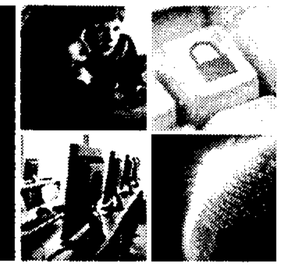
- Assists domestic and international partners with advice and guidance on cyber crime investigations.



- Represents Canada internationally at a number of multilateral venues where cyber is discussed (e.g. United Nations, Organisation for Security and Cooperation in Europe).

- Provides situational awareness on ongoing international cyber discussions.

- Positions Canada internationally to defend and promote its foreign policy interests related to cyber security.



Department of National Defence and the Canadian Forces

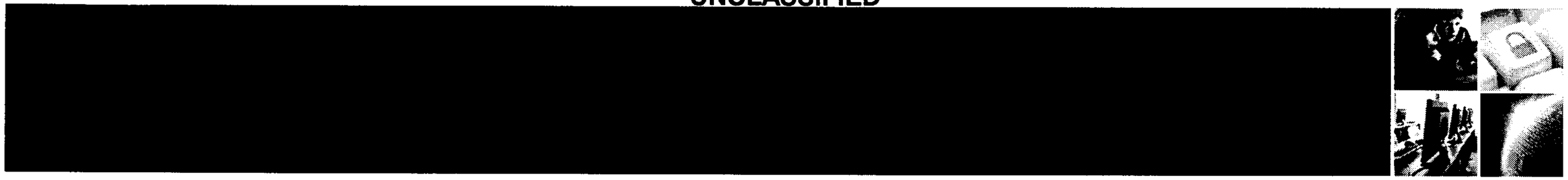
- Provides situational awareness on cyber threats and incidents.

- Provides options analysis for a potential military response in the event of a critical cyber attack.

Defense Research and Development Canada

- Leads the development of military cyber security science and technology in support of the Canadian Forces.

- Leads civilian cyber security research to support the Government of Canada, the private sector, and academia.



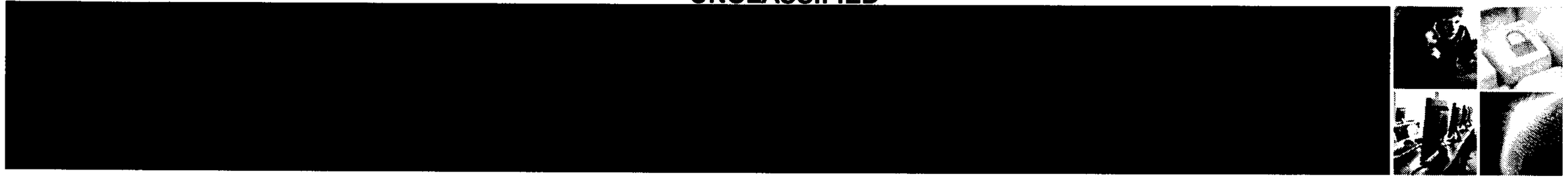
BUILDING A **SAFE** AND **RESILIENT CANADA**

Communications Security Establishment Canada

- Canada's signals intelligence agency.
- Provides advice to help protect government systems and those of importance to the government.

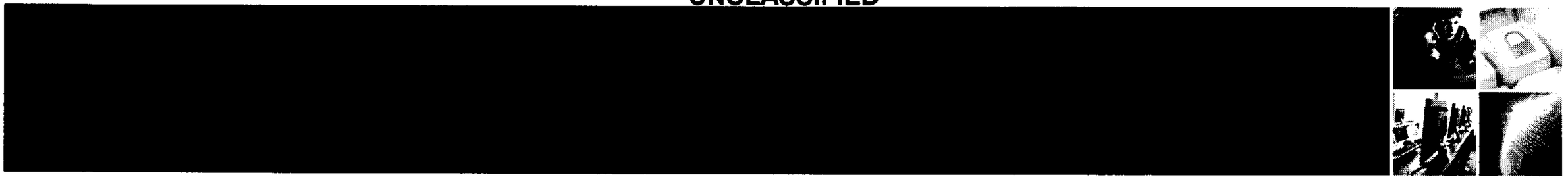
Canadian Security Intelligence Service

- Provides situational awareness and advice on cyber threats.
- Conducts national security investigations.



- Effective August 4, 2011, the Government streamlined and consolidated its IT architecture in the areas of email, data centres and networks.

- Shared Services Canada will:
  - Produce savings and reduce the Government's footprint;
  - Strengthen the security and safety of Government data; and
  - Realize economies of scale.



- Sets government-wide priorities for securing government information technology (IT) systems and networks.

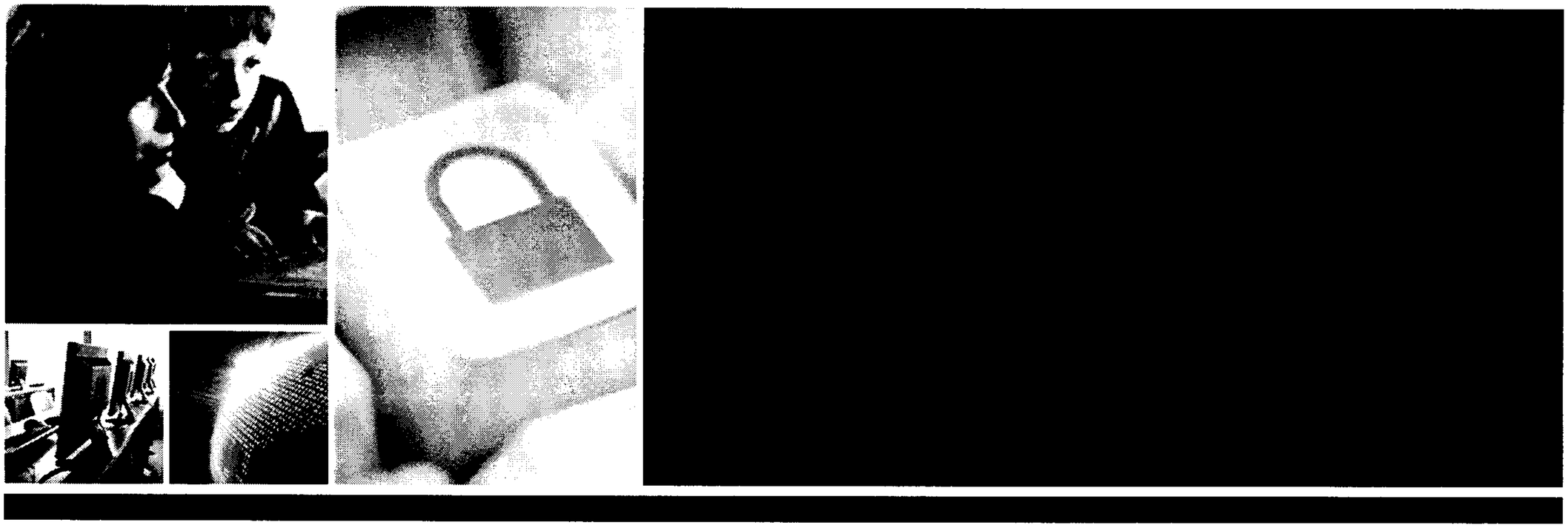
- Develops information technology policy for the federal government.
  - IT Policy developed by the Treasury Board Secretariat is implemented across all federal departments.

- Directs and oversees the information technology incident management plan for federal government systems.

- Provides oversight of post-mortem reviews and lessons learned in the event of a cyber incident affecting federal government systems.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



Canada

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

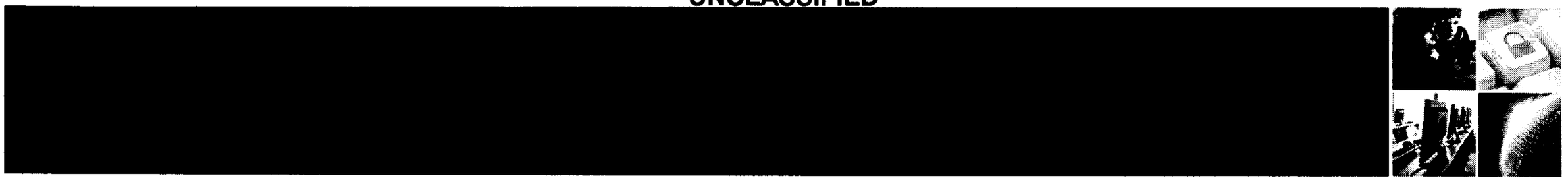
Canada's Cyber Security Strategy

One Year Later

January 2012

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

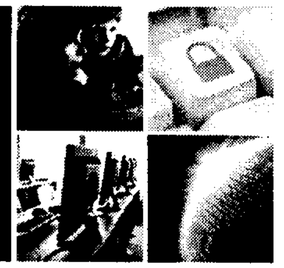
Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**

- Launched in October 2010.
- Signals cyber security as a priority investment for the Government of Canada.
- Coordinates and unifies domestic and international action.
- Built on three pillars:
  1. Secure Government systems.
  2. Partner to secure systems outside the Government of Canada.
  3. Help Canadians to be secure online.

[redacted]

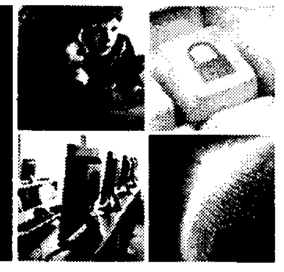


s.15(1) - Int'l
s.15(1) - Subv

- Establish clear federal roles and responsibilities.

- Strengthen security of federal information and systems.
  - Improve cyber hygiene throughout government.
  - [redacted]

- Strengthen international cyber security activities.
  - Deeper engagement with allies and partners
  - Focused engagement at international fora.



- Partner with provinces and territories.

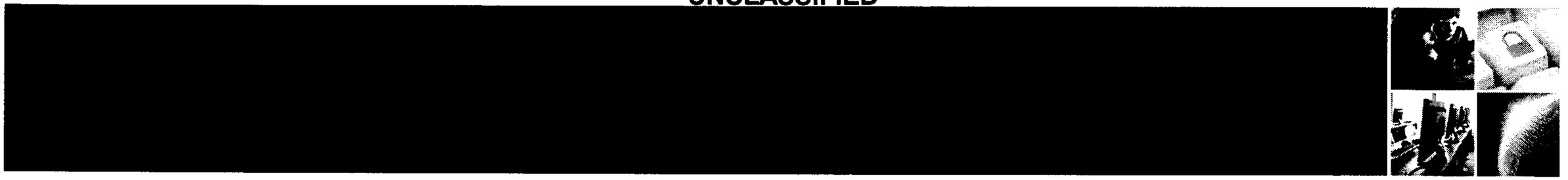
- Partner with critical infrastructure sectors.
  - Greater public-private collaboration through existing organisations.
  - Establish public-private partnerships if required.
  - Focus on three sectors: energy, telecommunications, and finance.

- Develop leading edge cyber security science and technology.
  - Leverage existing research networks to strengthen research and development.

- Promote public awareness, education, and engagement.
  - Launch of the get cyber safe.ca campaign.

- Strengthen legislative framework to address cyber crime.
  - Preparation of legislation to permit the ratification of the Budapest Convention.

- Enhance law enforcement capabilities.
  - Establish a Cyber Crime Fusion Center at the Royal Canadian Mounted Police to improve cyber crime statistics.



- Updating laws to reflect the realities of the digital world.

- Developed cyber security public awareness campaign.

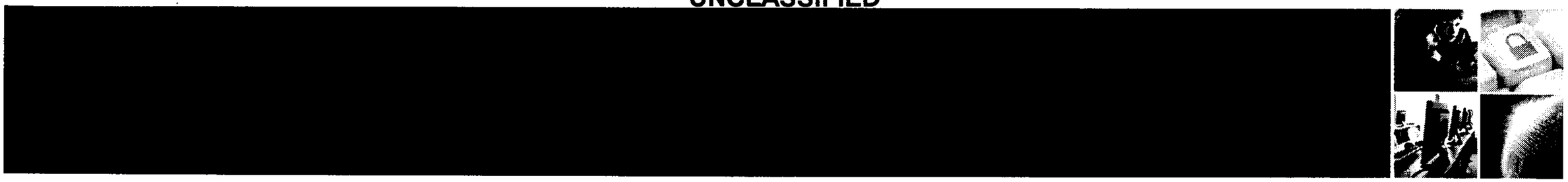
- Strengthening Canada's Computer Emergency Response Team.

- Streamlined and consolidated Government information technology (IT) infrastructure, and created Shared Services Canada.

s.14(a)

- [redacted]

- Using the National Cross Sector Forum and creating the Canadian Security Telecommunications Advisory Council to engage the private sector on cyber security.



- Passed two pieces of legislation to enhance cyber security.
  - Anti-Spam Bill:
    - Seeks to deter the most damaging and deceptive forms of spam from occurring in Canada.
    - Authorizes the creation of a spam reporting centre.
  - Bill S-4:
    - Amends the *Criminal Code* to create three new offences related to identity theft, with five-year maximum sentences.
    - Authorizes courts to order offenders to pay restitution to a victim of identity theft as part of their sentence.

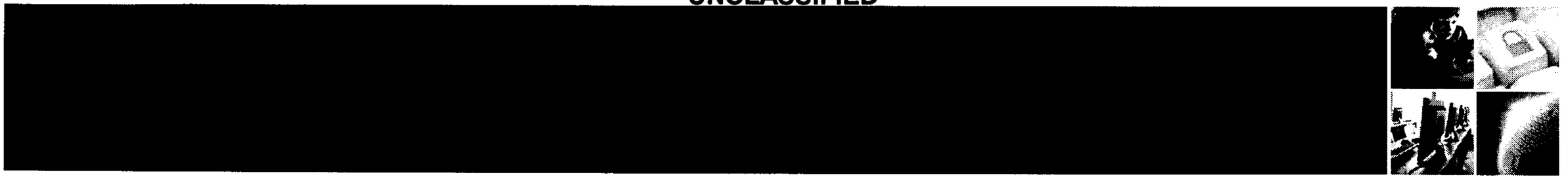
- Examining ways to provide law enforcement with modernized investigative tools to address cyber crimes (e.g. Budapest Convention).

- Provides Canadians with information on cyber threats in order for them to take action to protect themselves and their personal information.

- Includes advertising, a cyber-specific website, marketing partnerships and international coordination of messaging, as well as issues management in response to cyber incidents.

- Was launched in October to coincide with Cyber Security Awareness Month and the one-year anniversary of the Strategy.

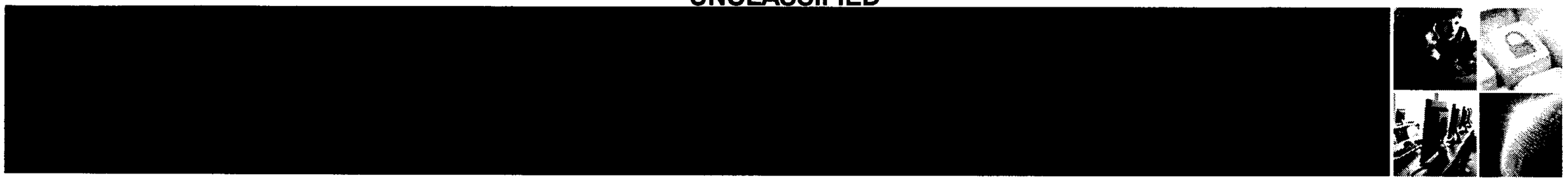
GETCYBERSAFE.CA



- On June 20, 2011, Canada's Canadian Cyber Incident Response Centre (CCIRC) became the national computer emergency response team for provinces, territories and critical infrastructure sectors.

- Moving to 15/7 operations for greater coverage.

- Integrated into the National Cyber Security Directorate at Public Safety Canada for greater operational and policy collaboration.



- Effective August 4, 2011, the Government streamlined and consolidated its IT architecture in the areas of email, data centres and networks.

- Shared Services Canada will:
  - Produce savings and reduce the Government's footprint;
  - Strengthen the security and safety of Government data; and
  - Realize economies of scale.

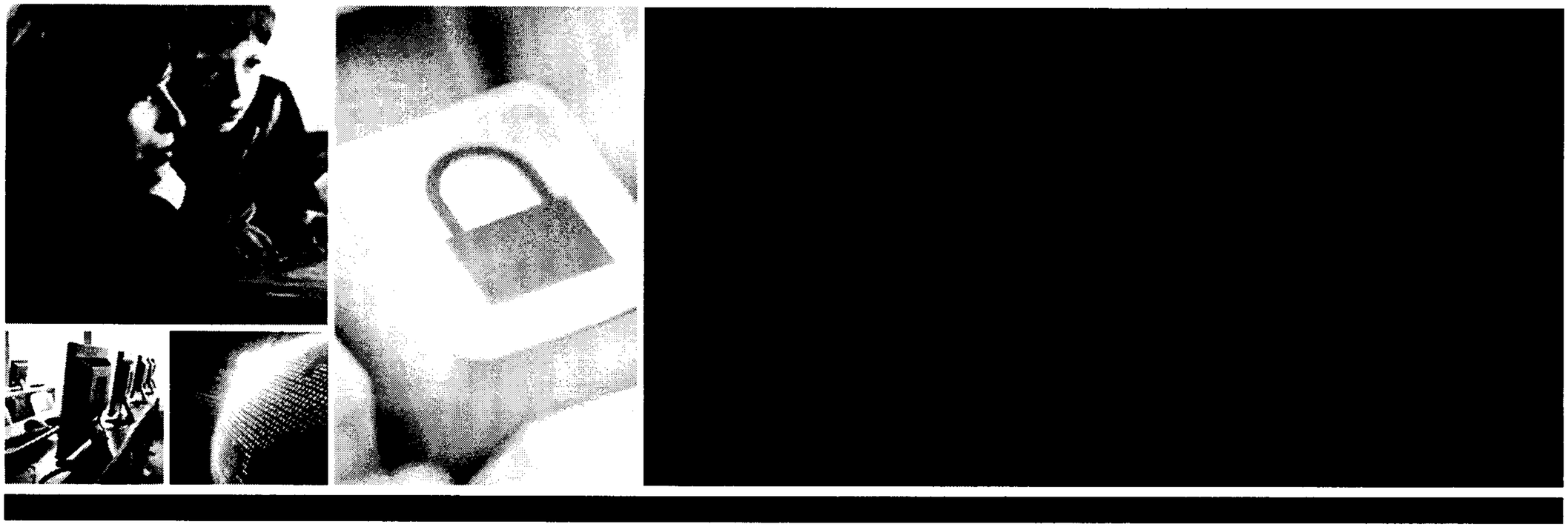
- Initiated dialogue with provincial and territorial interlocutors to strengthen intergovernmental engagement on cyber security.
- Key issues identified:
  - Clarify national operational roles and responsibilities;
  - Improve information sharing;
  - Better awareness raising; and
  - Possible development of a national cyber incident response framework.

- National Cross Sector Forum is comprised of representatives from the federal, provincial, and territorial governments, and critical infrastructure sectors to:
  - Establish an information sharing framework for sensitive information within the private sector and with government.
  - Identify key assets and critical systems.
  - Identify key interdependencies and vulnerabilities.

- The Canadian Security Telecommunications Advisory Committee is comprised of senior executives from the public and private sectors to:
  - Exchange information; and
  - Collaborate strategically on issues that may affect the confidentiality, integrity or availability of Canada's telecommunications infrastructure.

Public Safety Canada | Sécurité publique Canada

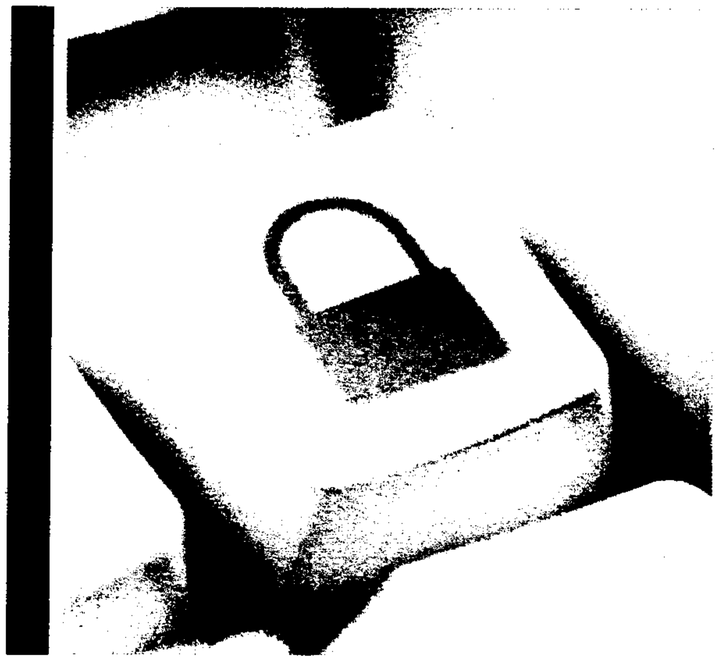
BUILDING A **SAFE** AND **RESILIENT CANADA**



Canada

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



Canadian Cyber Incident Response Centre (CCIRC)

January 2012
RDIMS: 538454

Canada

Objectives

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Brief on CCIRC – what it is, who it is, what it does
- Discuss challenges and opportunities
- Seek agreement on way forward

CCIRC – what it is

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Incident response centre
  - primary contact point into Government for domestic and international partners
  - CCIRC subject matter experts respond 9-5, 5 days a week
  - after hours coverage by Government Operations Centre
- Computer lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors

CCIRC – who it is

BUILDING A **SAFE** AND **RESILIENT CANADA**

- 22 FTEs, 14 staffed
  - mainly highly specialized computer specialists (CS) with knowledge of IT security, computer forensics, and incident handling
  - 4 positions to be staffed for analysis of multi-source intelligence and technical data and writing strategic assessments
- Organized into three functions:
  - Incident Handling – assists partners in identifying, mitigating, and managing incidents
  - Technical Support – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis
  - Strategic Initiatives and Situational Awareness – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers

CCIRC – what it does

BUILDING A **SAFE** AND **RESILIENT CANADA**

These partners…

Government S&I community

Critical Infrastructure

Provinces and territories

Five Eyes and International CERTs

Trusted vendors

Academia

Cyber security expert community

Open source

provide information to…

CCIRC

which provides these services:

Incident Handling and National Event Coordination and Assistance
- Direct technical assistance to partners and coordination of Government response to cyber events of national significance
- Audience: technical staff in partner organizations responding to cyber incidents
- Metric: 749 incidents responded to in 2011; 197 notifications to partners of compromised systems, 9 requests issued to shut down malicious systems in Nov/Dec 2011

Provision of Mitigation Advice
- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice
- Audience: technical staff in partner organizations
- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

Reporting and Analysis
- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis
- Audience: technical staff, decision makers (under development)

Current challenges

- Incident Handling and National Event Coordination and Assistance
  - we can't say no – difficult to prioritize clients and services without clearly defined mission and mandate; prospective client base too broad

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

  - ambiguity of roles in an emergency – absence of a national emergency policy for cyber creates ambiguity for Government and Public Safety
  - limited profile – increased awareness of CCIRC and a credible brand will increase incident reporting
- Provision of Mitigation Advice
  -
  - people – attraction and retention of specialized, bilingual, TOP SECRET staff an ongoing challenge
  - policy – sharing sensitive information
  -
- Reporting and Analysis
  - strategic analysis product for broader audience to be developed

Progress in 2011 – work underway within NCSD

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Incident Handling and National Event Coordination and Assistance
  - 6 positions staffed this year; 8 remaining to attain full complement of 22; process underway for 4 more CS03s
  - working with U.S. on plan to inventory and explore potential alignment of information products (e.g., flashes, alerts, technical reports) (NCSD*)
- Provision of Mitigation Advice
  - initiated investment in lab infrastructure
    - $420K this fiscal for some updated technology

s.16(1)(b)

  - [redacted]
  - launched development of secure web portal for info exchange with CI / PT
  - information-sharing MOUs under development with selected PTs and CI sectors (NCSD*)
- Reporting and Analysis
  - working with S&I community on potential joint products (NCSD*)

Near term objectives (January – March)

BUILDING A **SAFE** AND **RESILIENT CANADA**

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

- Incident Handling and National Event Coordination and Assistance
  - initiate discussions with PTs on national cyber incident response (NCSD*)
  - conduct federal tabletop exercises to clarify roles in a national response (NCSD*)

[redacted]

  - develop standardized training regime and integration packages (NCSD*)
- Provision of Mitigation Advice
  - increased engagement with PT and private sector partners (NCSD*, CCIRC)
  - launch secure portal as repository for CCIRC products and mitigation advice (CCIRC)
  - work with corporate branch on short-term accommodations plan for CCIRC
- Reporting and Analysis
  - identification of partner requirements and defining new products and services (NCSD*)

* Other divisions within NCSD engaged or leading

Near term objectives (cont.): Define mission space

BUILDING A **SAFE** AND **RESILIENT CANADA**

FOR DISCUSSION ONLY

Proposed 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, mitigation, and response to cyber events.

CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

Medium term objectives (April - September)

- Incident Handling and National Event Coordination and Assistance

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

  - [redacted]
  - conduct tabletop exercise with willing PTs and CI sector representatives to advance national cyber incident response framework and identify policy issues
  - begin implementation of alignment of information products with US-CERT

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

[redacted]

- Provision of Mitigation Advice
  - work with corporate branch on long-term accommodations plan for CCIRC and NCSD

s.16(1)(b)

[redacted]

  - explore options for [redacted] more technology
- Reporting and Analysis
  - pilot production of new products and services for new audiences (CCIRC)

Where CCIRC fits in *Canada's Cyber Security Strategy*

BUILDING A **SAFE** AND **RESILIENT CANADA**

Securing Federal Government Systems

Key actors:
- CSEC
- Shared Services
- TBS CIOB
- CF

Partnering to Secure Vital Systems Outside the Federal Government

Key actors:
- PS CCIRC, NCSD, CISCD
- CI Sector lead departments

Existing effort:
- PT, select CI (telecom, energy, finance)
- U5 CERTs

Future effort:
- trusted vendors
- international CERTs
- remaining CI sectors
- economic interests
- academia

Helping Canadians to be Secure Online

Key actors:
- PS Communications
- law enforcement
- Industry Canada
- CRTC
- Privacy Commissioner
- Competition Bureau

Audiences:
- Home users
- Academia
- Small business

State-sponsored cyber espionage ← ***Risk*** → **Crime**

Jan 4 2012

UNCLASSIFIED

INFORMATION BRIEFING NOTE FOR 228th PJBD: CANADA-UNITED STATES CYBER SECURITY COOPERATION

SUMMARY

- Canada and the United States cooperate extensively on cyber security issues across the public safety, military, and security and intelligence domains.

- The Cyber Security Working Group of the Emergency Management Consultative Group, co-chaired by the Department of Homeland Security and Public Safety Canada, coordinates cross-border activities across the various departments and agencies with a cyber security mandate.

- Priority areas for improvement identified within several bi-national forums include: operational cyber security coordination between governments; coordinated information sharing between governments and external partners, in particular the private sector and critical infrastructure; and coordinated public messaging both for citizen awareness and incident-related communications.

BACKGROUND

- Information Technology (IT) networks permeate virtually all areas of our society. Such systems underlie all economic and social activity and are indispensable for how governments manage their military, law enforcement, intelligence and national security functions. No singular federal department or agency is responsible for managing these various cyber security aspects, so each government faces a challenge in ensuring effective coordination of activities.

- Canada and the United States (U.S.) are engaged in a number of bilateral and multilateral initiatives and organizations that address cyber security issues. These include the Emergency Management Consultative Group (EMCG), the Beyond the Border initiative, the 2+2 forum of Deputies of public safety and defence, [redacted] and the Usual-5 forum of national cyber operations centres.

- The Cyber Security Working Group, first established under the EMCG and co-chaired by Public Safety Canada (PS) and the Department of Homeland Security (DHS), coordinates the activities of the departments and agencies engaged in cross-border activities through a joint action plan. This governance structure reflects the fact that, in Canada, the Minister of Public Safety is the Canadian government lead for cyber security coordination while DHS has the responsibility within the American Government of working with state and local governments, the private sector, academia, and international partners to assess, mitigate, and respond to cyber risks.

s.15(1) - Int'l

s.15(1) - Subv

- Three broad areas have been identified as priorities for further collaboration and enhancement:

    - operational cyber security coordination between our governments, in particular information sharing and coordination of cyber incident response between our respective national cyber operations centres;

    - improving information sharing with the private sector and critical infrastructure, including both incident-related material and regular briefings and presentations, so that it is done in a coordinated fashion between governments to ensure consistent messaging;

    - cyber-incident related public communications and public awareness activities should be coordinated bi-nationally to make them mutually reinforcing.

- Considering the significant extent to which critical infrastructure is shared and interconnected across the Canada-U.S. border, and the number of companies operating on both sides of the border and receiving information from both governments, improved cross-border coordination is paramount. It should be stated that provincial and state governments frequently collaborate, and citizens have access to both federal governments' wide range of public messages and services, further emphasizing the importance of cross-border coordination in our cyber security efforts.

CONSIDERATIONS

- These cooperation efforts are not without their challenges, and improving information sharing could be particular complex. It is recognized some sensitive information is difficult to share, both nationally and bi-nationally. However, the vast majority of cyber security information and situational awareness could and should be shared. While seamless coordination may be unrealistic, a significantly higher level of cooperation is possible both for operations and more generally as concerns external communication.

COMMENT

- The Cyber Security Working Group is actively managing this cross-border activity and developing a joint action plan that will ensure good coordination across the various departments and agencies involved in cyber security.

Prepared by:	Andrew McAllister, Public Safety Canada, 613 991 7002
Consulted:	Corey Dvorkin, Public Safety Canada, 613 990 9608
Responsible Director General:	Robert Dick, Public Safety Canada, 613 990 2661
Responsible Group Principal:	Lynda Clairmont, Public Safety Canada, 613 990 4976
Date Prepared:	January 4, 2012

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

For your meeting with:
Deputy Ministers Committee on Cyber Security
On: January 12, 2012

SECRET – with attachments

COPY

DATE:

File No.: 384919
RDIMS No.: Dragon 1075

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

(Information only)

ISSUE

You will be presenting two items at the inaugural meeting of the Deputy Ministers Committee on Cyber Security (DM Cyber), which is scheduled to take place on January 12, 2012, from 14:00 to 15:00 in the 19th floor boardroom at 269 Laurier Avenue West.

A copy of the DM Cyber agenda is enclosed for your ease of reference (**TAB 1**).

CURRENT STATUS

TAB 4: Cyber Security Roles and Responsibilities – 14:30 (10 minutes)
For information
Responding to a request made at the November 8, 2011 meeting of select DMs, you will present on roles and responsibilities of departments with respect to cyber security. This item follows the network hygiene item being presented by the Treasury Board of Canada Secretariat, and will be presented for information. The item occupies ten minutes on the agenda, including questions and answers, beginning at 14:30.

The roles and responsibilities of Government departments and agencies are generally understood for responding to a cyber incident affecting a Government network, though some clarification is necessary owing to the launch of Shared Services Canada. In the case of a cyber incident affecting an external entity, however, roles, responsibilities and capabilities are less clear.

A series of tabletop exercises beginning on January 13, 2012, will help to provide the necessary clarity, and identify policy and operational barriers for information sharing. Additionally, these exercises will support Public Safety Canada's initiative to establish a national cyber incident response framework, which would clarify the roles and responsibilities of Government, provincial and territorial partners, and private sector entities.

TAB 3: [redacted] **14:40 (5 minutes)**
For information

[redacted]

NEXT STEPS

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Mr. Corey Dvorkin, A/Director, Policy and Issues Management, at 613-990-9608.

Robert Dick
Director General
National Cyber Security Directorate

Enclosures: (3)

Prepared by: Melanie Mohammed

.../3

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

s.15(1) - Int'l

s.15(1) - Subv

Deputy Ministers Committee on Cyber Security

January 12, 2012 – 14:00 to 15:00
19th floor boardroom, 269 Laurier Avenue West

AGENDA

	Time	Item	Associated Documentation
	14:00	**Opening Remarks**	
1.	*5 min*	William Baker, Deputy Minister, Public Safety	N/A
		Deputy Ministers Committee on Cyber Security	
		William Baker, Deputy Minister, Public Safety	
	14:05	*For decision: Agree upon the proposed role and scope of the*	
2.	*5 min*	*Committee; and discuss Committee forward agenda.*	Draft Terms of Reference
		Network Hygiene	
		Michelle D'Auray, Secretary of the Treasury Board,	
		Treasury Board of Canada Secretariat	Deck: Cyber Security –
		For information: Provide an aperçu of the challenges in	the Challenge in
	14:10	*protecting Government IT systems, the actions taken to date,*	Protecting Government
3.	*20 min*	*and forward work.*	Systems
		Cyber Security Roles and Responsibilities	
		Lynda Clairmont, Senior Assistant Deputy Minister,	
		National Security, Public Safety Canada	
	14:30	*For information: Provide an overview of the roles and*	Roles and responsibilities
4.	*10 min*	*responsibilities of cyber security lead departments.*	dashboard
		[redacted]	
		Lynda Clairmont, Senior Assistant Deputy Minister,	
		National Security, Public Safety Canada	
		For information: [redacted]	
	14:40		
5.	*5 min*		
		FPT Clerks Meeting, January 23, 2012	
		William Baker, Deputy Minister, Public Safety	
	14:45	*For discussion: Seek views on the strategic objectives for the*	Deck: FPT Clerks
6.	*5 min*	*meeting.*	Meeting
	14:50		
7.	*10 min*	**Roundtable**	N/A

SECRET

CYBER SECURITY ROLES AND RESPONSIBILITIES

PROPOSED TALKING POINTS

- The roles and responsibilities dashboard provides a strategic overview for the areas of focus of key cyber security lead departments and agencies. What it doesn't show are the complexities of managing cyber security on a practical level.

- Roles and responsibilities during an incident affecting Government networks are generally understood, but some clarification is needed owing to the launch of Shared Services Canada. - updating of Government's Information Management Incident Management Plan.

- There is a greater lack of precision around how our departments would cooperate in responding to a cyber incident affecting an external organization, such as a provincial or territorial government, or a critical infrastructure sector.

- A series of tabletop exercises beginning on January 13, 2012, will help to provide the necessary clarity, and identify policy and operational barriers to information sharing. These exercises will contribute to Public Safety Canada's initiative to establish a **national** cyber incident response framework.

- In the case of an incident affecting an external entity, roles, responsibilities and capabilities are even more unclear.

ISSUE

Mr. William (Bill) Baker, Deputy Minister of Public Safety, will introduce this item and will invite you to speak. You will speak to the distribution of cyber security efforts across Government, with a view to informing Deputies on the roles and responsibilities of cyber security lead departments, and to speak to work that is currently underway to clarify and streamline these roles as they would play out under various circumstances.

A roles and responsibilities dashboard was distributed to participants at the beginning of the meeting, and is enclosed for your ease of reference.

BACKGROUND

In November 2010, members of the Directors General Committee on Cyber Security (DG Cyber) provided Public Safety Canada with a slide that described their department's mandate as it relates to cyber security. In November 2011, departments were asked to update or validate their response. This information was categorized so as to be able to be presented visually.

Comments received at the late November and early December 2011 meetings of DG Cyber and the Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber) indicated a need to better describe the roles of departments in terms of cyber security, primarily with regard to the role of defence departments, and with regard to critical infrastructure protection. It was suggested that a dashboard may be more representative and accurate means of doing this.

CONSIDERATIONS

The roles and responsibilities of Government departments and agencies as presented in the *Government of Canada Information Technology Incident Management Plan* (GC IT IMP) are generally defined were accepted for responding to a cyber incident affecting a Government network; however, owing to the launch of Shared Services Canada, this mechanism will need to be revised. In the case of a cyber incident affecting a province or territory, critical infrastructure sector or private sector entity, however, roles, responsibilities and capabilities are more ambiguous, with several varying interpretations.

A series of tabletop exercises beginning January 13, 2012, will help to provide the necessary clarity, and identify policy and operational barriers to information sharing. Additionally, these exercises will contribute to Public Safety Canada's initiative to establish a national cyber incident response framework. This framework would clarify the roles and responsibilities of Government, provincial and territorial partners, and private sector entities.

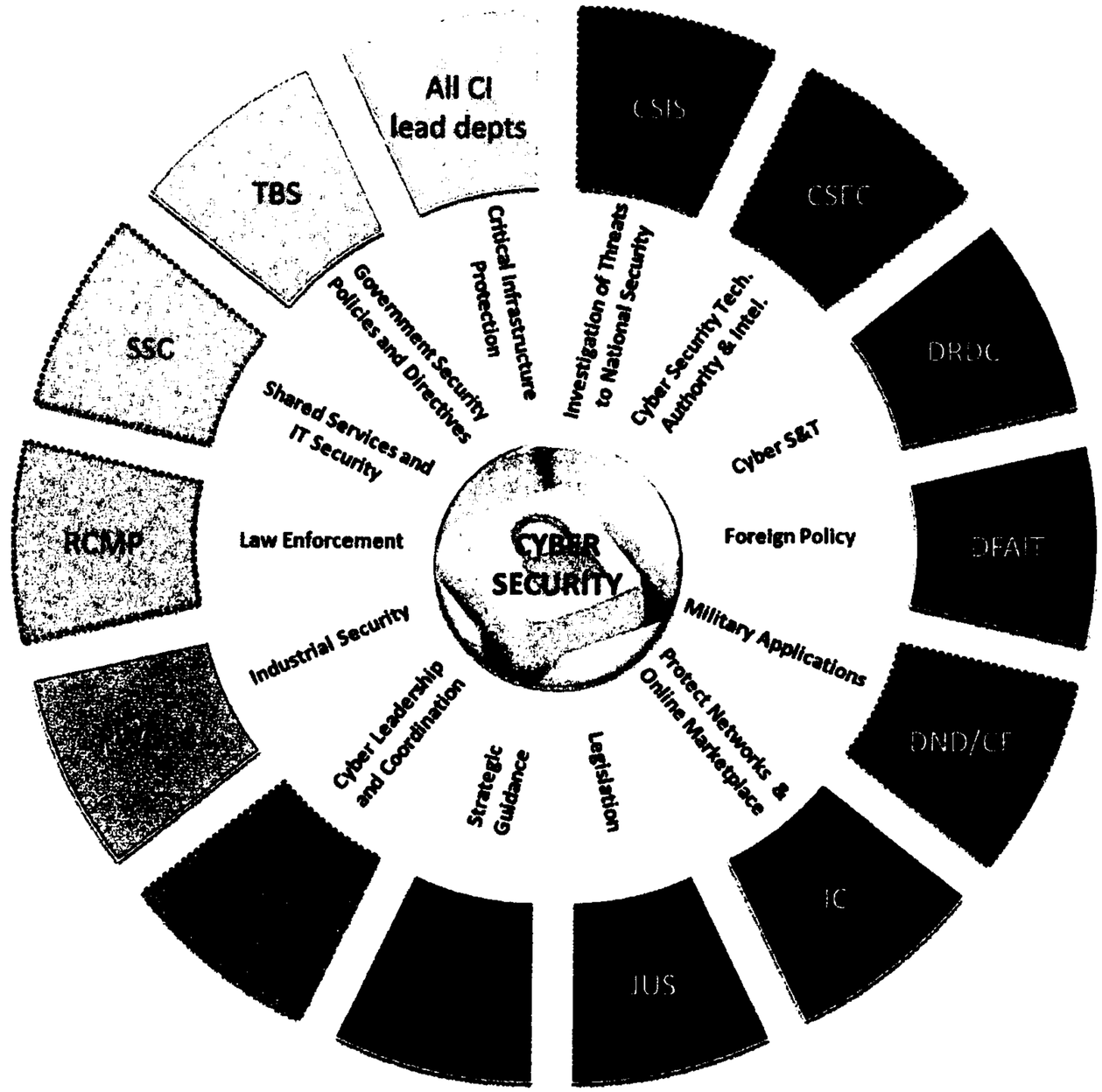
CONCLUSION

It is expected that the current dashboard, along with the exercises, will provide a better understanding of cyber security roles and responsibilities.

There is potential for synergy between Public Safety Canada efforts, and ongoing efforts by the Treasury Board of Canada Secretariat (TBS) to revise the GC IT IMP. We are open to coordinating with TBS so that one set of exercises could help inform our respective efforts.

Prepared by: Melanie Mohammed
Approved by: Corey Dvorkin and Adam Hatfield

Roles and responsibilities with respect to cyber security



Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

#534168

All critical infrastructure lead departments
Includes Finance Canada, Environment Canada, Health Canada, Transport Canada, Natural Resources Canada, Agriculture and Agri-Food Canada, and Public Safety Canada.

Treasury Board of Canada Secretariat
Establishes and oversees a whole-of-government approach to cyber security, including: setting government-wide direction and establishing priorities for securing government IT systems and networks; providing direction and advice to lead security agencies on the approach and implementation of measures for managing IT security incidents; and providing oversight of IT incident management, including post-mortem reviews and lessons learned.

Shared Services Canada
Streamlines and consolidates ICTs in the areas of email, data centres and networks, and for ensuring the confidentiality, integrity and availability of common IT services provided to departments.
Provides common information technology (IT) security services and other solutions to enable departments to exchange information with citizens, businesses and employees.
Gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to common IT services and Government IT critical infrastructure managed by Shared Services Canada, and communicates the information to the Canadian Cyber Incident Response Centre and, as authorized, to departments and cyber security partners.

Royal Canadian Mounted Police
Leads the criminal investigative response to suspected criminal cyber incidents involving critical information infrastructure (i.e., unauthorized use of computer and mischief in relation to data). Leads the investigative response to suspected criminal national security cyber incidents.
Assists domestic and international partners with advice and guidance on cyber crime threats.

Public Works and Government Services Canada
Provider of shared and common services. As part of its Industrial Security Program activity, ensures security in contracts awarded by the Department or when requested by other Government departments.
Ensures the protection of foreign and NATO classified information within the private sector in Canada.
The Industrial Security Sector maintains relationships with allies and negotiates Memoranda of Understanding on industrial security matters, including cyber security, in contracting.

Public Safety Canada
Leads and coordinates the implementation of *Canada's Cyber Security Strategy*, including the design of a whole-of-Government approach to performance measurement and reporting; engagement with provinces and territories, critical infrastructure, and international allies on strategic cyber security policy issues and national cyber incident management; and public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace.
The Canadian Cyber Incident Response Centre acts as Canada's national CERT (Computer Emergency Response Team) in providing assistance and mitigation advice to domestic partners and coordinating the national response to any cyber security incident.

Privy Council Office
Houses and provides support to the National Security Advisor to the Prime Minister.
Coordinates activities among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to national security issues.

Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

Communications Security Establishment Canada
Monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government through its sensor network, and provides mitigation and/or recovery advice and/or guidance to Government departments to help them recover from cyber incidents.
Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the Five Eyes cryptologic community. Undertakes classified research and development for cyber security.

Canadian Security Intelligence Service
Conducts national security investigations, reports to and advising the Government of Canada of activities constituting a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act*.
Provides analysis that will assist the Government of Canada in understanding cyber threats, the actors behind those threats, and overall situational awareness enabling the Government of Canada to better identify cyber vulnerabilities and take action to secure critical infrastructure, prevent cyber espionage or other related cyber threat activity.

Defence Research and Development Canada
Leads the development of military cyber security S&T in support of the Canadian Forces.
Leads domestic Public Safety Canada cyber security S&T efforts not specifically assigned to another department or agency through the Centre for Security Science and with domestic security partners in the Public Security Technical Program. This is delivered in partnership between Government, industry, academia and allies.

Department of Foreign Affairs and International Trade
Supports international bodies in mitigating cyber threats and assisting foreign governments in improving their cyber security profile and capabilities.
Contributes to diplomatic engagement in order to help shape the multilateral regulatory space that is emerging with respect to cyber security. Enables the Government to better position Canada on the international stage to defend and promote its foreign policy and cyber security-related interests.

Department of National Defence / Canadian Forces
Responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process.
Contributes to Government situational awareness during the monitoring and analysis, mitigation, and response phases of the *GC IT IMP* by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

Industry Canada
Responsible for spectrum management in Canada and for fostering a robust and reliable telecommunications system. Develops policies to ensure a safe and secure online marketplace. Helps to ensure the continuity of telecommunications during an emergency.

Department of Justice Canada
Supports initiatives of client departments and agencies through the provision of legal advice on matters relating to cyber policy and law.
In respect of certain matters, especially those relating to criminal law policy and information sharing, Justice plays a leading role. Departmental Legal Services within the Communications Security Establishment Canada had been designated as the centre of excellence on cyber-related legislation.

#534168

Page 409

is withheld pursuant to sections

est retenue en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

ISSUE

Mr. William (Bill) Baker, Deputy Minister of Public Safety, will introduce this item and will invite you to speak. [redacted]

BACKGROUND

[redacted]

SECRET

[redacted]

CURRENT STATUS

[redacted]

Prepared by: Ian Anderson
Approved by: Corey Dvorkin

Pages 412 to / à 413

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Sécurité publique Canada | Public Safety Canada

NON CLASSIFIÉ

Comité des sous-ministres sur la cybersécurité

Le 12 janvier 2012 – 14h00 à 15h00
Salle de conférence au 19e étage du 269, avenue Laurier ouest

ORDRE DU JOUR

	Heure	Item	Documentation connexe
1.	14h00 *5 min*	**Mot de bienvenue** William Baker, sous-ministre, sécurité publique	S/O
2.	14h05 *5 min*	**Comité des sous-ministres sur la cybersécurité** William Baker, sous-ministre, sécurité publique *Pour approbation : S'accorder sur le rôle et la portée du comité; et discuter du programme d'activités à long terme.*	Stipulations proposées
3.	14h10 *20 min*	**L'hygiène des réseaux** Michelle D'Auray, secrétaire du Conseil du Trésor, Secrétariat du Conseil du Trésor du Canada *Pour information : Donner un aperçu du défi quant à la protection des systèmes gouvernementaux, des efforts actuels et des initiatives à venir.*	Présentation : Le défi quant à la protection des systèmes gouvernementaux
4.	14h30 *10 min*	**Rôles et responsabilités en cybersécurité** Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, sécurité publique *Pour information : Donner une vue d'ensemble des rôles et responsabilités des ministères principaux en matière de la cybersécurité.*	Tableau de bord sur les rôles et responsabilités
5.	14h40 *5 min*	[redacted] Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, sécurité publique *Pour information : D[redacted]*	[redacted]
6.	14h45 *5 min*	**Réunion des greffiers FPT, le 23 janvier 2012** William Baker, sous-ministre, sécurité publique *Pour discussion : Recherche des commentaires sur les objectives stratégiques pour la réunion.*	Présentation : Réunion des greffiers FPT
7.	14h50 *10 min*	**Tour de table**	S/O

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:

File No.: 384313
RDIMS No.:523645

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

UPDATE ON THE WAY FORWARD FOR CONTROL SYSTEMS SECURITY

(Information only)

ISSUE

This memo provides an update on the progress Public Safety Canada (PS) has made to address the national issue of control systems security, further to the previous memo to you on this subject (June 2011).

BACKGROUND

Control systems are computer systems that manage physical processes, such as the flow of oil and natural gas through pipelines. They are essential to industry, society, and government, as they enable the operation of the nation's critical infrastructure, such as electricity, petroleum production, water, and transportation. Control systems utilize many of the same technologies as general information technology systems and are vulnerable to the same increasing threats. However, they are operated by control systems engineers and not IT personnel, have unique performance and reliability requirements, and often use software that may be considered unconventional to typical IT personnel.

Canada's Cyber Security Strategy identifies the need to partner with the private sector, using the mechanisms established by the *National Strategy and Action Plan for Critical Infrastructure*, to improve the cyber security of control systems in Canada. In June 2011, the National Cyber Security Directorate (NCSD) and the Critical Infrastructure and Strategic Coordination Directorate (CISCD) jointly developed a way forward.

CURRENT STATUS

Since June, significant progress has been made on proactively engaging the stakeholder community to explore what further actions are needed and ensuring that Government activities are well coordinated:

- On November 22-23, 2011, PS held the first of a series of planned regional control systems security workshops in St. John's, Newfoundland. The workshop

was aimed at assisting Canada's critical infrastructure owners and operators to better secure their most critical control system and information technology assets. Participants were from all levels of government and critical infrastructure and feedback has been exceptionally positive (**TAB 1**).

- The Canadian Cyber Incident Response Centre (CCIRC) is continuing its transition into its new role as the national Computer Emergency Response Team (CERT) and is including control systems security efforts as part of its broader focus. In support of this, CCIRC is currently equipping its technical laboratory with control system test-bed software that will help increase in-house expertise within the control systems security domain.

- Over the last two years, Defence Research and Development Canada's Centre for Security Science has provided $800,000 in funding to four research projects focused on control systems security (**TAB 2**).

- A Control Systems Security Interdepartmental Working Group, co-chaired by NCSD and CICSD and reporting to the DG Cyber Committee, has been established to coordinate Federal Government activities (**TAB 3**).

NEXT STEPS

NCSD and CICSD will continue to implement the way forward for control systems security. The way forward will be reviewed in January 2012, incorporating stakeholder input and new information obtained, and adjustments as needed proposed at that time.

Should you require additional information, please do not hesitate to contact Robert Dick, Director General, National Cyber Security at 613-990-2661 or Suki Wong, Director General, Critical Infrastructure and Strategic Coordination at 613-991-3583.

G.H.Hild

Robert Dick
Director General
National Cyber Security

Suki Wong
Director General
Critical Infrastructure and Strategic Coordination

Enclosures: (3)

Prepared by: Tom Campbell and Dorian Panchyson

Post Workshop Report
2011 Control Systems Security Workshop
St. John's, Newfoundland
November 22-23, 2011

Summary

The National Cyber Security Directorate (NCSD) and the Critical Infrastructure and Strategic Coordination Directorate (CISCD) of Public Safety Canada (PS) hosted a very successful training and community building workshop focused on control systems security. Participant feedback rated the workshop as exceptionally good.

Workshop Overview

The Control Systems Security Workshop was a training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators better secure their most critical control system and information technology assets. Recognized experts along with representatives from the federal Government provided briefs on the latest threats and steps that can be taken to increase the security of control systems.

The goals of the workshop were to:

1. provide a greater awareness of the threats and what resources are available to assist in mitigating them;
2. provide a trusted forum where control systems owners and operators can exchange information and ideas to help improve their security posture; and
3. help develop a trusted relationship between the federal, provincial and territorial governments; and control systems owners and operators.

The workshop was supported by PS regional offices, the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS) and Defence Research and Development Canada (DRDC).

Participants

The workshop was well attended with 60 participants, from federal (Public Safety Canada, RCMP, CSIS, DRDC, DFO, PWGSC, Environment Canada and Nav Canada), provincial (Newfoundland and Labrador, New Brunswick and Nova Scotia) and municipal (St. John's) governments, organizations from the critical infrastructure that own and operate control systems and academia.

Sécurité publique Canada | Public Safety Canada

RCMP·GRC

2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

s.19(1)

Tuesday, November 22, 2011

08:30 – 09:00 **Registration** (identification required)

09:00 – 10:15 **State of Control Systems Cyber Security**
[redacted] Department of Homeland Security

10:15 – 10:30 **Health break**

10:30 – 11:15 **Exercising Security: A look inside the NERC Cyber Risk Preparedness Assessment Program**
Mark Fabro, Lofty Perch

11:15 – 12:00 **Evaluating the Safety and Security of Automation Products & Systems**
John Cusimano, Exida

12:00 – 13:30 **Lunch break**

13:30 – 14:15 **SCADA security in the oil and gas sector**
Mark Fabro, Lofty Perch

14:15 – 15:00 **Control Systems Security Program (CSSP) cyber security products and services for owners and operators of Control Systems**
[redacted] Department of Homeland Security

15:00 – 15:15 **Health break**

15:15 – 16:00 **Canadian Cyber Incident Response Centre (CCIRC)**
Luc Beaudoin, Canadian Cyber Incident Response Centre

16:00 – 16:45 **Intrusion Detection/Prevention in Critical Networks**
Frank Marcus, Wurldtech

16:45 – 17:00 **Closing remarks**

Sécurité publique Canada | Public Safety Canada

RCMP·GRC

s.15(1) - Subv
s.19(1)

2011 Control Systems Security Workshop
St. John's Newfoundland
Agenda

Wednesday, November 23, 2011

08:45 – 09:00 **Registration** (identification required)

09:00 – 09:30 **Canada's Cyber Security Strategy**
Tom Campbell, Public Safety Canada

09:30 – 10:15 **Cybercrime and Critical Infrastructure Protection**
Jacques Boucher, Royal Canadian Mounted Police

10:15 – 10:30 **Health break**

10:30 – 11:15 **Cyber Security Evaluation Tool (CSET)**
[redacted], Department of Homeland Security

11:15 – 12:00 **Smart Grid and Advanced Metering Infrastructure Security Research Activities**
Mark Fabro, Lofty Perch

12:00 – 13:30 **Lunch break**

13:30 – 14:15 **Government of Canada Control Systems Security Research**
Rodney Howes, Defence Research and Development Canada

14:15 – 15:00 **Briefing**
[redacted] Canadian Security Intelligence Service

15:00 – 15:15 **Health break**

15:15 – 16:00 **Control Systems Cyber Security Training Opportunities**
[redacted] Department of Homeland Security

16:00 – 16:45 **Break-out Session**

16:45 – 17:00 **Closing remarks**

Defence Research and Development Canada
Control Systems Research Fact Sheet

The Public Security Technical Program at Defence Research and Development Canada's (DRDC) Centre for Security Science is funding a suite of research projects focused on Supervisory Control and Data Acquisition (SCADA) Systems, with the intention of improving Canadian expertise in control systems security. Two projects have been completed, and another two are in progress.

TITLE: Study in Cyber Security and Threat Evaluation in SCADA Systems

Project Lead: RCMP
Partnership: Lofty Perch Inc., PhireLight, 40 private sector and academic partners
Timeline: March 2010 – November 2011 (completed)
Funding: $200,000

Description: The project leveraged existing relationships with critical infrastructure owners and operators to develop tactical research reports on cyber threats to SCADA systems. The intention was to provide a comprehensive understanding of threats and counter measures that could empower public / private partnerships in mitigating risk to national critical infrastructure.

TITLE: Smart Grid Vulnerability Detection and Analysis

Project Lead: NRCan
Partnership: Lofty Perch Inc.
Timeline: April 2011 – April 2012
Funding: $200,000

Description: The project will conduct a risk management analysis of current Smart Grid systems, in order to assess threats, detect vulnerabilities, and identify countermeasures.

TITLE: SCADA Test Bed Analyzer

Project Lead: Public Safety Canada (CCIRC)
Partnership: Solana Networks, Bell Canada
Timeline: April 2011 to March 2012
Funding: $200,000

Description: The Canadian Cyber Incident Response Centre (CCIRC) is currently equipping its technical laboratory with control system test-bed software that will help increase in-house expertise within the control systems security domain. The project

focuses more on the analysis of the software component of SCADA systems and will be located in-house within the CCIRC technical laboratory.

The project will provide CCIRC's technical laboratory with a basic control systems setup to increase its capabilities and help incident handlers develop expertise within the control systems security domain. Ultimately, the intention is to improve the centre's capacity to service the demands of the private sector and the international Computer Emergency Response Team (CERT) community more broadly.

TITLE: SCADA Test Centre Control Room for the Red and Blue Team

Project Lead: Natural Resources Canada (NRCan)
Partnership: Royal Canadian Mounted Police (RCMP) Red Tiger Security, Inc.
Timeline: April 2011 to March 2012
Funding: $220,000

Description: The project will establish an off-site test lab focused on hardware security that will allow researchers to conduct penetration testing and various simulation exercises. It will focus more on hardware than software, including the testing of equipment and the transferring of knowledge to the community of practitioners.

The centre will seek to replicate the US' Idaho National Laboratory, a multi-dimensional research facility focused on areas of importance to national security, nuclear energy, and the environment.

Terms of Reference (TOR)
Government of Canada's Cyber Security of Control Systems Working Group

1. Context

Control systems manage everything from wastewater systems to power plants and pipelines, and their cyber security is critical to delivering the services and products upon which Canadians depend.

Canada's Cyber Security Strategy identifies the need to partner with the private sector through the mechanisms established under the *National Strategy and Action Plan for Critical Infrastructure* to improve the cyber security of control systems in Canada.

2. Mandate

Reporting to the Director General Working Group on Cyber Security (DG Cyber) this working group has been established by Public Safety Canada's National Cyber Security Directorate and Critical Infrastructure and Strategic Coordination Directorate to help clarify and scope the Government's role relating to control systems cyber security and to coordinate Government action in this area.

3. Membership

Membership will consist of manager level representatives from DG Cyber and lead departments responsible for critical infrastructure (CI) sectors as designated in the *National Strategy and Action Plan for Critical Infrastructure* as follows:

DG Cyber: Public Safety Canada, Canadian Security Intelligence Service, Communications Security Establishment Canada, Department of Foreign Affairs and International Trade, Department of National Defence, Defence Research and Development Canada, Industry Canada, Justice Department, Privy Council Office, Public Works and Government Services Canada, Royal Canadian Mounted Police, and Treasury Board Secretariat.

CI Leads: Public Safety Canada, Natural Resources Canada, Industry Canada, Finance Canada, Public Health Agency of Canada, Agriculture and Agri-Food Canada, Environment Canada, Transport Canada, and the Department of National Defence.

Additions to the above standing membership may be recommended by any member and are subject to the agreement of the working group.

4. Roles and Responsibilities

Meetings of the working group will be jointly chaired by Public Safety Canada's National Cyber Security Directorate, and Critical Infrastructure and Strategic Coordination Directorate.

Working group members are responsible for providing information on their departmental initiatives related to control systems security. They are also responsible for contributing to setting agenda items, and providing advice and recommendations to DG Cyber. Members will work collaboratively to develop a plan to identify and prioritize actions for securing control systems.

The working group will determine its meeting frequency as required, and decisions will be made by consensus.

5. Secretariat

Public Safety Canada will serve as the Secretariat to the working group. An agenda will be developed and circulated to all members prior to each meeting. A concise record of discussion and decisions taken will be provided following each meeting.

Public Safety Canada | Sécurité publique Canada

Exercise: Frozen Pond

Scenario Event Package
13 January 2012

Moderators: Robert Pitcher, Kent Schramm, Jeff Bonvie

FOR EXERCISE EYES ONLY

Canada

Background: January 10, 2012

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

s.16(1)(b)

- [redacted] an online anti-Canadian posting by b1narybrotherhood
- The online article posted was found on the following website: www.b1narybrotherhood.com
  - Registered in Montreal on JWeb services
- [redacted] aware of the organization and has provided the following assessment
  - New organization of Synonymous composed of hackivists who were not satisfied with recent direction of Synonymous activities
  - Focusing on environmental related causes
  - Have demonstrated capability in recent attack against Nevada government after federal initiative to extend the Hoover dam project, that would result in significant changes the environmental landscape

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

[redacted]

FOR EXERCISE EYES ONLY

Background: January 11, 2012

- On January 10th, Synonymous conducted a large scale website DOS against Mexican government assets
  - All federal Mexican website taken offline for a period of 4 hours
  - Synonymous claiming responsibility
  - Various media reporting on incident
  - Mexico releases IP address associated with this event to international CERTs

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

[redacted]

FOR EXERCISE EYES ONLY

Background: January 11, 2012

- Province of Alberta reports receiving suspicious emails
  - CCIRC Cyber duty officer receives report
  - Emails are spoofed to be from a municipal entity that is known to be on leave: *James Jones*
  - Emails contains a PDF file that appears to be suspicious in that it contains embedded encrypted content.
    - File: regulations.pdf

FOR EXERCISE EYES ONLY

Background: January 12, 2012

- CCIRC receives industry reporting from *OilCo* in Alberta
  - *OilCo* reporting receiving suspicious emails from *James Jones*
  - Email contains the same PDF attachment, but with email content targeting *OilCo*
    - File: regulations.pdf
  - Email contains one additional attachment
    - File: policy.doc
    - Initial analysis detects an imbedded virus set to activate on January 16th
    - Virus appears undetectable by modern AV software

s.15(1) - Int'l
s.15(1) - Subv
s.16(1)(b)

[redacted]

FOR EXERCISE EYES ONLY

Discussion Points?

- Matrix on CTU calling (See next 2 slides)
- How is CTU called?
- Regular working hours/After hours
- Alternate phone numbers
- At what point is the DG called?

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

[redacted]

FOR EXERCISE EYES ONLY

January 13: Inject 1

s.15(1) - Int'l
s.15(1) - Subv
s.16(1)(b)

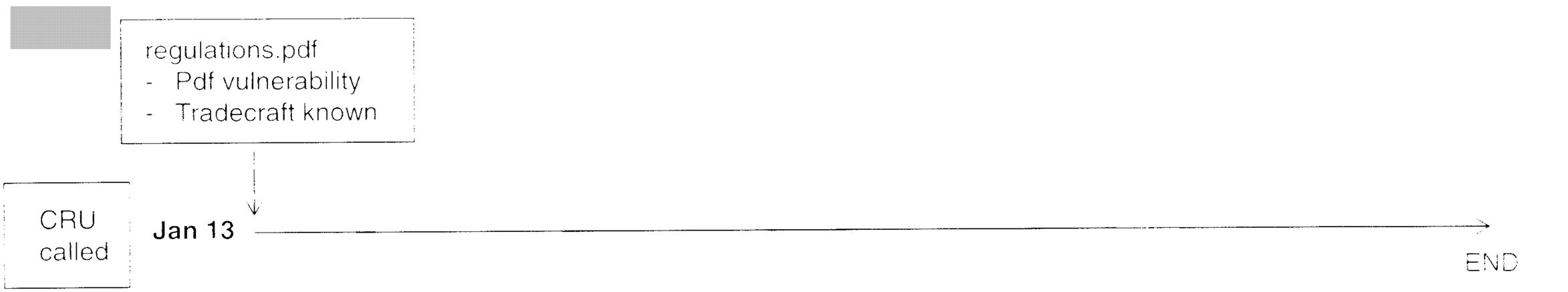
- [redacted] regulations.pdf
  - Embedded malware contains keylogger/rootkit
  - Exposes a zero day vulnerability in Adobe Reader that appears patched in the latest version (Released January 12th)
  - Vulnerable in all previous versions
  - Tradecraft related to a known threat actor

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline

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

s.16(1)(b)



FOR EXERCISE EYES ONLY

Discussion Points?

- Will the tradecraft information be shared at this juncture
- Actions taken by each member department?
- Comments/Questions/Concerns?

January 13: Inject 2

[redacted] policy.doc

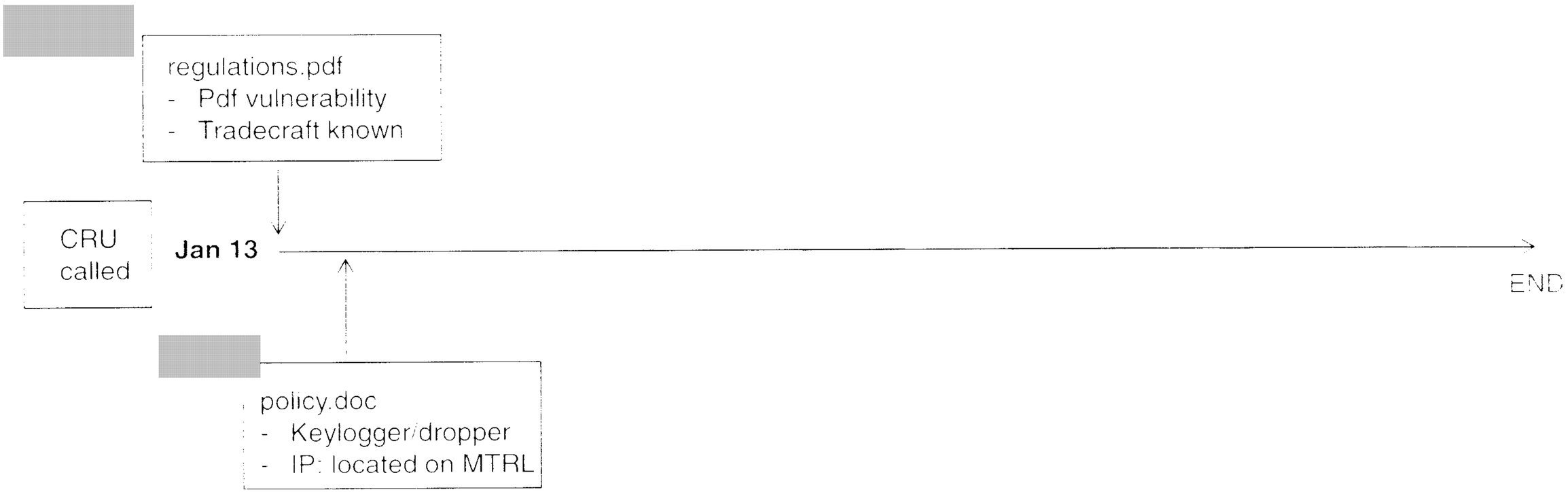
- Embedded keylogger program
- Malware dropper
  - Downloads: rhp.exe
  - connecting to IP 64.11.22.33
  - Registered to Lucius Borderer
  - Provider : JWeb Montreal
- rhp.exe is under investigation and is sent to members

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline

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

s.16(1)(b)



FOR EXERCISE EYES ONLY

Discussion Points?

- What are the potential Law Enforcement options available at this time?
- Information passage decisions: When is information shared within the partner departments?
- Actions taken by each member department?
- Comments/Questions/Concerns?

FOR EXERCISE EYES ONLY

January 13: Inject 3

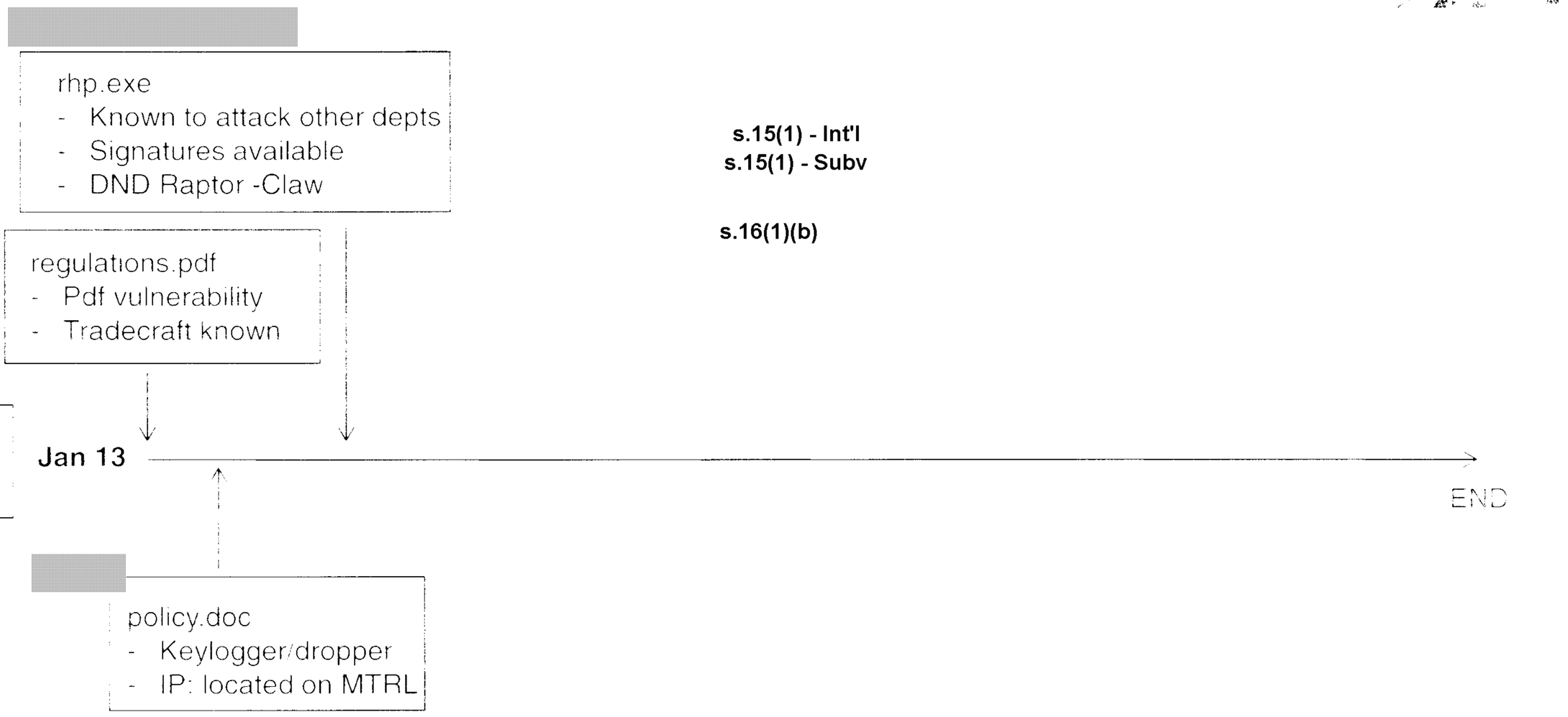
- [redacted] rhp.exe
  - rhp.exe is associated with 4 known attacks [redacted]
  - Attacks originated in September 2011

[redacted]

  - Signatures were developed and distributed to affected departments
- [redacted]: rhp.exe
  - Characteristics associated with ongoing investigation: Raptor-Claw
  - Senior level targeted email campaign

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline



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

s.16(1)(b)

FOR EXERCISE EYES ONLY

Discussion Points?

- Information dissemination: Can the information be shared with partners?
  - Information classification?
  - Impacts of military investigation?
    - What if state sponsored?
- Actions taken by each member department?
- Comments/Questions/Concerns?

January 14: Inject 4

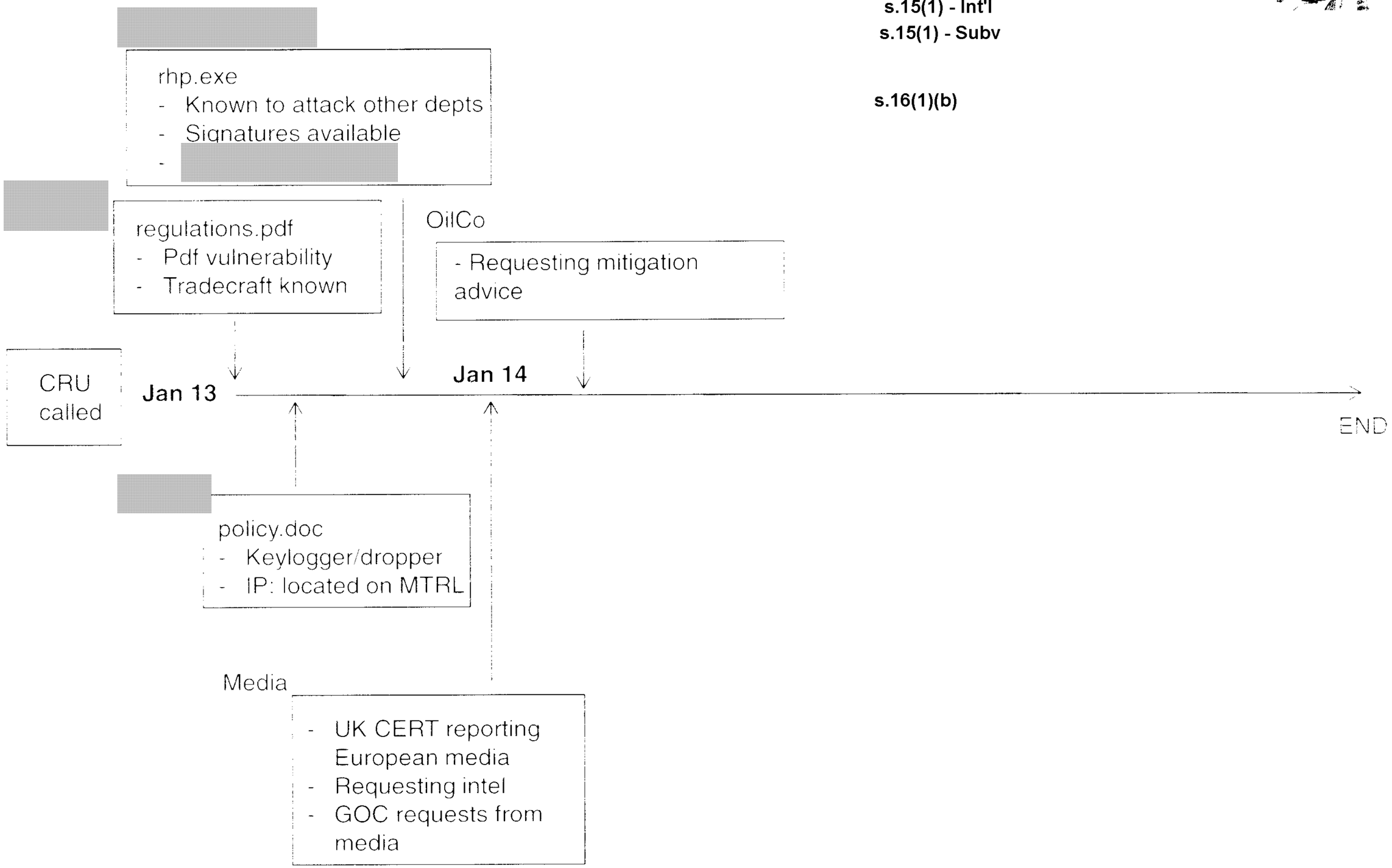
- CPNI (UK) reporting to CCIRC that various European media outlets reporting Synonymous planning to attack economic and financial interests related to Canadian endeavours
  - Various online postings indicating intent
- CPNI considers threat valid, and are actively tracking binary brotherhood as a threat to 2012 Olympics
  - Requesting any intelligence to date on threat
- GOC begins to receive requests for updates on situation from multiple Canadian news outlets
- OilCo requesting mitigation advice from CCIRC

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline

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

s.16(1)(b)



FOR EXERCISE EYES ONLY

Discussion Points?

- Information dissemination: Can the information be shared with international partners?
  - Information classification?
  - Information passage (both directions)?
- Options for domestic assistance?
  - Limitations?
- Actions taken by each member department?
- Comments/Questions/Concerns?

FOR EXERCISE EYES ONLY

January 14: Inject 5

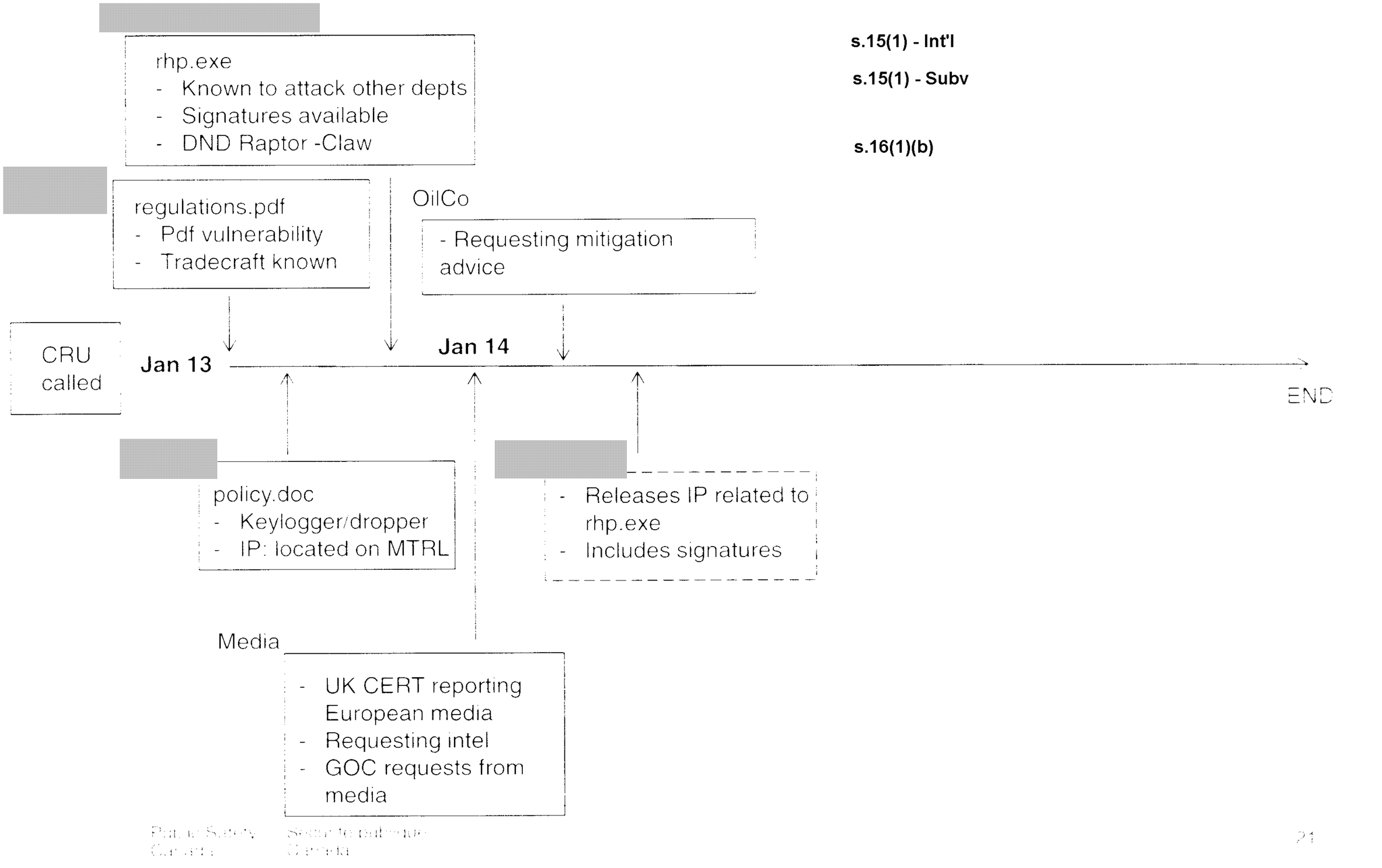
- releases signature files related to observed malicious activity on their networks
- Released signatures include markers associated with malware rhp.exe
-
-

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

s.16(1)(b)

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline



s.15(1) - Int'l

s.15(1) - Subv

s.16(1)(b)

FOR EXERCISE EYES ONLY

Discussion Points?

- Information dissemination: Can the information be shared with partners?
  - Information classification?
  - How does this affect GC classifications?
- Actions taken by each member department?
- Comments/Questions/Concerns?

January 14: Inject 6

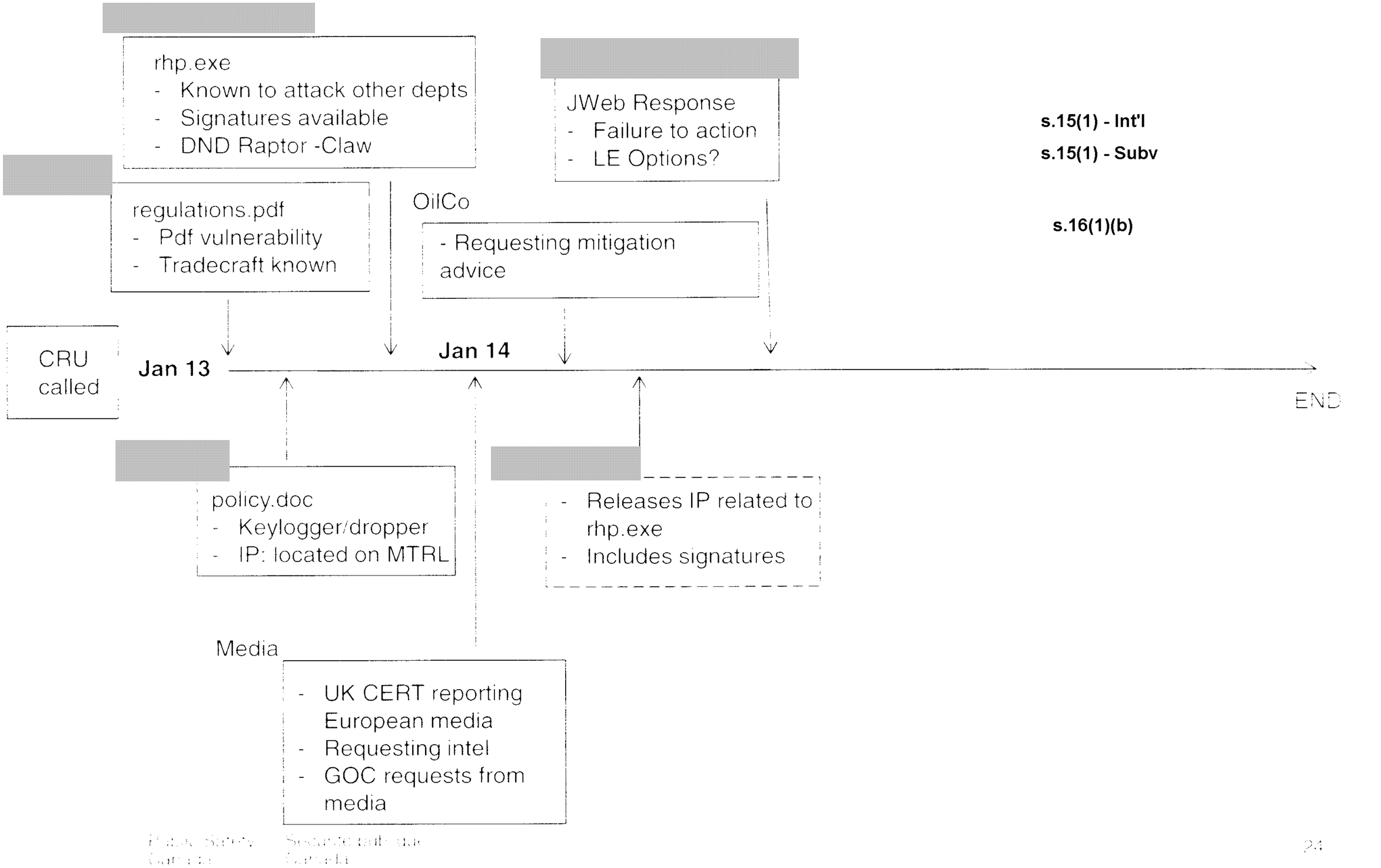
- [redacted]
- JWeb refuses to comply with request, IP continues to serve malicious software
- [redacted]

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

s.16(1)(b)

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline



s.15(1) - Int'l

s.15(1) - Subv

s.16(1)(b)

FOR EXERCISE EYES ONLY

Discussion Points?

s.15(1) - Int'l

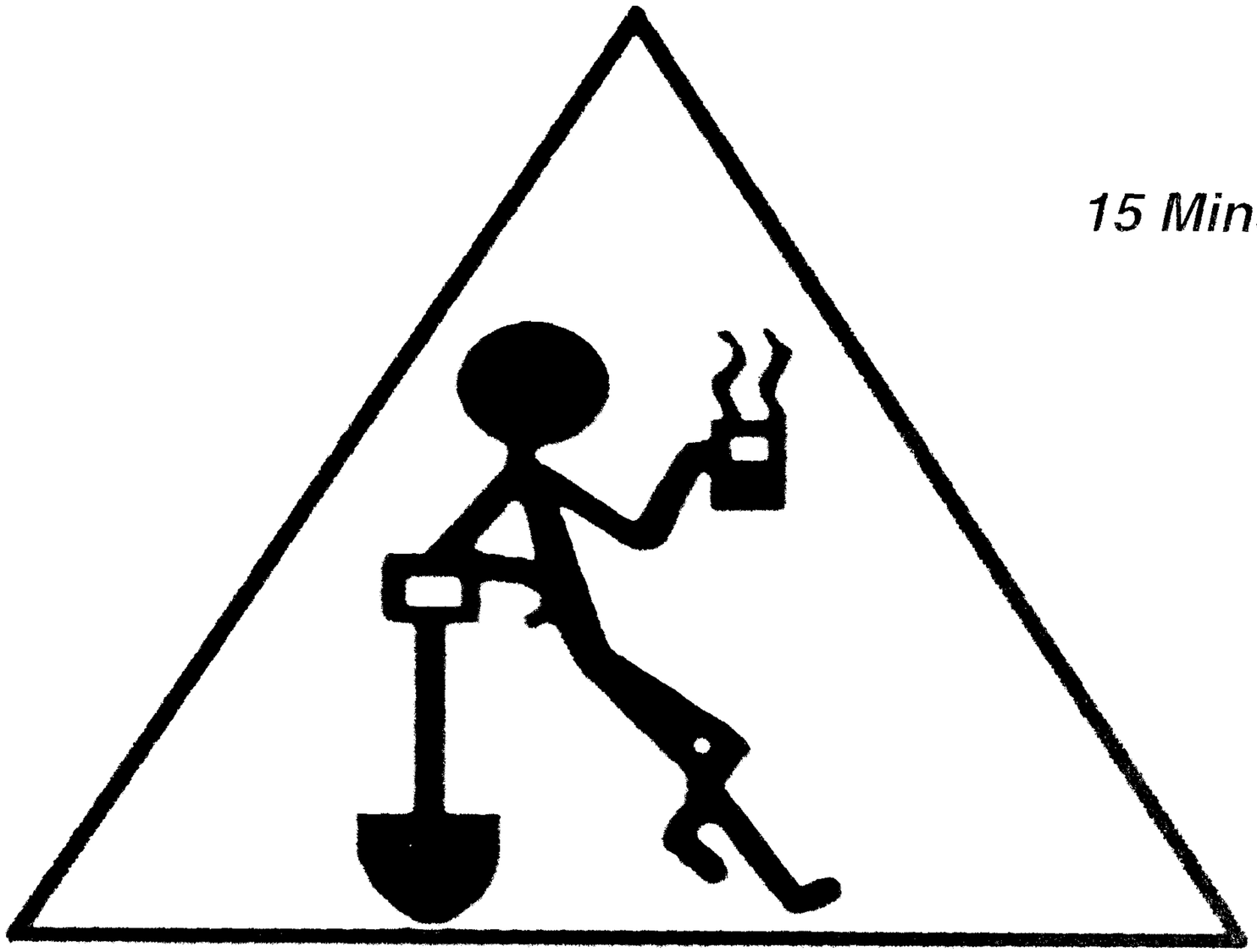
s.15(1) - Subv

s.16(1)(b)

- What options are available [redacted]
  - Timelines
  - Authority chain?
- Actions taken by each member department?
- Comments/Questions/Concerns?

FOR EXERCISE EYES ONLY

BREAK!



15 Mins...

January 15: Inject 7

- SANS.org releases signatures to public domain
  - Related to rhp.exe
    - Designed to download malicious programs
    - Intent unknown

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

s.16(1)(b)

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline

[redacted]

rhp.exe
- Known to attack other depts
- Signatures available
- DND Raptor -Claw

[redacted]

JWeb Response
- Failure to action
- LE Options?

[redacted]

regulations.pdf
- Pdf vulnerability
- Tradecraft known

OilCo
- Requesting mitigation advice

CRU called

Jan 13

Jan 14

Jan 15

END

[redacted]

policy.doc
- Keylogger/dropper
- IP: located on MTRL

[redacted]

- Releases IP related to rhp.exe
- Includes signatures

Media
- UK CERT reporting European media
- Requesting intel
- GOC requests from media

SANS
- Releases IP related to rhp.exe
- Includes Sigs

FOR EXERCISE EYES ONLY

Discussion Points?

- Actions taken by each member department?
- Comments/Questions/Concerns?

FOR EXERCISE EYES ONLY

January 15: Inject 8

- CCIRC Alert 12-505 released: Targeted email in circulation
  - Contains signatures and mitigation advice
- Reporting:
  - 5 energy industries report receiving email related to Alert 12-505
  - 15 agencies/departments within province of Alberta report receiving emails related to Alert 12-505
- JWeb complies [redacted]
  - Files include: rhp.exe
  - Stocktracker.exe
  - List of email address:
    - Province of Alberta
    - Tar sands companies
    - Toronto Stock Exchange

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

s.16(1)(b)

FOR EXERCISE EYES ONLY

s.15(1) - Int'l
s.15(1) - Subv
s.16(1)(b)

Frozen Pond: Event Timeline

[redacted]
rhp.exe
- Known to attack other depts
- Signatures available
- DND Raptor -Claw

[redacted]
JWeb Response
- Failure to action
- LE Options?

Partners
- Alert Released
- 5 CI (Oil and Gas)
- 15 Agencies in Albert Gov

[redacted]
regulations.pdf
- Pdf vulnerability
- Tradecraft known

OilCo
- Requesting mitigation advice

CRU called

Jan 13 — Jan 14 — Jan 15 — END

[redacted]
policy.doc
- Keylogger/dropper
- IP: located on MTRL

[redacted]
- Releases IP related to rhp.exe
- Includes signatures

[redacted] JWeb
- rhp.exe, stocktrader.exe
- Alberta emails
- Tar Sands emails
- TSX emails

Media
- UK CERT reporting European media
- Requesting intel
- GOC requests from media

SANS
- Releases IP related to rhp.exe
- Includes Sigs

Public Safety Canada / Sécurité publique Canada

31

000463

FOR EXERCISE EYES ONLY

Discussion Points?

- Actions taken by each member department?
- Comments/Questions/Concerns?

January 15: Inject 9

- CCIRC forwards alert to TSE contact
  - Including malware stocktracker.exe
- TSE contacts CCIRC requesting more information on Alert 12-505
- Conversation leads to discovery of stocktracker.exe signature confirmation on TSE based systems
- TSE requesting mitigation assistance

s.15(1) - Int'l
s.15(1) - Subv
s.16(1)(b)

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline

[redacted]
rhp.exe
- Known to attack other depts
- Signatures available
- DND Raptor -Claw

[redacted]
regulations.pdf
- Pdf vulnerability
- Tradecraft known

[redacted]
JWeb Response
- Failure to action
- LE Options?

OilCo
- Requesting mitigation advice

CCIRC/TSX
- TSE Sent Alert
- Request for info
- Signature detection

Partners
- Alert Released
- 5 CI (Oil and Gas)
- 15 Agencies in Albert Gov

CRU called

Jan 13 — Jan 14 — Jan 15 — END

[redacted]
policy.doc
- Keylogger/dropper
- IP: located on MTRL

[redacted]
- Releases IP related to rhp.exe
- Includes signatures

[redacted] JWeb
- rhp.exe, stocktrader.exe
- Alberta emails
- Tar Sands emails
- TSX emails

Media
- UK CERT reporting European media
- Requesting intel
- GOC requests from media

SANS
- Releases IP related to rhp.exe
- Includes Sigs

000466

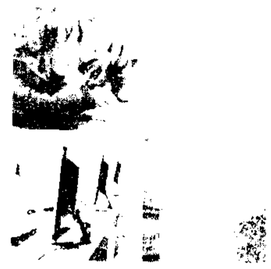
FOR EXERCISE EYES ONLY

Discussion Points?

- What services can the GC provide the TSE?
- Information sharing obstacles?
  - What protocols do we utilize?
- Actions taken by each member department?
- Comments/Questions/Concerns?

January 15: Inject 10

s.16(1)(b)



- [redacted]: stocktracker.exe
  - Malware denies usage of systems infected
  - Transfers itself over drives and network
  - Set to activate on January 16th
  - Malware connects to foreign IP address

s.16(1)(b)

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline

[redacted]

rhp.exe
- Known to attack other depts
- Signatures available
- DND Raptor -Claw

[redacted]

JWeb Response
- Failure to action
- LE Options?

CCIRC/TSX
- TSE Sent Alert
- Request for info
- Signature detection

[redacted]

regulations.pdf
- Pdf vulnerability
- Tradecraft known

OilCo
- Requesting mitigation advice

Partners
- Alert Released
- 5 CI (Oil and Gas)
- 15 Agencies in Albert Gov

CRU called

Jan 13 — Jan 14 — Jan 15 — END

[redacted]

policy.doc
- Keylogger/dropper
- IP: located on MTRL

[redacted]

- Releases IP related to rhp.exe
- Includes signatures

[redacted] JWeb

- rhp.exe, stocktrader.exe
- Alberta emails
- Tar Sands emails
- TSX emails

Media
- UK CERT reporting European media
- Requesting intel
- GOC requests from media

SANS
- Releases IP related to rhp.exe
- Includes Sigs

CCIRC
- stocktracker.exe
- Deny malware
- Network/drive spread
- Contacts Foreign IP

Public Safety Canada — Sécurité publique Canada

37

000469

FOR EXERCISE EYES ONLY

Discussion Points?

- Actions taken by each member department?
- Comments/Questions/Concerns?

s.15(1) - Int'l
s.15(1) - Subv
s.16(1)(b)

FOR EXERCISE EYES ONLY

January 15: Inject 11

- [redacted] IP address associated with stocktracker.exe
  - [redacted]
  - IP address in question associated with state run offensive cyber actions
- [redacted] aware of IP address associated with stocktracker.exe
  - Utilized in previous communication attempts [redacted]

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

s.16(1)(b)

FOR EXERCISE EYES ONLY

Frozen Pond: Event Timeline

[redacted]

rhp.exe
- Known to attack other depts
- Signatures available
- DND Raptor -Claw

[redacted]

JWeb Response
- Failure to action
- LE Options?

CCIRC/TSX
- TSE Sent Alert
- Request for info
- Signature detection

[redacted]

regulations.pdf
- Pdf vulnerability
- Tradecraft known

OilCo
- Requesting mitigation advice

Partners
- Alert Released
- 5 CI (Oil and Gas)
- 15 Agencies in Albert Gov

- [redacted]
- Associated with state

[redacted]

CRU called

Jan 13 — Jan 14 — Jan 15 — END

[redacted]

policy.doc
- Keylogger/dropper
- IP: located on MTRL

[redacted]

- Releases IP related to rhp.exe
- Includes signatures

[redacted] JWeb

- rhp.exe. stocktrader.exe
- Alberta emails
- Tar Sands emails
- TSX emails

Media
- UK CERT reporting European media
- Requesting intel
- GOC requests from media

SANS
- Releases IP related to rhp.exe
- Includes Sigs

CCIRC
- stocktracker.exe
- Deny malware
- Network/drive spread
- Contacts Foreign IP

Public Safety Canada — Sécurité publique Canada

000472

FOR EXERCISE EYES ONLY

Discussion Points?

- Actions taken by each member department?
- Comments/Questions/Concerns?

FOR EXERCISE EYES ONLY

January 15: Inject 12

- Various Energy Sector reporting suspicious connection attempts to IP 123.123.123.123 on approximately 250 computers across Alberta tar sands; Request CCIRC assistance
- Province of Alberta reporting approximately 1100 computers connecting to IP 123.123.123.123; Request CCIRC assistance
- TSE reporting approximately 200 computers connecting to 123.123.123.123; Request CCIRC assistance

s.16(1)(b)

- [redacted] rhp.exe
  - designed to access email on infected devices, infect all attachments in the sent folder, and resend those documents to all recipients
  - Upon email send, malware designed to format drive

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

FOR EXERCISE EYES ONLY s.16(1)(b)

Frozen Pond: Event Timeline

[redacted]

rhp.exe
- Known to attack other depts
- Signatures available
- DND Raptor -Claw

[redacted]

JWeb Response
- Failure to action
- LE Options?

CCIRC/TSX

- TSE Sent Alert
- Request for info
- Signature detection

[redacted]

regulations.pdf
- Pdf vulnerability
- Tradecraft known

OilCo

- Requesting mitigation advice

Partners

- Alert Released
- 5 CI (Oil and Gas)
- 15 Agencies in Albert Gov

- [redacted]
- Associated with state

[redacted]

CRU called

Jan 13 — Jan 14 — Jan 15 — END

[redacted]

policy.doc
- Keylogger/dropper
- IP: located on MTRL

[redacted]

- Releases IP related to rhp.exe
- Includes signatures

[redacted] JWeb

- rhp.exe. stocktrader.exe
- Alberta emails
- Tar Sands emails
- TSX emails

Computers infected:
- 250: tar sands
- 1100: gov AB cmps
- 200: TSE

Media

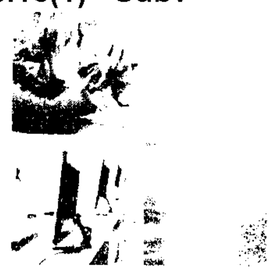
- UK CERT reporting European media
- Requesting intel
- GOC requests from media

SANS

- Releases IP related to rhp.exe
- Includes Sigs

CCIRC

- stocktracker.exe
- Deny malware
- Network/drive spread
- Contacts Foreign IP



FOR EXERCISE EYES ONLY

Frozen Pond: Malware Summary

REPORTING

Alberta:
- regulations.pdf

JWeb:
- rhp.exe
- stocktracker.doc
- Email lists : Alberta. Tar Sands. TSE

TSE:
- stocktracker.exe

- Alberta
1100 computers
- Energy Sector:
250 computers
- TSE
-200 computers
- 123.123.123.123

OilCo:
- regulations.pdf
- policy.doc

- Alberta:
15 departments
- OilCo
- 5 energy sectors
- policy.pdf

MALWARE

policy.doc
- Downloader
- rhp.exe

stocktracker.exe
- DOS
- Jan 16th
- IP 123.123.123.123

s.15(1) - Int'l

State sponsored
-
-
- Raptor-Claw

s.15(1) - Subv

regulations.pdf
- Keyloger/Rootkit
- Adobe Zero Day

rhp.doc
- Malware mailer
- IP 123.123.123.123
- Drive formatter

FOR EXERCISE EYES ONLY

Discussion Points?

- Actions taken by each member department?
- Comments/Questions/Concerns?
- What now…?

EndEX!

Public Safety Canada | Sécurité publique Canada

Exercise: Frozen Pond

Scenario Timelines

13 January 2012

Moderators: Robert Pitcher, Kent Schramm, Jeff Bonvie

FOR EXERCISE EYES ONLY

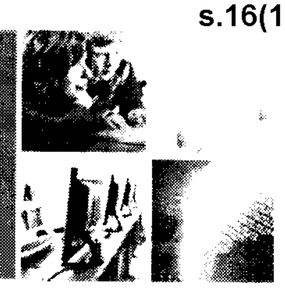
Canada

s.15(1) - Int'l

s.16(1)(b)

POR EXERCISE EYES ONLY

Frozen Pond: Event Timeline



SAFE RESILIENT CANADA

rhp.exe
- Known to attack other depts
- Signatures available
- DND Raptor -Claw

JWeb Response
- Failure to action
- LE Options?

CCIRC/TSX
- TSE Sent Alert
- Request for info
- Signature detection

regulations.pdf
- Pdf vulnerability
- Tradecraft known

OilCo
- Requesting mitigation advice

Partners
- Alert Released
- 5 CI (Oil and Gas)
- 15 Agencies in Albert Gov

-
- Associated with state
-
-

CRU called

Jan 13 — Jan 14 — Jan 15 — END

policy.doc
- Keylogger/dropper
- IP: located on MTRL

- Releases IP related to rhp.exe
- Includes signatures

JWeb
- rhp.exe, stocktrader.exe
- Alberta emails
- Tar Sands emails
- TSX emails

Computers Infected:
- 250: tar sands
- 1100: gov AB cmps
- 200: TSE

s.15(1) - Int'l

s.15(1) - Subv

s.16(1)(b)

Media
- UK CERT reporting European media
- Requesting intel
- GOC requests from media

SANS
- Releases IP related to rhp.exe
- Includes Sigs

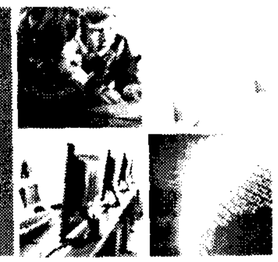
CCIRC
- stocktracker.exe
- Deny malware
- Network/drive spread
- Contacts Foreign IP

Public Safety Canada / Sécurité publique Canada

000480

FOR EXERCISE EYES ONLY

Frozen Pond: Malware Timeline



SAFE RESILIENT CANADA

REPORTING

Alberta:
- regulations.pdf

OilCo:
- regulations.pdf
- policy.doc

JWeb:
- rhp.exe
- stocktracker.doc
- Email lists : Alberta, Tar Sands, TSE

Alberta:
15 departments
OilCo:
5 energy sectors
- policy.pdf

TSE:
- stocktracker.exe

Alberta:
- 1100 computers
OilCo:
- 250 computers
TSE:
- 200 computers
123.123.123.123

MALWARE

policy.doc
- Downloader
- rhp.exe

stocktracker.exe
- DOS
- Jan 16th
- IP 123.123.123.123

State sponsored
[redacted]

regulations.pdf
- Keyloger/Rootkit
- Adobe Zero Day

rhp.doc
- Malware mailer
- IP 123.123.123.123
- Drive formatter

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

Meeting on January 16, 2012, with Mr. James Lambert, Canada's Ambassador to the Netherlands

ISSUE

- You will be meeting with Mr. James Lambert, Canada's Ambassador to the Netherlands (**TAB C**), to discuss cyber security in advance of your meeting with officials from the Office of the National Coordinator for Counterterrorism and Security.

STRATEGIC OBJECTIVES

- Obtain a debrief from Canadian officials on the opening of the National Cyber Security Centre (NCSC) and the related Conference as you will be discussing the Centre with Dutch officials.

- Seek an assessment from the Ambassador on the Dutch experience in implementing their *National Cyber Security Strategy*. It may be helpful to get his opinion of the relative political priority given to cyber security and how cyber is viewed by the private sector.

- Leave Canadian officials with a greater understanding of ongoing efforts to implement *Canada's Cyber Security Strategy* (**TAB D – Backgrounder**).

STRATEGIC CONSIDERATIONS

Public Safety Canada has a history of partnership with Dutch officials on a number of national security files, including cyber security. As the Netherlands continues to implement its national cyber security program, the Department is seeking to understand and learn from the experiences of the Dutch Government.

On January 12, 2012, an official from the Canadian Embassy will be attending the opening of the National Cyber Security Centre when the Dutch national Computer Emergency Readiness Team (GOVCERT.nl) will become the National Cyber Security Centre (NCSC). The NCSC is a public private partnership to address cyber security incidents and will collocate cyber incident handlers side by side with representatives from the private sector, law enforcement agencies, and the intelligence community. As part of the opening of the Centre, a conference is also being hosted by the Dutch Government, and features Ms. Neelie Kroes, the European Commissioner for the Digital Agenda, and Ms. Melissa Hathway, the former Director of the Joint Interagency Cyber Task Force.

Lessons learned from the Dutch experience could inform Public Safety Canada's efforts to strengthen the role of the Canadian Cyber Incident Response Centre (CCIRC) in dealing with Canada's critical infrastructure sectors. You should note that the officials from the Netherlands have notified CCIRC of these recent changes to ensure the continuity of cyber incident management service.

s.19(1)

Ambassador Lambert [redacted] with Erik Akerboom, the Netherlands' National Coordinator for Counterterrorism and Security. You will be meeting with Mr. Akerboom the next day. Mr. Akerboom also co chairs the Netherlands Cyber Security Council created in June 2011, which is a public private body with senior representation from government, industry and Dutch universities. His co chair is Mr Eelco Blok the Chief Executive Officer of the Netherlands based telecommunications company KPN.

It would be informative to seek Ambassador Lambert's views on the challenges and accomplishments of the Dutch in implementing their national strategy. <u>These views will be especially important given the recent major compromise of a Dutch company, DigiNotar, responsible for issuing security certificates for websites including those for individuals seeking to use government services securely online. This incident received sustained attention from the Dutch Cabinet.</u>

Furthermore, the National Security Operations Directorate has indicated (**TAB B**) that they would like to seek recommendations in order to set up meetings with officials in the Netherlands to discuss lawful interception. It would be useful to seek advice from the Ambassador as to which Dutch officials would be best placed to discuss lawful interception.

As a courtesy to the Ambassador, you may want to outline the objectives for your meetings in the Netherlands, which are:

- Obtain a greater understanding of the mechanisms through which the National Cyber Security Centre interacts with and supports critical infrastructure and the private sector on cyber security issues.

- Obtain a greater understanding of the experience of the Dutch Government in establishing their Cyber Security Council, comprised of government officials, private sector officials and academics. As the Government of Canada does not have a similar body, this could provide insight as to whether such an option should be explored.

- Leave counterparts with a greater understanding of the accomplishments achieved thus far in the implementation of *Canada's Cyber Security Strategy*.

- Signal Canada's desire for targeted collaboration with the Netherlands on cyber security issues, recognizing both nations have very limited resources for new programs.

s.13(1)(a)

s.15(1)

Canada will continue to promote norms in cyberspace and the Netherlands is seen, [redacted] as an important partner in this effort given their stance on Internet and cyber security policy issues.

TALKING POINTS ARE ON THE NEXT PAGE

Meeting on January 16, 2012, with Mr. James Lambert, Canada's Ambassador to the Netherlands

TALKING POINTS

Possible questions to ask Ambassador Lambert

- Public Safety Canada has recently narrowed the focus of the Canadian Cyber Incident Response Centre, which acts as our national CERT (Computer Emergency Readiness Team).

- We would like to learn how the National Cyber Security Centre interacts with and supports critical infrastructure and the private sector on cyber security issues.

- I'm interested in getting a sense of how the Dutch share information within the National Cyber Security Centre.

- Have you noticed any issues associated with cyber security information sharing between the public and private sectors?

- Given the amount of work we are undertaking with the private sector in Canada, in any of your meetings with the private sector here, have you gotten a sense of how well CEOs or other officials understand the cyber security environment.

- How has the creation of the Cyber Security Council or the DigiNotar incident had a significant impact on the visibility of cyber security issues in the Netherlands?

Objective for National Security Operations Directorate

Our Investigative Technologies and Telecommunications Program would like to set up working level meetings with Dutch counterparts on lawful interception, do you have recommendations as to which officials in the Netherlands deal with these particular issues?

Objectives for the meeting with Mr. Akerboom

- As you know, I will be meeting with Mr. Erik Akerboom, Dutch Coordinator for Counterterrorism and Security. My objectives for the meeting are to:

  - Obtain a greater understanding of the mechanisms through which the National Cyber Security Centre interacts with and supports critical infrastructure entities and the private sector on cyber security issues.

  - Obtain a greater understanding of the experience of the Dutch Government in establishing their Cyber Security Council, comprised of government officials, private sector officials and academics. As the Government of Canada does not have a similar body, this could provide insight as to whether such an option should be explored.

  - Leave counterparts with a greater understanding of the accomplishments achieved thus far in the implementation of *Canada's Cyber Security Strategy*.

  - Signal Canada's desire for targeted collaboration with the Netherlands on cyber security issues, recognizing both nations have very limited resources for new programs.

James Lambert – Ambassador of Canada to the Netherlands

James Lambert, (BA Honours, Queen's University, 1979; Graduate Studies, Norman Paterson School of International Affairs, Carleton University, (1980 - 1982) joined the Department of External Affairs in 1982 and served abroad in Lagos, San José, Tokyo, Mexico City and as Ambassador to the Republic of Guatemala with cross accreditation as Ambassador to El Salvador and High Commissioner to Belize.

At the Department of Foreign Affairs and International Trade Canada (Ottawa), he held positions in the International Economic Relations Division, the Asia Pacific Regional Coordination Division and the Caribbean and Central America Division. He served as Director General for Public Diplomacy before becoming in 2006 Director General of the Latin America and Caribbean Bureau.

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

Meeting on January 17, 2012, with Colonel Hans Folmer, Commander of the Cyber Task Force, Ministry of Defence, The Hague

ISSUE

- Colonel Hans Folmer, Commander of the Cyber Task Force of the Ministry of Defence (**TAB B**), will be briefing you on the implementation of the cyber programme in the Royal Netherlands Army and the establishment of a Defence Cyber Command and an Expertise Centre.

- This briefing session will serve as a forum to exchange experiences in the implementation of our respective cyber security strategies. As such, you may wish to provide a greater understanding of ongoing efforts to implement *Canada's Cyber Security Strategy* (**TAB C – Backgrounder**).

STRATEGIC OBJECTIVES

- Learn about the Dutch Ministry of Defence's cyber defence efforts.

- Leave officials with a greater understanding of ongoing efforts to implement *Canada's Cyber Security Strategy*.

STRATEGIC CONSIDERATIONS

In September 2011, the Dutch government announced that an estimated €2 million (approximately CAD$2.6 million) would be allocated to the Dutch armed forces in 2012 for cyber operations, with a total of €50 million (approximately CAD$65.1 million) being allocated between 2012-15. Funding is intended to reinforce the Ministry of Defence's current cyber defences and to develop the army's capability to partake in cyber operations.

It is expected that the development of Dutch cyber operations capability will focus on the improvement of the army's ability to defend its own networks, systems and information, and on the expansion of its cyber intelligence capabilities. Efforts will also focus on the National Cyber Security Centre that was stood up on January 12, 2012.

TALKING POINTS ARE ON THE NEXT PAGE

Meeting on January 17, 2012, with Colonel Hans Folmer, Commander of the Cyber Task Force, Ministry of Defence, The Hague

TALKING POINTS

Possible questions to ask Colonel Folmer

- What work have you undertaken in the implementation of the Dutch national cyber security strategy?

- How has the recent breach of security certificates at DigiNotar affected your work?

- As you may know, emergency management, national incident response, critical infrastructure protection and public awareness all fall under the purview Public Safety Canada. Furthermore, *Canada's Cyber Security Strategy* focuses overwhelmingly on public security, rather than on military issues.

- Canada's CERT (Computer Emergency Readiness Team) is the Canadian Cyber Incident Response Centre. This is also housed within Public Safety Canada. They provide assistance to our domestic partners outside of our federal government and coordinate the national response to any cyber incident.

- How do you coordinate activity with the new Dutch Cyber Security Council and the National Cyber Security Centre?

Colonel Hans Folmer

Colonel Hans Folmer is the Commander of the Cyber Task Force of the Ministry of Defence. He has been charged with the task of implementing the cyber programme in the Royal Netherlands Army and establishing a Defence Cyber Command and an Expertise Centre. Before this he was Chief Joint (C4ISR) Requirements Branch at the Ministry of Defence. Until 2010, he was Chief Operations of the EU Military Staff in Brussels and before that he led the Dutch-German Liaison Battalion in Eibergen.

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

Meeting on January 17, 2012 with Officials from the Cyber Security Council

ISSUE

- On Tuesday, January 17, 2012, you will be meeting with representatives from the Cyber Security Council of the Netherlands. The lunch will be hosted by Gerben Klein Baltink, the Secretary of the Cyber Security Council (biography not provided).

STRATEGIC OBJECTIVES

- Obtain a greater understanding of the role and responsibilities of the Dutch Cyber Security Council in advising the Government of the Netherlands and the private sector on cyber security issues. As the Government of Canada does not have a similar body, this could provide insight as to whether such an option should be explored in the Canadian context.

- Leave counterparts with a greater understanding of the accomplishments achieved in implementing *Canada's Cyber Security Strategy* (**TAB B - Backgrounder**).

BACKGROUND

As a fundamental part of Dutch efforts to reform the governance of cyber security, the Netherlands' *National Cyber Security Strategy* called for the creation of a Cyber Security Council. That Strategy highlights that "mutual trust is essential for cooperation and sharing information with each other. Government and business communities must work together as equal partners." On June 30, 2011, the Dutch Government officially installed the Cyber Security Council to advise the Dutch Government as well as the private sector on developments in digital security. The Cyber Security Council is also unique in that it provides solicited and unsolicited advice to the Government on digital security matters. The 14 member Council will set priorities, assess needs for further research and development, and examine how to share information with public and private sector entities. Membership of the Council is diverse and includes officials from government, the private sector and academia.

STRATEGIC CONSIDERATIONS

Canada does not have a similar advisory body on cyber security. It would be helpful to know whether such a Council is useful and effective in addressing key challenges such as:

- public private sector collaboration;
- encouraging businesses to take action to secure their networks; and,
- directing research efforts in the public and private sectors.

TALKING POINTS ARE ON THE NEXT PAGE

Meeting on January 17, 2012 with Officials from the Cyber Security Council

TALKING POINTS

- Canada is in the process of building relationships with critical infrastructure and other levels of government on cyber security. We are currently focused on working with the telecommunications, energy and financial sectors.

- One of our key challenges is building trust with the private sector. Businesses are often reluctant to discuss vulnerabilities related to cyber security, and we need to ensure that there are ways to share threat information quickly to ensure that systems are protected.

- Does the Cyber Security Council facilitate information sharing between the private sector, academia and government? If so, how?

- How is advice provided to government? Are there public reports or other mechanisms? Could you provide an example of how advice has been provided and the outcome?

- How will the Council determine relevant areas of research? What levers – for example, funding – does the Council have to encourage research in particular areas?

- Has the Council undertaken work to increase awareness on cyber security among CEOs? If so, how?

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

Meeting on January 17, 2012, with Mr. Erik Akerboom, National Coordinator for Counterterrorism and Security and Mr. Wil van Gemert, Director, National Cyber Security Centre

ISSUE

- On January 17, 2012, you will be meeting with Erik Akerboom, the National Coordinator for Counterterrorism and Security (**TAB B**), and Mr. Wil van Gemert, the Director of the National Cyber Security Centre (**TAB C**), from the Netherlands to discuss cyber security. The Netherlands has begun implementing the changes set forth in their *National Cyber Security Strategy*

STRATEGIC OBJECTIVES

- Obtain a greater understanding of the mechanisms through which the National Cyber Security Centre (NCSC) interacts with and supports critical infrastructure entities and the private sector on cyber security issues. As Public Safety Canada has recently repositioned the focus of the Canadian Cyber Incident Response Centre, it may be informative to compare this with the Dutch experience in expanding the scope of their national Government Computer Emergency Readiness Team (GOVCERT.nl) to establish the NCSC.

- Obtain a greater understanding of the role and responsibilities of the Dutch Cyber Security Council in advising the Government of the Netherlands on cyber security issues. As the Government of Canada does not have a similar body, this could provide insight as to whether such an option should be explored in the Canadian context.

- Leave counterparts with a greater understanding of the accomplishments achieved in implementing *Canada's Cyber Security Strategy* (**TAB D - Backgrounder**).

- Signal Canada's desire for targeted collaboration with the Netherlands on cyber security issues, recognizing both nations have very limited resources for new programs.

BACKGROUND

On February 22, 2011, the former Minister of Justice and Security, Ivo Opstelten presented Holland's *National Cyber Security Strategy: Success through cooperation* (**TAB E**). That Strategy discusses the policy problem, principles and goals for cyberspace as perceived by the Netherlands. It further outlines the actions and activities the Dutch Government intends to undertake to deliver on those objectives.

The Dutch Strategy is guided by the following principles:

- defining clear responsibilities between departments while strengthening existing government initiatives on cyber security;
- renewing the focus on international cooperation, public private partnerships and individual responsibility; and,
- leveraging the collective efforts of industry and citizens to help the government secure cyberspace.

There are many notable similarities between the Dutch and Canadian approaches to cyber security, including:

- improving the governance of cyber security issues;
- improving threat and risk assessment;
- increasing vital infrastructure resilience;
- improving response capacity for cyber disruptions and attacks;
- intensifying law enforcement response to cybercrime; and,
- increasing domestic research and education on cyber security.

The *Strategy* makes clear that the Dutch will encourage self-regulation among industry and would only consider legislation and regulations should that option fail. There is also strong sentiment that measures to protect and national security must be proportionate with the safeguarding of fundamental rights. Overall, their Strategy focuses on improved incident management and increased law enforcement actions as the means to improve cyber security in the Netherlands.

STRATEGIC CONSIDERATIONS

Three months following the release of their national strategy, the Netherlands suffered a serious cyber attack. In June 2011, DigiNotar, a digital certificate authority, suffered a compromise that led to its eventual bankruptcy in September 2011. The attack targeted the secure credentials of hundreds of websites, including the Dutch Government, Google and Skype. As the incident had compromised website certificates issued for secure user communications with the Dutch Government, which would enable criminals to act as a legitimate Government website unbeknownst to users. This incident was actively managed by the Dutch Cabinet over four days. Following the incident, DigiNotar was criticized for not having taken basic security measures in its business practices. The company also faced scrutiny for putting the security and privacy of its clients at risk by not immediately reporting the attack to customers or the Dutch authorities.

Also in June 2011, the Dutch Government established a Cyber Security Council to advise the Dutch Government as well as the private sector on cyber security developments. The 14 member Council will set priorities, assess needs for further research and development, and examine how to share information with public and private sector entities. Membership of the Council is varied and includes officials from government, the private sector and academia. As Canada does not have a similar advisory body on cyber security, it would be useful to obtain an assessment on the effectiveness of the Cyber Security Council.

Starting on January 12, 2012, the current Government Cyber Emergency Readiness Team (GOVCERT.nl) will become the NCSC. This effort will bring together liaisons from law enforcement and intelligence agencies, representatives from private sector businesses and critical infrastructure entities to enable and broaden relationships between the national CERT and stakeholders. The establishment of the NCSC is expected to improve the resiliency of Dutch networks through information sharing, threat and incident response and crisis coordination.

As the Canadian Cyber Incident Response Centre (CCIRC) positions itself as Canada's cyber security coordination centre, it would be useful to understand the challenges the Dutch dealt with in integrating industry into the NCSC. Public Safety Canada will need to explore and address considerations surrounding information sharing, non-disclosure and industry competition as it works to augment CCIRC. Dutch authorities have already notified CCIRC of the relevant changes to incident management contact procedures in the Netherlands to ensure fluid response in case of an incident as the NCSC comes online. CCIRC interacts with international CERT bodies, including the Netherlands, on an incident to incident basis, like the DigiNotar incident.

At the London International Cyber Conference, Mr. Akerboom discussed the Dutch response to the DigiNotar incident. In describing the lessons learned, he focused on the importance of international cooperation, information sharing and the need to actively manage the response to incidents. He further offered his opinion that serious incidents such as the one experienced by the Netherlands will be inevitable worldwide and will require appropriate plans and response to manage and mitigate the effects of such incidents.

Other related initiatives intended to support their Strategy include a review of the Netherlands' *Telecommunications Act*, building capacity within the Ministry of Defence and establishing mechanisms with the private sector to prevent digital espionage. These three initiatives are currently beyond the scope of Canada's own Strategy. As nothing has been released publicly about these initiatives, it would be useful to understand what steps the Dutch are taking in this regard as well as what, if any, legislative measures they may be considering.

TALKING POINTS ARE ON THE FOLLOWING PAGE

Meeting on January 17, 2012, with Mr. Erik Akerboom, National Coordinator for Counterterrorism and Security

TALKING POINTS

Canadian Progress Made to Date

- We are working diligently to establish and build strong relationships with critical infrastructure, and other levels of government in Canada. We are focused on working with the telecommunications, energy and financial sectors at this time.

- Recently, Public Safety Canada transitioned the responsibility for the Government of Canada CERT to the Communications Security Establishment Canada and streamlined the role of the Canadian Cyber Incident Response Centre to focus on critical infrastructure and cyber systems outside the Government of Canada.

- Having the Canadian Cyber Incident Response Centre function with both of these roles was not yielding the results we needed. Canada will continue to adjust roles and responsibilities as we move forward with implementing our Strategy.

- One of the key challenges we see is addressing the trust issues associated with the private sector. Quite often businesses are reluctant to discuss vulnerabilities associated with cyber security, and we need to ensure that there are ways to share threat information quickly to ensure that systems are protected.

Dutch Progress Made to Date

- We would be interested in hearing your impressions of the DigiNotar incident and the impact that it had on the reforms underway. This really seemed to test your Strategy right as you were in the process of implementation, is there anything that you would have changed?

- Have the efforts of your Government or the DigiNotar incident led to a greater understanding of the importance of cyber security among critical infrastructure and private sector stakeholders?

- In what ways do you expect that information sharing challenges will be addressed through the creation of the National Cyber Security Centre?

- Are there particular efforts underway to enhance the ability of the private sector to protect themselves that have not been publicly disclosed given their sensitivity?

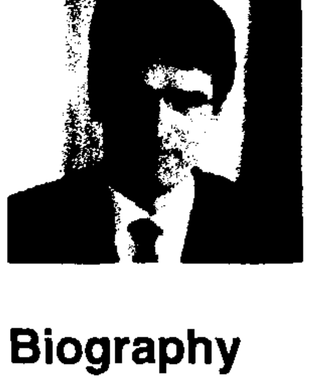
- Canada was happy to receive notification of the change in contacts from your officials in advance of the shift in responsibilities.

Identify Ways to Cooperate with the Netherlands

Responsive Only

- We could consider an exchange of best practices on information sharing between private and public sector entities as well as discussing ways to encourage the promotion of norms in cyberspace begun at the London International Cyber Conference.

Erik Akerboom – National Coordinator for Counterterrorism and Security – Ministry of Security and Justice, the Netherlands



Biography

Erik Akerboom (1961) began his career at the Police College in Apeldoorn, and went on to study political science at the VU University in Amsterdam. Until 1998 he held a number of posts within the police service: head of a community police team, district commander and head of the regional criminal investigation support service. He was then appointed director of the Democracy and Rule of Law Department of the General Intelligence and Security Service (AIVD). On 1 April 2009 he replaced Tjibbe Joustra as National Coordinator for Counterterrorism, who occupied the post from 1 April 2004 to January 2009.

Erik Akerboom also sits on a number of advisory committees in the field of security and education, and he is dean of the Strategic Leadership course at the Dutch Police College. Together with Eelco Blok (KPN) he is also co-president of the Cybersecurity Council.

Wil van Gemert

Mr. Wil van Gemert commenced in mid-January at Office of the National Coordinator for Counterterrorism and Security (NCTb). His prior position was that of Chief Information Officer at the Netherlands General Intelligence Service (AIVD), and before that Director of Homeland Security (AIVD). Furthermore Mr. van Gemert held several management positions within the police force.

Elly van den Heuvel

Acting head of the National Cyber Security Centre / managing director GOVCERT.NL

Biography

Elly van den Heuvel is an experienced manager, who has had a long career within Dutch government. Van den Heuvel has held various positions at the Ministry of Security and Justice. As Head of IT of the Ministry of Security and Justice, she was responsible for the development of long-term policy within the field of IT.

In 2008, she was appointed General Manager of GOVCERT.NL, the Cyber Security & Incident Response Team for the Dutch Government. At GOVCERT.NL she focuses on strengthening existing (inter)national joint ventures with the members of the Cert-community, partners, stakeholders and other interested parties. She attaches considerable value to the further professionalisation of cyber security.
GOVCERT.NL will form the basis for the National Cyber Security Centre to be opened on 1 January 2012. This centre will be formed as a public-private partnership. Drawing up an accurate threat assessment in cooperation with other organisations so that interested parties can respond proactively has her special attention.

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

The National Cyber Security Strategy (NCSS)

Success through cooperation

1. Introduction

The Netherlands stands for safe and reliable ICT[1] and the protection of the openness and freedom of the Internet. The increasing dependence on ICT makes society increasingly vulnerable to abuse and (large-scale) disruption. This is why the cabinet presents the National Cyber Security Strategy which has been prepared with contributions from a broad range of public and private parties, knowledge institutes and social organisations. With this Strategy the cabinet meets the Knops and Hernandez[2] motions and shapes the integral approach to cyber crime announced in the coalition agreement.

Structure of the paper
This strategy comprises two parts. The first part, Chapters 2 through 4, sets out an analysis of the problem, the basic principles of the policy area of cyber security and the goal to be achieved. The second part, Chapter 5, sets out a number of action lines and per line priority activities which this cabinet wishes to carry out itself and with other parties to improve cyber security.

2. Developments which require action

ICT is of fundamental importance for our society and economy
Safe and reliable ICT is of fundamental importance for our prosperity and well-being and forms a catalyst for (further) sustainable economic growth. In Europe 50% of the growth in productivity is due to the application of ICT[3]. The Netherlands aspires to be among the world leaders in the use and application of ICT in society and at the same time guarantee the safety of the digital society. The ambition is to grow into the *Digital Gateway to Europe*.

Society is vulnerable
ICT offers opportunities, but also increases the vulnerability of a society in which ever more vital products and services are intertwined. A deliberate or unintentional disruption as a result of technical or human failure or due to natural causes can lead to social disruption. The complexity of ICT facilities and our increasing dependence on them lead to new vulnerabilities and can facilitate disruption. Examples of this are the rapid developments of mobile data traffic and cloud-computing which entail new vulnerabilities and new possibilities of abuse. The increase in the use of Internet services whereby personal data must be used and the increase in the popularity of social media also result in new vulnerabilities and abuse, for example, in the form of identity theft.

Recent examples
Recent incidents illustrate this notion of vulnerability and abuse. For example, in the second half of 2010 advanced malware - Stuxnet – was discovered which is specifically geared to industrial process automation. Analysis showed that the development of this malware must have cost a great deal. There is suspicion that this attack was financed by a state, directed at the vital infrastructure in another state, with worldwide side effects in other (vital) organisations.
In an internationally coordinated action, at the end of 2010 the Netherlands National Police Force was involved in a joint venture with partners at home and abroad to tackle a large botnet, a collection of computers of often unsuspecting owners which can be abused remotely for, e.g., criminal activities. The botnet, called Bredolab, was controlled from Armenia, with a focal point in the Netherlands and had branches in various other countries. Worldwide, millions of computers were part of this botnet, which was used, inter alia, to send spam and carry out DDoS attacks.
The measures that a number of companies took against WikiLeaks was a reason for WikiLeaks supporters to carry out worldwide DDoS attacks against, inter alia, Paypal, Mastercard, the Public

---

[1] ICT is the entirety of digital information, information infrastructures, computers, systems, applications and the interaction between information technology and the physical world regarding which there is communication and information exchange.
[2] Knops motion; Second Chamber of Parliament, parliamentary year 2009-2010, 32 123 X, no. 66; Hernandez Motion ; Second Chamber of Parliament, parliamentary year 2010-2011, 32 500 X, no. 76.
[3] Euro commissioner Kroes during the opening of the WCIT conference 2010 in Amsterdam.

Prosecution Office and the police. This resulted in the websites of these organisations being temporarily unavailable and the simplicity of hacktivism became clear.

> ***Cyber security*** *is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information.*

Cooperation between existing parties in the digital society is necessary, including at an international level
In the actual event of a cyber attack it is often difficult to determine what the cause or source is. It can be an individual, an organisation, a state or a combination of these players. Often it is not immediately clear what type of cyber threat[4] is involved. In a cyber attack use is often made of the same techniques and methods[5]. All of this makes extensive cooperation between parties involved with cyber security of great importance, from government organisations which focus on separate types of threats, companies which maintain the network and information infrastructure, to knowledge institutes in the area of cyber security and citizens.

Digital society is global. Cyber attacks and disruptions cross over national borders, cultural and legal systems in the blink of an eye. It is often unclear which jurisdiction applies and it is uncertain whether applicable laws can be effectively enforced. The cabinet wants to improve the effectiveness of action against abuse in the digital world, wherever it comes from.

3. Basic principles

Investing in cyber security means to invest in our future, our economic growth and our innovation. Not only because it makes safe ICT and safe use of ICT possible in the Netherlands, but also because the Netherlands is an important player in the knowledge and development of the domain of cyber security. This requires a high priority for cyber security (civil-military, public-private, national-international, throughout the entire safety chain) which has to result in a resilient ICT infrastructure, in resilient vital sectors, fast and effective response and an adequate legal protection in the digital domain. The following basic principles apply.

Linking and reinforcing initiatives
There are many on going initiatives in the area of cyber security. However, there is a lack of coherence with regard to a number of issues. The findings in the national Trend Report on Cyber Crime and Digital Safety 2010 and the Report on ICT Vulnerability and National Security of the National Security Thinktank supports this view. That is why double activities are removed and initiatives are combined. Where possible existing initiatives form the basis for further expansion and if necessary the cabinet will develop new initiatives.

Public-Private Partnership
ICT infrastructure, products and services are for the greater part supplied by private sectors. Continuity and certainty of supply are not only important for the business world in connection with their continuity. Society itself has an interest in this, e.g. to prevent social unrest due to disruptions. Mutual trust is essential for cooperation and sharing information with each other. Government and business communities must work together as equal partners. The relevant parties must derive added value from participation in joint initiatives. A good cooperation model with clear tasks, responsibilities, powers and safeguards supports this.

Individual responsibility
All users (citizens, companies, institutions and public authorities) take suitable measures to secure their own ICT systems and networks and to prevent security risks for others. They are careful when

---

[4] Cyber crime, cyber terrorism, cyber activism, cyber espionage or cyber conflict
[5] Like malware, botnets, spam, phishing and targeted attacks

storing and sharing sensitive information and respect the information and the systems of other users.

Division of responsibility between departments
In line with the basic principles of the National Security Strategy, the Minister of Security and Justice is in charge of the coherence and cooperation within the field of cyber security and is accountable in this respect. Besides this, each party retains its own tasks and responsibilities.

Active international cooperation
The cross-border nature of threats makes it essential to focus on strong international cooperation. The basic principle is an international 'level playing field'. Many measures will only be effective if they are aligned or implemented at an international level. The Netherlands supports and actively contributes to the efforts of, e.g., the EU (Digital Agenda for Europe and the Internal Security Strategy), NATO (development of cyber defence policy in the framework of the new strategic concept), the Internet Governance Forum and other joint ventures. The Netherlands is a proponent of a broad ratification and implementation of the Cyber Crime Convention of the Council of Europe.

The measures to be taken must be proportionate
There is no such thing as one hundred percent security. The Netherlands makes choices in tackling cyber security activities on the basis of the weighing up of risks. A number of core values in our society play an important part. Privacy, respect for others and fundamental rights such as the freedom of expression and information gathering must be maintained. An appropriate balance must remain between, on the one hand, our desire for public and national security and, on the other, the safeguarding of our fundamental rights. Measures must be proportional. Toward this end safeguards and review mechanisms, including the existing supervision functions, are utilised and where necessary reinforced.

Self-regulation if possible, legislation and regulations if necessary
Government and businesses achieve the desired digital security first through self-regulation. If self-regulation does not work, the options of legislation and regulation are reviewed. The basic principles are that regulations may not result in an unnecessary distortion of competition and must ensure a level playing field as much as possible, that the administrative burdens are not disproportionately increased and the costs are reasonably proportional to the benefits. Developments are rapid. This can result in legislation quickly becoming obsolete. The cabinet will determine whether legislation should be adjusted to the developments in the digital domain.

4. Goal of the strategy

Security and confidence in an open and free digital society
The goal of this strategy is to reinforce the security of the digital society, in order to increase confidence in the use of ICT by citizens, the business community and government. Toward this end, the Dutch government wants to work together more effectively with other parties on the security and the reliability of an open and free digital society.

This will stimulate the economy and increase prosperity and well-being. Good legal protection in the digital domain is guaranteed and social disruption is prevented or adequate action will be taken if things were to go wrong.

5. Work plan "Work in progress"

The following action lines have been chosen to achieve the goal of this National Cyber Security Strategy:
- The Netherlands will see to an integral approach by public and private parties.
- The Netherlands will see to adequate and topical threat and risk analyses.
- The Netherlands will reinforce the resilience against ICT disruptions and cyber attacks.

- The Netherlands will reinforce the response capacity to deflect ICT disruptions and cyber attacks.
- The Netherlands will intensify investigation and prosecution of cyber crime.
- The Netherlands will stimulate research and education.

Concrete actions for the action lines are set out below.

Work in progress
A lot of activity is already going on with regard to the subject of cyber security as a whole. A number of priority new activities or activities to be enhanced are elaborated below. The degree in which these activities are elaborated differs. For a number of activities the process is still at an early stage, so that at present no broadly supported picture can be presented of the activity to be realised. We are therefore clearly dealing with work in progress. After publication of this action plan, the elaboration of these points will be continued with the relevant parties.

5.1. Setting up the Cyber Security Board and National Cyber Security Centre

The concern for digital security lies with many different parties in the Netherlands. At present there is still insufficient coherence between the entirety of good policy initiatives, information provision and operational cooperation. The cabinet therefore finds it important that there is a joint approach with the business community and knowledge and research institutions. The goal is the reinforcing of the network and taking care of the coordination from strategic to operational level.

- The cabinet believes a new network-oriented joint venture form is necessary to achieve the integral and coherent approach to cyber security. The input of the cabinet is the establishing of a Cyber Security Board on which representatives of all relevant parties have a seat at strategic level and in which agreements are made on the implementation and elaboration of this strategy. In the coming months, in consultation with all relevant parties, it will be decided how to set up the Board. The government will facilitate the Board.

- It is a wish of the cabinet that public and private parties, on the basis of their own tasks and within the statutory options, information, knowledge and expertise, be brought together in a National Cyber Security Centre so that insight can be gained into developments, threats and trends and support can be offered for incident handling and crisis decision making. The cabinet invites public and private parties to join this Centre. A joint venture model will be developed to enable this.

- The cabinet will expand and reinforce the current GOVCERT.NL[6] and place it within this Centre.

The cabinet's goal is for the Board to be operational on 1 July of this year and the Centre on 1 January 2012.

5.2. Preparing threat and risk analyses

The reinforcing of security starts with insight into vulnerabilities and threats. By bringing knowledge and information of (inter)national public and private organisations[7] together and analysing them, better insight is gained into topical and possible new vulnerabilities and threats. Alignment is sought with the working method of the national security strategy: i.e. charting risks and identifying capacities which have to be reinforced in order to prevent threats and to be able to respond to disruptions. With this knowledge, all target groups can take measures in the entire chain, from prevention to response and investigation and prosecution.

---

[6] GOVCERT.NL focuses on reinforcing information security within the Dutch government and does so by monitoring sources via internet, giving advice on ICT vulnerabilities and issuing alerts in the event of threats and by offering support to government organisations when handling ICT-related incidents.

[7] Inter alia GOVCERT.NL, AIVD and MIVD[7], police, Extraordinary Investigation Services (e.g. FIOD, SIOD), supervisory agencies (e.g. OPTA and Consumer Authority), National Inspectorates (e.g. the Public Health Inspectorate), private parties (e.g. ISPs and security vendors), national and international knowledge and research institutions.

- One of the tasks of the National Cyber Security Centre is the creation of one joint and integral picture of the topical threats of ICT, inter alia in the form of the Trend Report Cyber Crime and Digital Security which was first published in 2010.

- AIVD and MIVD[8] (Netherlands information and security services) provide knowledge for the forming of this picture. Where necessary they will reinforce their cyber capacity.

- Annually the cabinet will be informed via the National Risk Assessment[9] of the threats to national security. Cyber security will be paid extra attention.

5.3. Increasing the resilience of vital infrastructure

Social unrest due to ICT disruptions or cyber attacks must be prevented. Various parties have a responsibility in this respect, from citizen to supplier. The user must be able to rely on an ICT product or service being safe to use. The supplier must therefore offer a sufficiently safe ICT product or service. The user must also take the necessary security measures him-/herself.

- The Telecommunications Act will be updated in 2011. A number of existing agreements with the biggest telecoms companies on the continuity of their vital telecommunications infrastructure will be converted into regulations. This concerns the reporting of disruptions of fall-out of services, minimum requirements in the area of continuity of services, and the alignment with international standards. Where possible there will be alignment with a European joint approach to these topics.

- In the coming years the Cyber Crime Information Exchange will be continued under the flag of CPNI.nl[10]. This year it will be reviewed how the cooperation between CPNI.nl and the National Cyber Security Centre will be given shape.

- Together with the vital organisations, the government will stimulate the use of the usual minimum ICT security standards on the basis of good practices. The cabinet works with vital sectors to gain insight into possible measures to combat the disruption of their vital ICT facilities. On the basis hereof the government is urging vital sectors to take the identified measures. An example of this is the Emergency Communication Facility (NCV) which will replace the current Emergency Network as of 1 May 2011. Vital organisations will have the opportunity to connect to the Emergency Communication Facility.

- Specifically to prevent (digital) espionage the cabinet has developed a package of measures. For companies an Espionage Vulnerability Analysis Manual is available with which they can increase their resilience to espionage.

- The government believes the increasing of individual resilience to be of great significance. That is why the cabinet is working to bring about that 80% of the vital organisations in the vital sectors of Public Administration and Public Order and Security will have a continuity plan by the end of 2011, which plan will set out the scenario of a large-scale disruption of ICT and electricity.

- In the middle of 2011 the cabinet will establish one security framework for information security for national government services and will present new Information Security Categorised

---

[8] The AIVD and MIVD have a unique information position with regard to cyber threats (such as digital espionage, cyber terrorism and cyber extremism) due to the research which is conducted in the interests of national security.

[9] The National Risk Assessment elaborates various types of threats to national security with a uniform method in scenarios for the mid-long term and gives them scores as to probability and impact. Proposals are then made for reinforcing capacities to reduce the (consequences of the) threats.

[10] The Cyber Crime Information Exchange provides a platform where vital sectors and government parties exchange information in a trusted environment on incidents, threats, vulnerabilities and good practices in the area of cyber crime and cyber security. The goal is to increase the resilience of these parties to disruptions.

Information Regulation[11]. A nationwide monitoring cycle for information security will also be established.

- In the course of 2011 the cabinet will decide whether travel documents will include an electronic Identity card which satisfies the highest reliability level for citizens. Citizens can then reliably identify themselves via the Internet and place a qualified electronic signature whereby privacy is guaranteed.

- The government is implementing the European disclosure obligation for data leaks with regard to the Telecom Sector. In addition, on the basis of the Coalition Agreement a proposal for a disclosure obligation will be elaborated in the event of loss, theft or abuse of personal details for all services of the information society.

- In 2011 the cabinet will make choices on security in relation to the processing of personal details. The European developments in the area of privacy will provide direction in this respect. The cabinet will inform the Second Chamber of Parliament in the near future regarding the position on privacy. The disclosure obligation will be included therein.

- In consultation with the ICT suppliers, the cabinet wants to look for options for improving the security of hard- and software and is also intended to make agreements on secure hard- and software at international level. In addition, the Netherlands is actively participating in the Internet Governance Forum which is facilitated by the United Nations. The goal of this is to play an active role, in the global context of an open and transparent dialogue, of touching upon topics which can contribute to this strategy, such as improving the game rules on the Internet and combating abuse.

- The cabinet wants to consult with suppliers to make information on the security of ICT products and services better available for the user[12]. The government, together with the suppliers of ICT products and services, will continue developing target-oriented national campaigns for citizens, companies and the government which are geared to current developments and vulnerabilities[13].

5.4. Response capacity for withstanding ICT disruptions and cyber attacks

In order to be able to adequately respond to various threats and to be able to return to a stable situation in the event of a disruption of attack, various response activities are necessary. The relevant organisation will in the first instance itself deal with ICT incidents which lead to a breach of the availability, integrity or exclusivity of the network and information infrastructure. The government will respond adequately where incidents can lead to social disruption or harming of vital objects, processes or persons.

- In the summer of 2011 the cabinet will publish the National ICT Crisis Plan. This plan will include a exercise plan, which aligns both national and international exercises.

- The ICT Response Board (IRB), a public-private joint venture which gives the crisis decision making organisations advice on measures to combat or counteract large-scale ICT disruptions, will come into operation in 2011 and will be placed as a function in the National Cyber Security Centre.

---

[11] The National Bureau for Connection Security (NBV) of the AIVD promotes the security of special information by making approved and self-developed security products available, by offering assistance during the implementation thereof, by making a contribution to policy and regulations in this area and by giving advice on information security.

[12] Good examples are the "knock 3 times" campaign of the banks, which was directed to citizens, the initiative "Protect your business" of the industry association ICT~Office to encourage SMEs to carry out a risk analysis and good information security, the campaign "Cybersafe yourself" for colleges and universities and "Webwijs" of Bits of Freedom.

[13] Examples of this are the campaigns "Safe on the Internet", "Digi-abled and Digi-aware" (by ECP-EPN). The "Waarschuwingsdienst.nl" for current threats by GOVCERT.NL also serves this goal.

- Internationally focus will be on reinforcing the cooperation in the operational response between the CERT organisations in Europe and besides that the goal is to reinforce the International Watch and Warning Network (IWWN) which currently functions as informal globally operating consultation in the event of ICT incidents.

- The social impact of a large-scale terrorist attack on or via the Internet can be substantial. The Terrorism Combating Alerting System (ATb) will therefore be expanded with a cyber component and drills will be carried out.

- The Ministry of Defence is developing knowledge and capacities to be able to operate effectively in the digital domain. The maximum goal is to achieve options for the exchange of knowledge and expertise with civil and international partners. In addition, studies will be carried out on how the Ministry of Defence can make knowledge and capacities available for its third (primary) task within the ICMS (intensification of civil-military cooperation) agreements.

- A cyber education and training centre (OTC) will be founded.

- In order to further enhance the resilience of the own networks and systems, the tasks of the Defence Computer Emergency Response Team (DefCERT) will be further expanded in the coming years. In addition, investments will be made in increasing the security awareness among the personnel and there will be accreditation of systems and processes.

- A doctrine for cyber operations is being developed for the response to an attack to protect individual resources and units.

5.5. Intensifying investigation and prosecution of cyber crime

The rapid development of cyber crime requires effective combating in order to maintain confidence in the digital society. Toward this end the enforcement bodies in the criminal law chain (primarily the police and other investigation services, but also the Public Prosecution Office and the judiciary) which are charged with combating cyber crime must have a sufficient number of specialists. This concerns the very specialist handling of complex cases ("high tech crime") and the handling of less complex (high volume) cases which affect the confidence that citizens, the SME sector and the rest of the business community have in ICT. The goal is for the willingness to report an offence and the chance of catching the perpetrators to increase and that perpetrators are dealt with more severely. International cooperation also enables cross-border crime to be tackled better.

- The cabinet intends to realise the establishing of an expert pool and to set up a register of experts for government, universities and the business community, so that scarcely available expertise can be shared and specialists are offered a challenging career perspective.

- With regard to law enforcement the cabinet is focusing on more cross-border investigations with investigation departments of countries within Europe and with other international partners. In addition, the cabinet will be focusing on further international legislation and regulations for cyber crime.

- At the national level a steering group will be established to tackle priority crime. For cyber crime the goal is that in the entire criminal law chain there are sufficient specialists to adequately tackle cyber crime cases. The chairman of this steering group will have a seat on the Cyber Security Board. The Public Order & Safety Inspectorate will review the functioning of the police in the investigation of cyber crime.

- Within the current budgetary framework of the police, the coming years there will be a shift to greater investigation capacity and within that context also in the direction of investigation and prosecution of cyber crime. These are Internet monitors and specialists within the regions and with the High Tech Crime Team of the National Police Force. The intention is for the High Tech Crime Team to be dealing with some 20 cases in 2014. The investigation and prosecution services will participate in the National Cyber Security Centre.

- The cyber crime programme approach will play a central role in the coming years in, inter alia: the setting up of a knowledge centre within the police, the reinforcement of the police organisation and the effective shift within the existing capacities. The Public Prosecution Office and the judiciary will have a sufficient number of specialised public prosecutors, secretaries of the public prosecution office, judges and cyber law magistrates.

5.6. Stimulating research and education

Scientific and applied research and the stimulation of the development of innovative security solutions are a driving force for cyber security. A good education at all levels is necessary to continue producing reliable ICT and to be able to continue withstanding threats. A professional vocational group is a prerequisite for the growth of the digital economy in the Netherlands.

- The cabinet will better align research programmes of the government and where possible of scientific research centres and the business community in the National Cyber Security Board. In addition the government will supervise the aforementioned parties even more actively than now when tapping into multiplying research funds of, e.g., European and Euregion funds.

- Reinforcement of education at all levels is necessary to be able to continue withstanding threats and to continue producing reliable ICT and is a prerequisite for the growth of the digital economy in the Netherlands. Together with the vocational groups and the education sector a plan will be developed for the expansion of the share of ICT security in the appropriate courses. Continued effort will be put into a study of the possibilities of certification and qualification of information security professionals. This requires that the content of the courses be clear. A good example of this is the initiative of the vocational group of information security officers to make the characteristics of the various courses clear.

6. Financial consequences

The above activities will be dealt with within the existing budgets.

> Return address P.O. Box 20301 2500 EH The Hague The Netherlands

To: the President of the Lower House of the States General

Date 23 December 2011
Subject Cyber Security

National Coordinator for Counterterrorism and Security

Oranjebuitensingel 25
2511 VE The Hague
P.O. Box 16950
2500 BZ The Hague
www.nctv.nl

Our reference
NCTV/5718756/11

Annexes
4

Digital information exchange has become essential to the functioning of Dutch society, both to commerce and in the operations of the authorities. We are immediately affected by breaches of Internet security and its cross-border nature requires a comprehensive and international approach. The events surrounding DigiNotar, the recent incidents as represented in media coverage in the context of 'Lektober'(Leaktober: Each day in October, the IT news site 'Webwereld' revealed an IT privacy leak in a website or government service), and the discovery of the Duqu virus have endorsed the 'sense of urgency' of this government in an expeditious implementation of the National Cyber Security Strategy (NCSS). By means of the NCSS, the government - together with the major parties from the business and academic sectors - has developed a basic plan for a comprehensive approach to cyber security, thus implementing the public-private, civil-military, and international cooperation in an innovative manner. Good progress has been made, but the plan still requires further elaboration.

During the General Consultations on National Security of 1 June 2011, I promised the Lower House a cyber security threat assessment and a cyber security legal framework, including an overview of the legal bottlenecks. The Lower House also requested more information about legislation on cybercrime in Austria, and in particular on jurisdiction. In the plenary debate on DigiNotar of 13 October 2011, the Lower House requested more detailed information about the National Cyber Security Centre (NCSC) that will be operational from 1 January 2012. By virtue of the Hennis-Plasschaert c.s.[1] motion, the Lower House furthermore requested in this debate to introduce a statutory duty of notification, a so-called 'security breach notification'.

The purpose of this letter is to inform the Lower House about the points mentioned above, also on behalf of the Minister of Economic Affairs, Agriculture and Innovation, the Minister of the Interior and Kingdom Relations, the Minister of Defence, and the Minister of Foreign Affairs. These points have been dealt with in the context of the NCSS in the past few months.

You will be informed about the following:

- The Cyber Security Assessment Netherlands (CSBN); this letter includes the analysis of the CSBN, the response from the Cyber Security Council (CSR), and the response from the government. You will find the complete CSBN and the complete response from the CSR enclosed with this letter.
- The Cyber Security Legal Framework: this letter will deal with the legal framework relevant to cyber security in more detail. You will find an extensive description of the cyber security legal framework in the enclosed document Cyber Security Legal Framework.

---

1 See Parliamentary Papers 2010/11, 26 643, no. 202.

- Structure of the National Cyber Security Centre (NCSC); this letter includes an outline description of the structure of the NCSC. In the enclosure with this letter, you will find the detailed version of the proposal on the structure of the NCSC.

Requests for advice regarding the implications of developments in the cyber domain for foreign security and defence policy - as well as the international law aspects - have been submitted to the Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law. The response of the government to the advice, which is expected in the first quarter of 2012, will discuss the international security dimension of cyber threats in greater detail, as cyber threats also have major consequences for foreign and military policies. During the General Consultations on National Security of 1 June 2011, the Lower House requested me to examine the article in the Wall Street Journal on the fact that the US consider each cyber attack as an act of war and to indicate how the Netherlands deal with this. The Lower House will be informed about this point in the policy response to the advice of the Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law. The policy response will be sent to the Lower House in the first quarter of 2012.

The Cyber Security Assessment Netherlands

The Cyber Security Assessment Netherlands (CSBN) was made by Govcert.nl and follows on from and links up to the National Risk Assessment and the National Trend Report Cybercrime and Digital Security 2010 that was published in November 2010 (2010-2011, 28 684, no. 292). The CSBN provides insights into the problems of cyber security and distinguishes between different forms of threats in the area of cyber security. For the development of the CSBN, the insights gained by the General Intelligence and Security Service, the Military Intelligence and Security Service, the National Police Services Agency, the National Coordinator for Counterterrorism and Security, and Govcert.nl in the performance of their respective tasks were bundled. This information was supplemented by the knowledge shared with them by the private parties with which they cooperate. The CSBN was subsequently submitted to the Cyber Security Council (CSR). The CSR provided advice to the government on the basis of the CSBN. You will find the CSR's response enclosed.

The CSBN is focused on threats present in the IT domain for the Dutch situation , but takes developments abroad into consideration as well, with the emphasis being on intentional acts. The CSBN includes information about types of perpetrators, targets, current threats, and vulnerabilities that could facilitate successful or attempted attacks.

At an international level, research into the scope of cybercrime and cyber attacks is still at a developmental stage as well. It is important to obtain a better understanding of the risks and incidents in the cyber domain. This notion is shared internationally. Although threat intelligence is shared in the trusted public-private networks, the affected organisations and companies in the Netherlands, but also in other countries, are still reticent about sharing information about incidents.
In order to get a broader and more quantitative picture of the problems, the NCSC will seek alignment with private parties more frequently and on a structural basis.
Insight into the nature and scope of cyber attacks will be increased on the basis of the existing public-private knowledge and information exchange, supplemented

by the introduction of a duty of notification, the so-called 'security breach notification' (2011-2011, 26 643, no. 202) proposed in the Hennis-Plasschaert c.s. motion.

Analysis and response to the Cyber Security Assessment Netherlands

Actors
The Cyber Security Assessment Netherlands (CSBN) sketches a wide range of groups who make use of technology and vulnerabilities to carry out cyber attacks in the Netherlands. The largest potential cyber threats are posed by states and criminals and to a lesser extent by hacktivists, script kiddies, and terrorists.
Criminals are responsible for the majority of all cyber incidents, as a result of which these are most tangible to society. States are, however, able to mobilise the knowledge and resources to carry out the most sophisticated and large-scale attacks.

Threats and vulnerability
Cyber espionage, cyber sabotage, and cybercrime are the major cyber threats the Netherlands is currently faced with. The year 2011 saw an increase in these incidents.

Cyber espionage and cyber sabotage
The CSBN shows evidence of an increased threat of cyber espionage. Public authorities and private organisations alike have been the target of cyber espionage on a regular basis, also in the Netherlands. These cyber attacks are aimed at obtaining confidential information of economic or political value or immediate pecuniary advantage.

The increasing probability of cyber sabotage is worrisome. For the time being, there has not been any evidence that the Netherlands appears to be a concrete target, but the Netherlands is vulnerable because it depends heavily on IT systems. An important development and warning in this area was the Stuxnet attack in 2010 and more recently the related Duqu virus. Stuxnet was the first known targeted attack on industrial control systems (ICS), also referred to as SCADA systems (Supervisory Control and Data Acquisition). Such attacks currently constitute a potentially serious threat to national - and possibly also international - security if critical infrastructure (such as energy, water, and finance) is struck. In the case of such complex attacks, the risk of social disruption is realistic.

Cybercrime
The majority of all cyber incidents concern cybercrime, of which the most substantial impact will be on society. It is clearly visible that the authorities, the business sector, and individual citizens run a real risk of falling victim to cybercrime. Businesses and citizens face the greatest threat from cybercrime. This serious threat, which is developing at a rapid pace, incurs substantial costs and is still increasing. Cybercrime is very attractive to perpetrators, for they can make fast money with a limited investment, whereas chances of being caught are slim. High-tech cyber criminals lead the way in improving methods of attack to make their attacks less visible and more goal-oriented. Cyber criminals are well-organised and have specialised in specific areas, in which they provide services. They carry out their attacks in temporary partnerships they enter into on Internet forums.

New developments
New developments that require attention are information security when contracting out services 'in the cloud' and the increased use of mobile equipment. When services are contracted out 'in the cloud' it is more difficult to establish whether the security of the data is adequate. In addition, there is the increased use of mobile equipment, which poses a growing risk due to the high penetration degree of this equipment. It is expected that serious attacks aimed at mobile equipment will increase in the next few years.

Response from the Cyber Security Council
The Cyber Security Council (CSR) gives solicited or unsolicited advice to the government about relevant developments in the area of cyber security. The CSR is composed of members from public, private, and academic parties. In performing this task, the CSR drew up a response to the Cyber Security Assessment Netherlands (CSBN).
The CSR agreed largely with the CSBN and endorsed the most relevant threats mentioned therein. With regard to the CSBN, the CSR mentioned two points requiring attention in order to further strengthen the CSBN. The first point concerns further qualitative development of the CSBN. The second point concerns further quantification of the threats. For this purpose it is necessary to cooperate with the private sector in order to be able to make an assessment that is as complete as possible. The CSR indicated that the CSBN should be a product of public-private cooperation and that it will provide its assistance in achieving this. The CSR furthermore indicated that it will set the following priorities next year: i) increase awareness of cyber threats among citizens, authorities, and the business sector; ii) increase attention for a proactive approach in addition to preventive measures; iii) availability of up-to-date and reliable threat and risk assessments; iv) develop an adequate response capacity that is supported by multiple actors; and v) increase and direct research and knowledge building.

Government response
The objectives identified in the National Cyber Security Strategy (NCSS) are in line with the problems outlined in the CSBN. The government has, for instance, developed a set of countermeasures in the area of cyber espionage and sabotage. A Vulnerability Analysis Manual has been made available for businesses, which they can use to increase their resilience. The Lower House has been informed about this by letter (2010-2011, 30 821, no. 13). In the next few years too, substantial investments will be made in strengthening and developing cyber capacities to address the military threat that emanates from cyber espionage and sabotage. The Lower House has been informed about this by letter (2010-2011, 32733, no. 1) and in the defence budget for 2012 (2011-2012, 33000x, no. 2). With regard to cybercrime, the government will take appropriate action to strengthen, among other things, the High-Tech Crime Team. The Lower House has been informed about this by letter (2010-2011, 29 628, no. 256). In the context of the Cyber Security Research Agenda, the public, private, and academic parties are focussing on, among other things, new developments and their associated risks. The military possibilities of application in the cyber domain have increased at a rapid pace and various armed forces have operational cyber capacities at their disposal or are developing them. The armed forces must be able to carry out cyber operations in support of regular military operations and must have an excellent intelligence position in the cyber domain. As announced in the letter titled 'Defence after the credit crisis' (Defensie na de krediet crises) (2010-2011 32733, no. 1) and in the defence budget for 2012 (2011-2012 33000 X, no. 2), the Ministry of Defence will therefore make investments to considerably strengthen its capacities and develop them further.

It is necessary that the Ministry of Defence develop the knowledge and capacities to take offensive actions in the cyber domain. The armed forces must also be able to make it impossible for an opponent to take action in the cyber domain. In this context, the armed forces must establish escalation dominance over each opponent in order to be able to be effective in all circumstances. The development of offensive capacities will also strengthen the defensive capacities at the same time. This will be realised in 2012, among other things by developing a defence cyber doctrine. In order to ensure the deployability of the armed forces, measures will furthermore be taken to increase cyber resilience, in particular by extending the tasks of the Defence Computer Emergence Response Team (DefCERT). Early next year, DefCERT will conclude an agreement with the NCSC to increase the cooperation. This concerns both information exchange and support (staff support and otherwise) in contingencies. The intelligence and knowledge position of the Ministry of Defence will also be strengthened in the next few years, in particular by increasing the capacity at the Military Intelligence and Security Service. The cooperation with the General Intelligence and Security Service will also be intensified.

In January 2012, the Cyber Task Force will be established under the leadership of the Chief of the Netherlands Defence Staff; the Cyber Task Force will be responsible for the development of cyber capacities. The priorities for the Ministry of Defence will subsequently be the formation of a Defence Cyber Command and a Defence Cyber Expertise Centre, which will also be responsible for increasing national and international cooperation.

International information exchange and cooperation are essential to a proper threat assessment and adequate approach to incidents. The Netherlands is therefore seeking alliances with cyber security centres in various countries, building on existing cooperations such as the CERT networks. NATO's revised cyber policy, which was drawn up in connection with the new Strategic Concept, which explicitly includes cyber threats, sharing information and improved response, also contains important objectives that were advocated by the Netherlands. The Netherlands has furthermore invested in cooperation at the European level. Consequently, the government will continue the comprehensive approach laid down in the NCSS unabatedly.

The government endorses this response from the CSR and will fully implement the CSR's recommendations. In 2012, the government will consequently aim for a quantitative and qualitative improvement of the CSBN. The National Cyber Security Centre (NCSC) will seek alignment with private parties on a more frequent and structural basis for further quantification of the threats as described in the CSBN. The government has readily accepted the CSR's offer to provide assistance in further quantifying the identified threats.
Qualitative improvement of the CSBN is an ongoing process. The CSBN will be further developed into a fully-fledged threat and risk assessment. The second CSBN will be sent to the Lower House in the middle of 2012. The priorities of the CSR are in line with the points the government will focus on in 2012 in the context of the NCSS: i) increase awareness of cyber threats among citizens, authorities, and the business sector; ii) increase attention for a proactive approach in addition to preventive measures; iii) availability of up-to-date and reliable threat and risk assessments; iv) develop an adequate response capacity that is supported by multiple actors; and v) increase and direct research and knowledge building. The Lower House will be informed about the progress of the implementation of the NCSS in the spring of 2012.

Cyber Security Legal Framework

During the General Consultations on National Security of 1 June 2011 mentioned above, the legal framework for the implementation of the National Cyber Security Strategy (NCSS) was discussed. In the enclosed Legal Framework, it was decided to adopt the different stages of promoting cyber security as a starting point: prevention, supervision, duties of notification, intervention, investigation, and repression. This is preceded by the relevant constitutional and treaty frameworks. Finally, attention is paid to the safeguards in this area that are of importance to individuals.

The Legal Framework does not only deal with laws and regulations that are aimed specifically at cyber security. It also deals with laws and regulations on powers and other possibilities that may be relevant in the context of cyber security. The document consequently has a broad scope, but it is not intended as an exhaustive overview of legislation, but primarily as an identification of relevant aspects. Various public and private parties involved in this area have been consulted for the purpose of drawing up this letter.

With regard to the Cyber Security Legal Framework, it is important to know what must be understood by the term 'cyber security'. It was decided to adopt the definition as used in the NCSS of 22 February 2011.[2] In this document, the term 'cyber security' is defined as free from the risk or damage caused by IT disruption or failure or abuse of IT.

The risk or damage due to abuse, disruption or failure include reduced IT availability and reliability, breach of the information stored in IT, and impairment of the integrity of that information. Cyber security consequently provides for both intentional and unintentional incidents and disruptions of IT networks.

Cyber security is a broad area in which many aspects overlap with many other policy areas, including privacy policy, telecommunication policy, and foreign security and defence policy. These areas have only been included in this Legal Framework insofar as there appears to be an immediate connection. With regard to privacy policy, including the obligation to notify data leaks (personal data), please refer to the letter to the Lower House titled:

'Processing and Protection of Personal Data' (*Verwerking en bescherming persoonsgegevens*) (Lower House of Parliament 2010-2011, 32 761 no. 1) and the commitments made during the General Consultations of 15 September 2011.

As indicated above, requests for advice regarding the implications of developments in the cyber domain for foreign security and defence policy, including attention to international law aspects, have been submitted to the Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law. The Lower House will be informed about this subject in the short term. In relation to the Franken motion (Senate, 31051, 17 May 2011), I would like to emphasise that this government attaches great value to the protection of privacy and that it will take due consideration of this aspect in drafting new laws and regulations, also in the area of cyber security.

Constitutional and treaty frameworks

---

2 Lower House of Parliament 26643 no. 174.

The constitutional and treaty frameworks describe the rights and duties of the authorities with respect to citizens. The constitutional and treaty frameworks are relevant in particular if the legislator decides to adopt additional laws and regulations on cyber security. In these cases, the legislator must determine whether the laws and regulations proposed are in line with these frameworks.

As far as current laws and regulations on cyber security are concerned, these have been reviewed against the constitutional and treaty frameworks already in the drafting stage. In principle, the court does not review laws and regulations against the constitutional framework after the date of entry into force: this review is excluded by Section 120 of the Dutch Constitution. The court does have the possibility to determine whether laws and regulations and government actions are in line with treaties that may be relied upon, such as the European Convention of Human Rights ("**ECHR**").

Pursuant to Section 10 of the Dutch Constitution and Article 8 of the ECHR for instance, everyone has the right to respect for his or her privacy. Privacy relates to numerous areas, which vary greatly in nature[3] and include, for instance, one's home, correspondence, and communication by telephone or other means of communication.

The starting point of these provisions is that the authority may exclusively place restrictions on privacy in cases that have been provided for under or pursuant to the law. Pursuant to Article 8 of the ECHR, these restrictions are only permitted if they are necessary for the protection of specific interests, including national security and public safety as well as the economic well-being of a country. Section 10(2) of the Dutch Constitution furthermore requires that the law prescribes rules regarding the recording and provision of personal data.

It is evident that respecting the constitutional and treaty frameworks is beyond dispute.
This is the guiding principle in drafting new laws and regulations, in which context the specific points from the Franken motion[4] regarding privacy are endorsed by the government.

Prevention and supervision
At this stage, it is important to prevent a cyber incident from occurring, among others things by checking and improving security, collecting information about risks, and exchanging information among parties.

Legislation of a general nature
The Dutch Civil Code applies in those cases where the authorities (as a client) enter into a contractual relationship with a contractor. This contractual relationship is an important preventive means to improve the level of information security by provisions that impose a specific level of information security on the contractor.

By means of the Dutch Personal Data Protection Act, personal data processors are obliged to take appropriate technical and organisational measures to protect personal data against loss or any form of unlawful processing. This is a general obligation on personal data processors. The Dutch Data Protection Authority is the

---

3 See Parliamentary Papers II 1975-1976, 13 872, no. 3 p. 40.

4 See Senate, session year 2010-2011, 31 051, D.

supervisory authority charged with the supervision of the general obligation. In various sectors, however, certain sector-specific obligations apply that must be fulfilled. In the letter to the Lower House titled 'Processing and Protection of Personal Data' (*Verwerking en bescherming persoonsgegevens*) (Lower House of Parliament 2010-2011, 32 761 no. 1), the State Secretary for Security and Justice and the Minister of the Interior and Kingdom Relations extensively discussed the approach to sanctions for violating the Dutch Personal Data Act.

Intelligence and security services
The Dutch Intelligence and Security Services Act 2002 describes the tasks and regulates the powers of the Dutch intelligence and security services, namely the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD).
Within the scope of the description of their tasks, the AIVD and MIVD are authorised to investigate cyber attacks and the threat thereof in and from the cyber domain. The Intelligence and Security Services Act 2002 was drafted in a period when aspects which are currently considered as belonging to the cyber domain did not play a prominent role in the sphere of activity of these services. It will be examined carefully whether the Intelligence and Security Services Act 2002 contains elements which have been superseded by advancing technological developments and which limit the services unintentionally in the proper execution of their tasks in the cyber domain.

The Minister of the Interior and Kingdom Relations and the Minister of Defence will inform you about this subject separately, if necessary.

Sector-specific obligations
In addition to general laws and regulations, there are also sector-specific laws and regulations such as obligations for the various sectors.
These laws and regulations are often characterised by the specific focus on the sector. This does not alter the fact, however, that these laws and regulations may be relevant for the purpose of cyber security. The Legal Framework explains a number of obligations that apply to financial institutions, mains services, telecommunication services, care institutions, and railway transport. Pursuant to the supervisory powers assigned to the sector-specific supervisory authorities, these authorities supervise the manner in which the duties of care laid down in laws and regulations which are applicable in the relevant sector are implemented.

However, the sector-specific duties of care have often been formulated in a general way and have not been designed specifically for the prevention of cyber security incidents. These duties of care will be further specified, in particular in those cases in which the institutions are of vital public interest. In this way, the supervisory authorities will be better equipped to monitor aspects that are relevant to cyber security. Specification will be effected on the basis of consultations with the relevant sectors and supervisory authorities and with the assistance from experts from the National Cyber Security Centre (NCSC) that is to be established next year.

Duties of notification and measures
In general, there is a duty of notification under criminal law if a state secret is breached or if someone is in mortal danger/ if lives are at stake. These cases are, however, extremely specific. In contractual relations, it is also possible to demand a duty of notification or deem it good contractor behaviour.

There are also various sector-specific duties of notification of diverse nature. Institutions quoted on the stock exchange, for instance, must immediately disclose any price-sensitive information. As far as immediate duties of notification are concerned, various procedures have been started. It is important to note in this context that the government has adopted as a starting point that it will not examine the possibilities of laws and regulations until self-regulation has proved ineffective.

Firstly, there are two duties of notification that ensue from the proposed amendment of the Dutch Telecommunication Act. This legislative proposal has been submitted to the Senate.

The legislative proposal contains two duties of notification for different supervisory authorities at a common centre. The first duty of notification (Section 11.3a of the Dutch Telecommunication Act) deals with breaches that have a detrimental effect on the protection of personal data. The scope of application of this Section is limited to providers of electronic communication services.
Secondly, this legislative proposal also introduces a duty of notification regarding the continuity of electronic communication networks and services by means of the proposed Section 11a.2. This Section deals with breaches of security or loss of integrity as a result of which continuity was severely disrupted Contrary to the duty of notification from Section 11.3a, the duty of notification from Section 11a.2 is consequently not specifically designed for personal data.

The above-mentioned duties of notification are, however, sector-specific duties of notification. These duties of notification arise from European Directives.
In a broader sense, it was previously announced in the Coalition Agreement that the government would come up with a proposal for a duty of notification for all services of the information society in the event of loss, theft or abuse of personal data, with the data leaks being notified to the national supervisory authority. The State Secretary for Security and Justice[5] already indicated that a legislative proposal on this subject will be submitted for consultations in the short term. In this case it concerns a duty of notification which centres on the element of personal data.

By virtue of the Hennis-Plasschaert c.s.[6] motion, the Lower House furthermore requested in the debate on DigiNotar of 13 October 2011 to introduce a statutory duty of notification, a so-called 'security breach notification'. This notification of breaches is intended for organisations that are involved in information systems which are of vital public interest. This duty of notification has not yet been discussed in the Legal Framework, as it does not relate to existing laws and regulations. It is evident from the Legal Framework, however, that there is currently not an immediately obvious Act of Parliament within the current legal framework that could be used to include this duty of notification without delay. The relevant legislation (see the examples above) is after all sector-specific in nature or aimed at personal data. The Hennis-Plasschaert c.s. motion indicates that the notification should be aimed at those information systems that are vital to public interest.

Before the summer recess of 2012, the Lower House will be informed about the manner in which this duty of notification will be structured and in which manner information can be shared with the National Cyber Security Centre (NCSC).

---

5 In reply to oral questions during question time of 25 October 2011.

6 See Parliamentary Papers 2010/11, 26 643, no. 202.

Important guiding principles for the government in this context are reducing the administrative burden and ensuring the confidentiality of shared information with the NCSC.

Intervention and investigation
The authorities have various intervention options when a cyber incident occurs or threatens to occur. These powers ensue from criminal law, administrative law, and - to a limited extent - civil law. In addition, the authorities have powers in exceptional circumstances, for instance to control a crisis or an imminent crisis or if these are insufficient, the powers provided by the Dutch Coordination (Exceptional Emergencies) Act. Practice shows, however, that the latter are used very rarely, due to the stringent conditions.

Government interventions at the time of a cyber crisis or imminent cyber crisis, when national security is at issue, must fulfil a number of requirements before they will be effective in this area. First of all, the scope of the measures must be adequate, for cyber incidents usually do not only occur within the IT sector itself, but affect more than one sector. Secondly, effective intervention requires technical or other expertise in order to being able to assess the complex consequences correctly. Thirdly, it is important that expedient action can be taken in case of an attack or disruption or threat thereof.

The current legal framework shows that there is presently not a legal basis for government intervention along the line outlined above.
It is true that the Minister of Economic Affairs, Agriculture and Innovation has far-reaching powers pursuant to Chapter 14 and Section 18.9 of the Dutch Telecommunication Act, but these powers are limited to providers of electronic communication networks and services. It consequently appears that the parties that are relevant to the vital interests of the Dutch State cannot be reached adequately at present.

As stated above, taking expedient action is also essential at the time of an imminent cyber crisis. When national security is at issue, which is the case if vital interests of the Dutch State and/or the public interests are threatened to such an extent that it is a matter of social disruption or potential social disruption, it is possible to convene the Ministerial Committee for Crisis Management (MCCB). In case of cyber crises, there may not be any time to await these ministerial consultations and it may be desirable to have another Minister assume temporary powers. The possibility of transferring a number of specific existing powers to the Minister of Security and Justice, so that immediate action can be taken, is currently only possible at the time of a terrorist threat.

Although regular structures will usually be perfectly capable of dealing with the incident in most cases, it seems desirable for the authorities to have new additional powers available in the above-mentioned crisis situation so that they can take expedient, efficient, and coercive action.
This is endorsed by experiences gained during recent incidents such as the DigiNotar crisis.

Just as in the case of a 'security breach notification' as proposed in the Hennis-Plasschaert motion, there does not seem to be any immediately obvious legislation with respect to cyber crises either within the current legal frameworks, on the basis of which it is possible to take expedient, efficient, and coercive action in the event of crises. Research into additional intervention options will consequently be regarded in conjunction with the elaboration of the 'security

breach notification'. The Lower House will be informed about the results of this research before the summer recess of 2012.

Investigation
Section 5.3 of the Legal Framework also deals with the investigative powers under criminal law. Both at the national and international level, procedures have been started to examine the necessity of amending laws and regulations in order to have sufficient possibilities for investigation on the Internet as well. The previous government submitted a number of draft legislative proposals for advice in 2010. The outcome of this advisory procedure has resulted in the conclusion that more time is required to come to actual legislative proposals. Other issues ensuing from practice, such as combing the Internet, are being explored. I will send the Lower House further information about this before the summer of 2012.

Enforcement and repression
The possibilities of enforcement and repression that are relevant to cyber security may ensue from both administrative law and criminal law.
Interesting in this context - considering the often cross-border nature of cyber incidents - is the issue of international jurisdiction regarding data. The Netherlands has adopted the position that it has jurisdiction over data that are stored on servers located on Dutch territory.

Safeguards
Laws and regulations provide safeguards to private parties in order to monitor government action in the context of cyber security and, if necessary, to take legal action against it. The safeguards referred to in this context are those concerning legal rights under administrative law (objection and appeal), civil law (damages), and criminal law (including ECHR). The Dutch Government Information (Public Access) Act regulates the disclosure of information by the authorities and the Dutch Personal Data Protection Act regulates the processing of data that may identify natural persons directly or indirectly.

Keeping the legal instruments up-to-date is an ongoing process
This government advocates secure and reliable IT and the protection of the openness and freedom of the Internet.
Increased dependence on IT makes society increasingly vulnerable to abuse and disruption, large-scale or otherwise. This is the reason why the government adopted the National Cyber Security Strategy in February of this year.

The existing Cyber Security Legal Framework, the basic structure of which has been enclosed with this letter, basically gives sufficient points of reference for its implementation. Considering the cross-border nature of the cyber domain, the Netherlands will contribute actively to an adequate international legal framework. Keeping the legal instruments up-to-date is consequently an ongoing process. On several points it has been established that additional instruments may be necessary to improve cyber security in the Netherlands. These instruments do not always have to be of a legal nature.

For the purpose of an open and free cyber society, it is essential that the authorities respect and protect privacy.

IT is an important driving force behind economic growth; government measures aimed at the security and reliability of IT should consequently not impose an unnecessary administrative burden that may result in a deterioration of

international competitiveness. The starting point is always: self-regulation where possible, legislation where necessary.

Jurisdiction in Austria
In reply to your request for more information about the assumed cross-border jurisdiction within Austrian cybercrime legislation, I can advise the following. Austria has included a prohibitory provision sanctioned pursuant to administrative law in its Telecommunication Act regarding cold calling, spam, and text messages. If the prohibited cold call, spam or text message did not occur or was not sent from Austria, the place where the prohibited cold call, spam or text message is received is designated as the scene of the offence. [7] This guarantees jurisdiction for Austria, as it is the country where the direct consequence of the offence manifests itself.

As it concerns an administrative sanction that is designed specifically for spam and text messages, this construction does not offer a solution for international criminal investigations.
As stated above, the Netherlands is bound by existing international law agreements, which cannot be changed unilaterally. The Dutch efforts are aimed at strengthening the possibilities for an effective approach to cross-border cybercrime. The Netherlands will do so by encouraging the ratification of the Convention on Cybercrime of the Council of Europe and, practically, by establishing joint investigation teams in Europe and by entering into international bilateral cooperation.

National Cyber Security Centre (NCSC)

The NCSC will be operational as from 1 January 2012. The ambition of the NCSC is to increase cyber resilience of Dutch society. The NCSC will aim to achieve this by gaining insight into, among other things, cyber trends, threats, incidents, and vulnerabilities, and furthermore by providing a perspective for action or support when a threat, incident or crisis occurs. The NCSC will structure its ambition along the following three pillars:

- Developing and providing expertise and advice
- Providing assistance and response in the event of threats or incidents
- Strengthening crisis management

The success of the NCSC depends on the input of knowledge and expertise from both public and private parties. Important preconditions in this context are close cooperation and being able to share information about a confidential basis. The authorities will invest in the NCSC by means of, among other things, the contribution (in January 2012) from Govcert.nl, the ICT Response Board[8], and representation from various relevant public parties (including the General Intelligence and Security Service (AIVD), Police, Public Prosecution Service, Defence, and Netherlands Forensic Institute (NFI)). With this strong basis, the government invites other relevant private and public parties to join the NCSC. In 2012, the government will aim for linking critical infrastructure sectors to the NCSC. So far, several appropriate steps have been taken in this area in the form of participation of private parties in the public-private ICT Response Board. The year 2012 will see a process of linking the Information Sharing and Analysis Centres with the NCSC. In this context, the following sectors will be the first to be approached: energy, IT/Telecommunication, finance, drinking water, surface

---

7 See § 107(6) of the Austrian Telecommunication Act.

8 In which experts of both public and private parties will participate.

water defence and management, and transport. Together with all partners (in particular the vital sectors), the NCSC is working on increasing cyber resilience of the Netherlands. Each party will have its own responsibility for this purpose. In this context, the NCSC will assist the different parties and act as a facilitator in order to enable them to fulfil this responsibility in an adequate manner.

In Conclusion

The CSBN provides insight into the problems of cyber security and distinguishes between different forms of threats in the area of cyber security on a regular basis. Cyber spying, cyber sabotage, and cybercrime are the major cyber threats the Netherlands is currently faced with. The government will continue the comprehensive approach laid down in the NCSS unabated. In 2012, the government will consequently aim to achieve a quantitative and qualitative improvement of the CSBN. The second CSBN will be sent to the Lower House in the middle of 2012.

In concrete terms, the government will focus on in 2012 in the context of the NCSS: i) increase awareness of cyber threats among citizens, authorities, and the business sector; ii) increase attention for a proactive approach in addition to preventive measures; iii) availability of up-to-date and reliable threat and risk assessments; iv) develop an adequate response capacity that is supported by multiple actors; and v) increase and direct research and knowledge building. The Lower House will be informed about the progress made in the spring of 2012.

It is evident from the Cyber Security Legal Framework that there is currently not an immediately obvious Act of Parliament within the current legal framework that could be used to include the elaboration of this duty of notification, as proposed in the Hennis-Plasschaert motion. The Lower House will be informed about the manner in which the duty of notification will be implemented before the summer recess of 2012. It is also evident from the Cyber Security Legal Framework that it seems desirable to have new additional powers available in the event of a cyber crisis, which powers could be used by the government to take expedient, efficient, and coercive action. This is endorsed by experiences gained during recent incidents such as the DigiNotar crisis. Just as in the case of the duty of notification proposed in the Hennis-Plasschaert motion, it may be concluded with respect to cyber crises that there does not seem to be any immediately obvious legislation on the basis of which it is possible to take expedient, efficient, and coercive action in the event of a crisis. Research into additional intervention options will consequently be regarded in conjunction with the duty of notification, the so-called 'security breach notification'.

The NCSC will be operational in January 2012. The NCSC will structure its ambition along the following three pillars: i) Developing and providing expertise and advice; ii) Providing assistance and response in the event of threats or incidents; and iii) Strengthening crisis management. The authorities will invest in the NCSC by means of the contribution from Govcert.nl, the ICT Response Board (in which experts of both public and private parties will participate), and a representation from various relevant public parties (including the General Intelligence and Security Service (AIVD), Police, Public Prosecution Service, Defence, and Netherlands Forensic Institute (NFI)). With this strong basis, the government invites other relevant private and public parties to join the NCSC. In 2012, the government will continue its efforts in this context.

Both during bilateral visits and during the London Conference on Cyberspace in November 2011, where politicians and representatives from the business sector and civil society organisations from approximately 60 countries talked about a common agenda for the cyber domain, the Netherlands highlighted its approach and many countries and participants appeared to be interested in cooperating with the Netherlands. This will be followed up in 2012.

The government will aim at strengthening security in the cyber domain unabatedly. In order to achieve this, the comprehensive approach together with the private parties of the National Cyber Security Strategy (NCSS) and international partners will take centre stage.

The Minister of Security and Justice

I.W. Opstelten

Annex: National Cyber Security Centre (NCSC)

1. Why an NCSC?

Dutch society is becoming more and more dependent on the digital infrastructure and as a result of this it is vulnerable to the disruptions of vital functions such as telecommunication, banking, water treatment, and energy. Disruptions may, among other things, be related to cybercrime, cyber espionage, and targeted cyber attacks such as Stuxnet[9]. Examples that occurred recently are DigiNotar, the 'leaks' in various government and public websites, and the Duqu malware. These disruptions, intentional or unintentional, may have consequences for the prosperity and welfare of Dutch society.

The National Cyber Security Strategy (NCSS), as adopted by the government, was presented on 22 February 2011. The NCSS emphasises a comprehensive approach (public, private, and academic) to cyber security, because the responsibility for cyber security in the Netherlands lies with many different parties. In order to improve the relationship at the operational level, the government will dedicate itself to set up a National Cyber Security Centre (NCSC), where parties will be able to meet and cooperate.

2. Tasks Formulated in the NCSS

The government announced in the NCSS that the NCSC will be operational as from 1 January 2012. The government formulated the following tasks:
To bring together public and private parties in order to exchange information, knowledge, and expertise so that insight may be gained in developments, vulnerabilities, threats, and trends and assistance may be provided in dealing with incidents and crisis decision making. The government invites private and public parties to join the National Cyber Security Centre (NCSC). In order to make this possible, the government will develop a cooperation model. The current GOVCERT.NL will be expanded, strengthened, and incorporated into the NCSC.

3. Ambition

The ambition of the NCSC is to increase cyber resilience of Dutch society. The NCSC will aim to achieve this by gaining insight into, among other things, trends, threats, incidents, vulnerabilities, and risks in the cyber security domain. It will furthermore provide a perspective for action when a threat, incident or crisis occurs. The NCSC will structure its ambition along the following three pillars:

<u>Developing and providing expertise and advice</u>

The NCSC is a centre where expertise about cyber security is present and is developed, partly through the input of knowledge and expertise from cooperation partners. The NCSC will focus this expertise on the following four themes:

a. To increase the awareness of end users, managers, policy makers, and administrators about the nature, scope, and urgency of cyber threats, among other things, by strategic publications such as the Cyber Security Assessment Netherlands (CSBN).
b. To contribute to the prevention of possible cyber incidents by providing guidelines for cyber security.
c. To share knowledge by providing products such as fact sheets for managers and detailed White Papers for IT experts.
d. To provide advice about possible perspectives for action in the event of vulnerabilities or threats. This advice may be provided in general or to a specific party (e.g. tailor-made advisory services).

---

9 National Cyber Security Strategy, see Parliamentary Papers 2010/2011, 26643, no. 174.

Providing assistance and response in the event of threats or incidents

By building up knowledge and expertise, the NCSC will be capable of providing adequate assistance in the event of a threat or an incident. Starting point for the NCSC is to provide a secondary response towards the Central Government and a tertiary[10] response towards the critical infrastructure sectors. In concrete terms, the NCSC will provide the following:

- Warnings about acute threats;
- Assistance from a distance or on site in, among other things, technical, communicative, and legal aspects.
- Services such as cleaning botnets and making evaluations of incidents.

Strengthening crisis management

The NCSC will fulfil a major role in the event of an IT crisis. The NCSC may also contribute to strengthening crisis management by providing assistance in cyber exercises (large scale or otherwise) and scenarios. The core activities of the NCSC in the event of an IT crisis are as follows:

- Facilitate the ICT Response Board (IRB): an IRB will be set up if a crisis occurs[11]. The IRB will subsequently issue an advice to take measures to the national crisis structure. The IRB is guaranteed through the NCSC;
- Operational coordination: The NCSC is responsible for coordinating the collection and interpretation of operational information. In addition, the NCSC assists in the implementation of the measures adopted by the national crisis management structure.

The crisis-related procedures will be laid down in the National IT Crisis Plan.

4. Cooperation: For and by Cooperation Partners

The NCSC will form a cooperating platform (physically and virtually) where the leading public and private partners (including academic and research institutions) in the area of cyber security will be brought together and where sharing operational information / knowledge will be facilitated in an effective and reliable manner.

The added value is provided if information, knowledge, and expertise are shared among the partners with a clear focus or used effectively by bundling (e.g. during a major IT crisis).

The forms of cooperation offered by the NCSC include the following:
(1) Liaison: partners are engaged in the NCSC through one or more liaisons (working at the NCSC on a daily basis);
(2) Contact person: A contact person will continue to function within his/her own organisation/network organisation, but will act as the point of contact for this organisation/network organisation on behalf of and towards the NCSC.

---

[10] Explanation of services with regard to incident response:

- Primary incident response: incident response by the institution's and companies' own internal IT organisations (existing capacity and under one's own responsibility);
- Secondary incident response: a coordinating and sector-oriented 'CERT' is responsible for incident response within a sector or line of business (the sector-oriented CERT for the Central Government is the NCSC, and for the academic sector it is Surf Cert);
- Tertiary incident response: incident response as a supplement to the secondary incident response. For example: the deployment of the NCSC as a supplement to the incident response to vital sectors (e.g. assistance for Surf Cert from the NCSC).

[11] The composition of the IRB depends on the type of crisis and consists of public and private experts.

(3) Ad hoc cooperation in, for instance, theme-oriented projects or research projects.

NCSC's most important cooperation partners are the following:

- The Central Government and the critical infrastructure sectors. They have a special position in ensuring a secure and stable cyber society; the products and services of the NCSC are consequently tailored primarily to these partners;
- National and international organisations with public duties. These organisations include intelligence and security services, investigation services, forensic examination services, and defence;
  a. National and international knowledge and research partners. These partners include universities and other national and international knowledge and research centres;
  b. The research and other parties mentioned in the National Cyber Security Research Agenda;
  c. National and international private suppliers. These partners include Internet service providers, IT security specialists or other knowledge suppliers or services providers. Private suppliers are engaged in the NCSC on a structural basis to ensure that quick action can be taken at the time of an IT crisis or threat;
  d. National and international cyber security community. This community consists of public and private CERTs in the Netherlands and abroad, as well as international Cyber Security centres and networks and constitutes the international backbone of knowledge, information, and response.

5. Development of NCSC: Growth Model

For the purpose of building up confidence among the cooperation partners within the NCSC, the NCSC will use a growth model. In the course of time, the number of cooperation partners will be increased and the relationship with the partners will be consolidated further to ensure the quality of the services.

<u>What will have been realised by January 2012?</u>

The NCSC will be launched in January 2012. The contours of the NCSC are already visible (including operational management, accommodation, IT, and appointment of the NCSC Director) and measures have been taken to strengthen staff capacity[12] and resources.
The organisation of the NCSC has been laid down. The NCSC will function where appropriate from its new roles and tasks (including the relevant mandates), in which the current tasks of GOVCERT.NL have also been incorporated in the NCSC. Several cooperation partners, such as intelligence, security, and investigation services, will contribute knowledge and expertise. The ICT Response Board is operational.

<u>What will happen in the course of 2012?</u>

In 2012, the cooperation will be fleshed out further by linking an implementation group of cooperating organisations to the NCSC. This implementation group will be composed of organisations from the Central Government and a selection of organisations from the critical infrastructure sectors. It is expected that the 6

---

12 This strengthening also concerns persons with specific expertise in the area of cyber security.

preconditional vital sectors[13] as well as the financial sector will be linked to the NCSC. These sectors are of vital importance to the functioning of Dutch society and will be hit hardest in the event of a crisis[14]. In order to further deepen the relationship with the vital sectors, the NCSC will participate actively in the Information Sharing and Analysis Centres of the vital sectors.

What will happen as from 2013?

The foundations of the NCSC will be expanded and strengthened further. The NCSC will have drawn up a strategic plan for the years 2013-2016 which provides a framework for the implementation of the NCSC. This plan will include the lessons learnt in 2012 as well as the new ambitions for the next two years. The cooperation with the partners will have been given more structure and will be ready for a broader roll-out.

The range of products and services will be extended and improved in quality. The number of cooperation partners will also be increased. Alliances will, for instance, be sought with the other vital sectors and other target groups such as non-vital multinationals. Finally, alliances will also be sought at this stage with national and international knowledge and research partners.

6. Governance

The performance of the activities and the accountability for the results of the NCSC will be organised on the basis of a cycle of annual reports and accounts.

a The annual reports and accounts will be drawn up under the responsibility of the head of the NCSC. The annual reports and accounts will be drawn up together with all active partners in the NCSC (public, private, and academic partners). By means of the annual reports and accounts, the parties will ensure that the tasks to which they contribute within the NCSC are safeguarded and that clear performance agreements have been made.

b The annual reports and accounts will be assessed and adopted by an NCSC programme group, consisting of public-private representatives, under the responsibility of the National Coordinator for Counterterrorism and Security. Following the adoption, the annual reports and accounts will be submitted to the Cyber Security Council (CSR) for notification.[15] The Lower House of Parliament will be informed about the annual reports and accounts by means of the annual progress report on cyber security.

The NCSC will be managed by a head who will be charged with the day-to-day management. This head is responsible for the performance of the tasks of the NCSC. These tasks include the formation of a cooperating platform, incident response, operational management during a crisis, and the activities agreed upon for fulfilling NCSC's role to provide expertise and advice. In addition, the head will be responsible for the financial results of the products and services provided by the NCSC.

---

[13] Electricity, natural gas, drinking water, telecommunication/IT, surface water defence and management, and road and other transport during a crisis.

[14] In this context, the financial sector is a trendsetter in the implementation of cyber security in its sector.

[15] There is not a direct controlling relationship between the NCSC and the CSR. The NCSC does provide products to the CSR (e.g. the Cyber Security Assessment Netherlands (CSBN) to be published on a regular basis).

The appointment of a head/director for the NCSC to perform the core tasks of the NCSC and the use of cycle of annual reports and accounts will ensure sufficient distance to and independence of 'policy'. At the same time, it is important that 'policy' is adequately informed about operational information and knowledge from the NCSC that is relevant for policy development, so that the advice provided on political issues is realistic and based on the latest developments.

The organisational responsibility for the NCSC, such as general IT facilities and accommodation, falls under the responsibility of the Ministry of Security and Justice and the National Coordinator for Counterterrorism and Security. Because the NCSC is part of the Ministry of Security and Justice, the continuity of the NCSC is guaranteed.

7. Sharing Information in a Trusted Environment

One of the functions of the NCSC is to be the place where public and private parties and public parties among themselves can share information. The centre will perform a pivotal function. The NCSC uses the starting point that it will be a trusted environment where parties can and will feel free and secure to share information within the current legal frameworks. The confidentiality of this information will consequently be guaranteed in conformity with the agreements that will be made with the partners. The partners will conclude an agreement setting out the agreements about the manner in which the information will be shared. The agreements may, for instance, relate to the manner in which the information will be protected or to the nature of the information shared. The starting point is that existing legislation is the guiding principle for the participants. Specific participants in the NCSC, such as the intelligence and investigation services, are, for instance, bound by a specific legal framework about the manner in which they are permitted to share information. Establishing mutual confidence among the parties in order to share information will take time and will be achieved gradually.

8. Finance

The Ministry of Security and Justice has made a provision in its budget for the basic funding of the core activities of the NCSC. This provision is made, among other things, for the key tasks of the NCSC, such as sharing information and developing knowledge, but also for office facilities and other facilities for the physical liaisons/participants. This will create a sound financial basis for the NCSC. Additional tasks or activities will be financed according to different flows of financing:

- Programme, project or task finance: if the NCSC carries out specific programmes, projects or tasks that fall under the political or other responsibility of a different party (e.g. network monitoring of the Central Government), a separate agreement for the provision of services will be concluded between the relevant party and the NCSC (including agreements about financial resources). This finance may also include subsidies or research funds, for instance through the EU.
- Subscription finance: this means that parties pay a remuneration for specific products and/or services provided. This will cover the costs incurred. This model is currently used by GOVCERT.NL.
- Finance with by 'paper transactions': the basic principle is that the cooperation partners contribute and share information within the NCSC under their own responsibility (and budget).

Dutch Anti Botnet Initiative

Niels Huijbregts
Public Affairs officer
XS4ALL Internet

nielsh@xs4all.net

Brussels, March 16, 2011

[redacted]

What

Co-operation between Dutch ISP's to fight botnets

Initiated by 7 ISPs and OPTA in 2009

bbned Online [redacted] TELE2 Ziggo

upc kpn OPTA

Currentely 15 ISPs have joined the initiative, covering over 90% of the Dutch broadband market

Why

3 reasons:

1. fighting network abuse is necessary

To protect customers, our own network and the internet in general

Why

3 reasons:

2. PR: media attention creates awareness

Internet security is complex: customers must understand that they have a role to play

Why

3 reasons:

3. Taking action is better than waiting for regulation

How

Treaty containing 3 elements

1. Informing customers
2. Isolating infected connections
3. Sharing knowledge and information

How

1. Informing customers

Easy to understand, yet thorough information about security risks and threats, and how to deal with them

How

2. Isolating infected connections

Filtering, blocking, disconnecting or isolating customer connection upon finding out is part of a botnet.

XS4ALL: walled garden with only partial block

How

3. Sharing knowledge and information

Informing other ISPs about detected infections, sharing information on internet security related issues

SMALL

It works!

Treaty became effective in january 2010 and has been working quite well since then.

Lessons learned

This initiative is a good thing: customers understand the problem, are willing to co-operate in keeping the internet clean.

Lessons learned

It isn't easy to convince management that shutting down customer connections is a good thing.

Lessons learned

It's even harder to convince management that they have to make substantial investments in a system which is user-unfriendly and doesn't have a clearly predictable ROI

Lessons learned

The Dutch Anti Botnet Initiative was created by policy makers, not by network security people.

Security people tend to be suspicious of everything and co-operation is based on trust.

Lessons learned

Co-operation between competitors requires trust.

Trust takes time to grow. Don't force it.

XS4ALL

Current developments

15th ISP joined the treaty last week

Current developments

Central information clearing house

Collecting and interpreting data on trojan infections and botnets; Supply this information to relevant ISPs

We're currently looking for funding

XS4ALL

Questions?

Meeting on January 18, 2012, with Mr. H. David Plunkett, Canada's Ambassador to the European Union

ISSUE

- You will be meeting Mr. H. David Plunkett, Canada's Ambassador to the European Union (**TAB E**), to discuss cyber security in advance of your meeting with officials from the European Commission's Directorate General of Information Society and Media and the European Network and Information Security Agency.

STRATEGIC OBJECTIVES

- Seek an assessment from the Ambassador of the political priority given to cyber security and more broadly on the Digital Agenda in Europe.

- Leave Canadian officials with a greater understanding of ongoing efforts to implement *Canada's Cyber Security Strategy*.

STRATEGIC CONSIDERATIONS

As background for Mr. Plunkett, you may wish to note the priority placed on implementing *Canada's Cyber Security Strategy*. A number of accomplishments to date have been included at **TAB F**.

In October 2011, meetings with European Commission officials indicated that the appropriate organization with which to discuss cyber security was the Directorate General of Information Society and the Media. To date, Canada has not yet officially met with European officials responsible for cyber security although our colleagues in the United States (U.S.) have established an EU-U.S. Working Group on Cyber Security. It would be useful to hear the Ambassador's sense of the political priority attached to Europe's Digital Agenda and the subsequent efforts to enhance cyber security.

Given his past experience as Canada's Chief Trade Negotiator and the ongoing efforts to negotiate a Canada-EU Free Trade Agreement, the Ambassador may have useful observations of how to handle jurisdictional challenges.

As a courtesy to the Ambassador, you may want to outline the objectives for your meetings in Brussels, which are:

- Obtain a greater understanding of how the EU advances cyber security while managing jurisdictional challenges presented by member states and national organizations responsible for cyber security. This may inform how Public Safety Canada can assess different approaches to engage stakeholders.

- Obtain an understanding of how the European Commission and the European Network and Information Security Agency (ENISA) work together and with the private sector as this may outline areas where Public Safety Canada could engage more efficiently with European states on incident management and response.

- Leave counterparts with a greater understanding of the accomplishments and challenges associated with the implementation of *Canada's Cyber Security Strategy*.

- Indicate Canada's support of promoting norms in cyberspace and of European efforts to undertake cyber security awareness month.

Canada will continue to promote norms in cyberspace and the EU is seen, [redacted] as an important partner in this effort given their stance on Internet and cyber security policy issues.

The National Security Operations Directorate has indicated (**TAB B**) that they would like to seek recommendations in order to set up meetings with officials in EU to discuss the security of the telecommunications sector. It would be useful to seek advice from the Ambassador as to which EU officials would be best placed to discuss the telecommunications policy. Critical Infrastructure Policy has provided background material regarding their international engagement with the EU, should the Ambassador indicate an interest (**TAB C**). National Security Operations has provided briefing material in the instance the Ambassador raises the *Criminal Code* listing of the Mujahedin-E-Khalq (**TAB D**).

TALKING POINTS ARE ON THE FOLLOWING PAGE

s.13(1)(a)

s.15(1) - Int'l

Meeting on January 18, 2012, with Mr. H. David Plunkett, Canada's Ambassador to the European Union

TALKING POINTS

- The Canadian government puts a high priority on cyber security, both domestically and internationally. What priority is afforded to cyber security at the political level in Europe?

- The Canadian government considers a digital economy strategy to be one of its most important objectives. The Government is reviewing Canada's telecommunications policies to create a more globally competitive telecommunications sector. I'd be interested to hear from your perspective, how European efforts to implement a Digital Agenda are faring.

- I understand that the EU and United States have established a bilateral cyber security working group. Would there be an appetite among European officials for such a similar Canada-EU bilateral cyber security working group?

- Canada has limited resources for international cyber security engagement and as such, should the EU approach us to formalize cooperation, Canada would have to target any potential engagement to ensure that it achieves outcomes under *Canada's Cyber Security Strategy*.

Objectives for National Security Operations Directorate

Our Investigative Technologies and Telecommunications Program would like to set up working level meetings with EU counterparts regarding the security of the telecommunications sector, do you have recommendations as to which officials in the EU deal with these particular issues?

Objectives for the meeting with Mr. Purser and Mr. Servida in Brussels

- As you know, I will be meeting with Mr. Stephen Purser, Head of the Technical Competency Department, European Commission and the European Network and Information Security Agency (ENISA), and Mr. Andrea Servida, Deputy Head of Unit, European Commission, Information Society and Media Directorate General. My objectives for that meeting are to:

  - Obtain a greater understanding of how the European Union advances cyber security while managing jurisdictional challenges presented by member states and national organizations responsible for cyber security. This may inform how Public Safety Canada can assess different approaches to engage stakeholders.

  - Obtain an understanding of how the European Commission and ENISA work together and with the private sector as this may outline areas where Public Safety Canada could engage more efficiently with European states on incident management and response.

  - Leave counterparts with a greater understanding of the accomplishments and challenges associated with the implementation of *Canada's Cyber Security Strategy*.

- Indicate Canada's support of promoting norms in cyberspace and of European efforts to undertake cyber security awareness month.

H. David Plunkett - Ambassador of Canada to the European Union

H. David Plunkett was nominated Ambassador of Canada to the European Union on July 22, 2011. He is married to Hettie Stevens, and they have a son, Jesse. Mr. Plunkett succeeds Ross Hornby.

Studies:

B.A. (political science), University of British Columbia, Canada, 1975
M.A. (international relations), University of Nijmegen, The Netherlands, 1979

Professional career:

2009 - 2011: Associate Assistant Deputy Minister and Chief Negotiator, Bilateral and Regional Trade Policy and Negotiations, Foreign Affairs and International Trade Canada.

2006 - 2009: Director General of Bilateral and Regional Trade Policy, Foreign Affairs and International Trade Canada.

2002 - 2006: Minister (Commercial and Economic), High Commission of Canada, London, United Kingdom.

1998 - 2002: Director of the European Union Division, Foreign Affairs and International Trade Canada.

1993 - 1997: Counsellor (Trade Policy), Embassy of Canada, Washington DC, United States of America.

1991 - 1993: Deputy Director of the U.S. Trade Policy Division, Foreign Affairs and International Trade Canada.

1987 - 1991: Counsellor, Permanent Mission of Canada to the General Agreement on Tariffs and Trade, Geneva, Switzerland

1981 - 1987: Trade Policy Officer, Department of External Affairs Canada

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

London International Cyber Conference

Table of Contents

Cover	Memorandum for the Canadian Delegation
Tab 1	Glossary of Common Cyber Security Terms International Organization Cheat Sheet
Tab 2	Conference Agenda / List of Participants
A	Economic Growth and Development
B	The Social Benefits of Cyberspace
C	Tackling Cyber Crime
D	Safe and Reliable Access
E	International Security
[redacted]	[redacted]
Tab 4	[redacted]
Tab 5	[redacted]

s.15(1) - Int'l

s.15(1) - Subv

SECRET

DATE:

File No.:

MEMORANDUM FOR THE CANADIAN DELEGATION

LONDON INTERNATIONAL CYBER CONFERENCE
OCTOBER 31 – NOVEMBER 3, 2011

(Information only)

ISSUE

This note provides a briefing on the London International Cyber Conference on November 1-2, 2011 i

An unclassified and abridged version of this briefing material for ease of transportation during the conference proceedings,

BACKGROUND

Just as the appropriate role of the state in the economic, social, cultural, and security policy has been contested throughout history, this debate is playing out in cyberspace. States have differing views on notions of sovereignty, the role of state intervention in the economy, the rule of law, and the appropriate limits on individual freedoms to name a few.

As cyberspace plays an increasingly larger role in personal and commercial activity, it is challenging traditional conceptions of the role of state, both domestically and internationally. The traditional social contract between states and their citizens is slowly being challenged, and in some cases creating some significant frictions. Internationally, states are grappling with how the existing international law norms of behaviour that have governed state interactions offline apply online. This fundamental reassessment of how cyberspace fits into pre-existing constructs is causing anxiety and uncertainty among states and businesses who are unsure of how best to operate in this new environment.

s.15(1) - Int'l

s.15(1) - Subv

s.13(1)(a)

While the motivations for advocating the need for internationally-binding instruments vary, their impact is likely to have a detrimental impact on the benefits that cyberspace has brought to date. Greater state control over cyberspace may stem the free flow of goods and services online, make it easier for states to monitor individuals' activities online, pose a risk to global interoperability, and threaten national security. Furthermore, it is premature to discuss binding instruments for cyberspace given the lack of a common understanding how cyberspace fits into existing conceptions of the role of the state.

As expectations of proper behaviour, cyber norms would create societal pressures to guide online activity without creating binding obligations. Unlike treaties, which only bind states, norms would be applicable to all cyberspace stakeholders.

The London International Cyber Conference will formally launch the cyber norms discussion,

CONFERENCE PARTICIPATION

CONFERENCE PROCEEDINGS

On the morning of November 1, The Rt. Hon. William Hague, U.K. Foreign Secretary, will make a speech opening the Conference and outline the case for cyber norms.

Following the speeches, Mr. Hague will chair a panel where participants will broadly address some of cyberspace's implications for the global economy, human rights, and education.

For the remainder of the first day and for the entirety of the second day, delegations will attend a series of panel discussions, each of which will address one of the five key themes of the Conference:

1. Economic growth and development;
2. Social benefits;
3. Cybercrime;
4. Safe and reliable access; and
5. International security.

Each of these panels will moderated by a U.K. Cabinet Minister, and there will be an opportunity for the audience to engage the panellists.

Public Safety Canada, in collaboration with the Department of Foreign Affairs and International Trade, Industry Canada, the Department of Justice, and Canadian Heritage, has drafted a series of background notes for each of the panels (**TABS A to E**).

Topics on several of the panels may overlap. As such, some information in the briefs appear in more than one note.

s.13(1)(a)

s.15(1) - Int'l

s.15(1) - Subv

At the end of the Conference, the U.K. will release a "Chair's Summary" which will summarise the discussions

CONSIDERATIONS

The London Conference comes at a time where countries and international organisations are increasingly jockeying to promote their interests in the multitude of international venues where discussions on the future of cyberspace are taking place.

At the United Nations (U.N.) General Assembly, the PRC and the Russian Federation, supported by Tajikistan and Uzbekistan, have introduced a draft and non-binding "International Code of Conduct for Information Security" **(TAB 4)**.

Also at the U.N. General Assembly, Brazil, India and South Africa are looking to promote a proposal for a new U.N. body to "coordinate and evolve coherent and integrated global public policies pertaining to the Internet." This was a key outcome of last month's meeting of the Internet Governance Forum in Kenya.

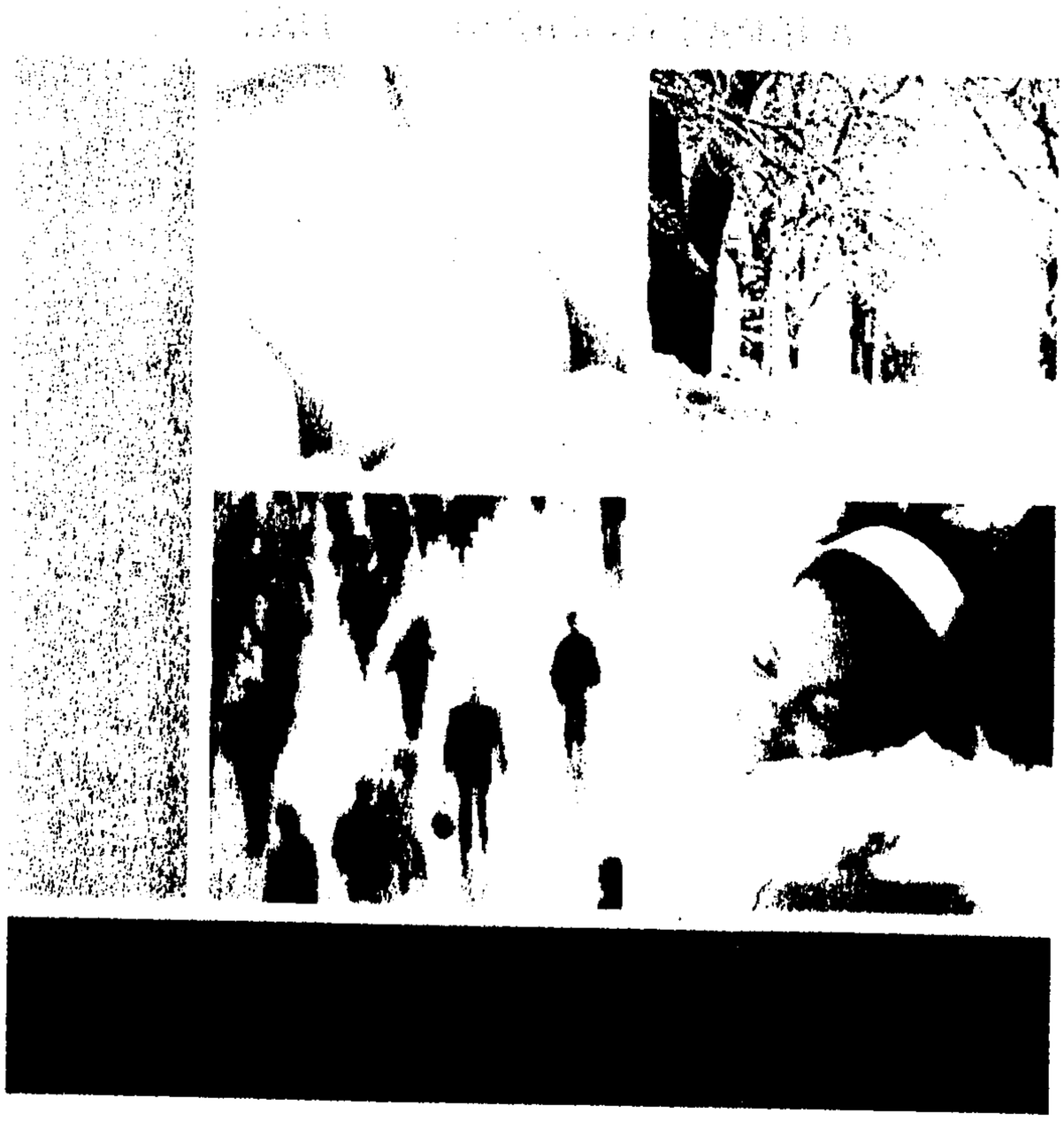
s.15(1) - Int'l

s.15(1) - Subv

Canada needs to remain proactive in these discussions to ensure that any emerging cyber norms or governance structures reflect Canadian interests and values.

Much of what follows the Conference will be determined by the tone set by its discussions.

Prepared by : Alexandre Grigsby



NATIONAL CYBER SECURITY DIRECTORATE
GLOSSARY OF COMMON CYBER SECURITY TERMS

JUNE 17 2011
RDIMS #438312
Version 1.1

Canada

Computer Network Defence (CND) – actions taken through the use of computer networks to protect monitor, analyze, detect and respond to unauthorized activity within a department or organization's information systems and computer networks. [2]

Computer Network Exploitation (CNE) – enabling operations and intelligence collection acapabilit8ies conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. [2]

Computer Network Operations (CNO)– comprise computer network attack, computer network defence and related computer network exploitation enabling operations. [2]

Computer Security Incident Response Team (CSIRT) – See CERT.

Command and Control (CNC) Server – a system (often also compromised) which is used to control all of the infected computers in a distributed botnet.

Cryptography – the discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [1] The conversion of the information into this new protected form is referred to as encryption. The conversion of information back to its original form is decryption.

D

Decryption – decoding of a message which has been encrypted (see cryptography)

Denial of Service (DoS) Attack – a type of cyber attack aimed at overwhelming or otherwise disrupting the ability of the target system to receive information and interact with any other system.

Deep Packet Inspection – the detailed analysis of a data packet in order to determine if the contents of the packet contain malicious or otherwise unwanted data.

Distributed Denial of Service (DDOS) Attack – a denial of service attack which utilizes a series of computer systems which are in the form of a distributed network. In a DDOS attack, more than one system is attacking the target. Often DDOS attacks utilize botnets.

Digital Forensics - generally considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. [1]

E

Encryption – converting information from one form to another to hide its content (see cryptography)

Exploit - is a defined way to breach the security of an IT system through a vulnerability. [1]

J

K

Keystroke Logger – software or hardware designed to capture a users keystrokes on a compromised system. The keystrokes are stored or transmitted so that they maybe used to collect valued information.

L

M

Malware - malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

Metadata - data that describes the structure and workings of an organizations use of information, and the systems it uses to manage that data.

N

Network Administration - day to day operation and management of network processes and users.

O

P

Packet - a formatted block of information carried by a computer network. When data is formatted into a packet, the network can transmit longer messages more efficiently and reliably than unformatted bytes.

Patch - a small piece of software designed to update or fix problems with a computer program. This includes fixing bugs, reducing vulnerabilities, replacing graphics and improving the usability or performance.

Peer to Peer (P2P) Network - relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating power in a low number of servers. These networks are often used for sharing content files containing audio and video data.

Phishing - an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

they can have undesirable effects. Once installed, spyware tracks the infected computer's activity and reports it to others, such as advertisers. Spyware also consumes memory and processing capacity, which may slow or crash the infected computer.[1]

T

Trojan - a malicious program that is disguised as or embedded within legitimate software. The term is derived from the gift the ancient Greeks presented to the citizens of Troy during the Trojan War, as a ruse to infiltrate and sack the city.[2]

U

V

Virtual Private Network (VPN) - a private communications network usually used within a company, or by several different companies or organisations to communicate over a wider network. VPN message traffic can be carried over a public networking infrastructure (i.e. the Internet) on top of standard protocols, or over a service provider's network with a defined Service Level Agreement between the VPN customer and the VPN service provider. VPN communications are typically encrypted or encoded using SSL to protect the traffic from other users on the public network carrying the VPN.[2]

Virus - a computer program that can spread by making copies of itself. Computer viruses spread from one computer to another, by making copies of themselves, usually without the knowledge of the user. Viruses can have harmful effects, ranging from displaying irritating messages to stealing data or giving other users control over the infected computer. A virus program has to run before it can infect a computer, generally doing so by attaching itself to other programs or hide in code that is executed automatically when a user opens certain types of files.[1]

Vulnerability - a flaw or weakness in the design or implementation of an information system or its environment that could be intentionally or unintentionally exploited to adversely effect an organization's assets or operations.[2]

W

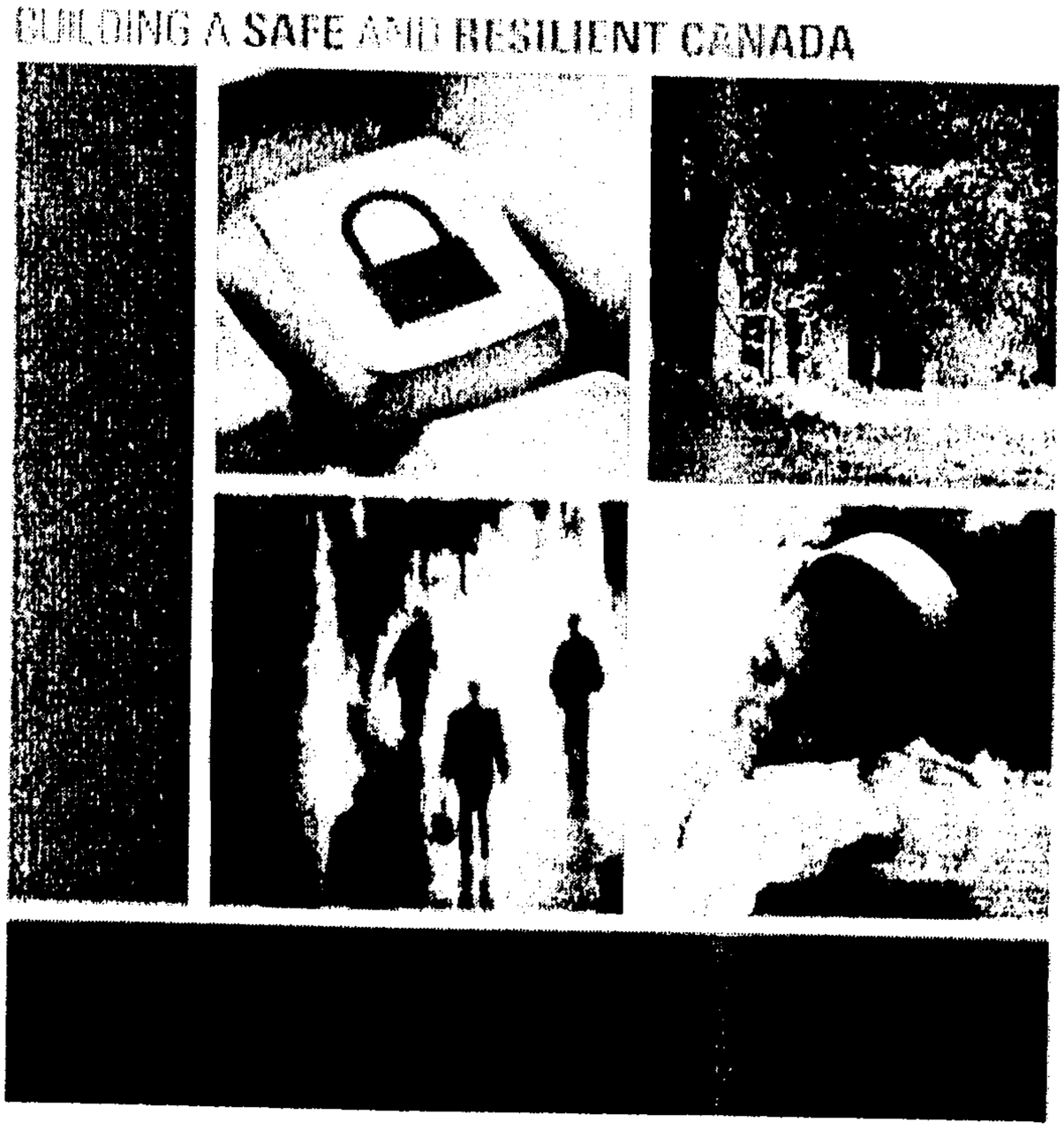
Worm - a self-replicating computer program. It uses a network to send copies of itself to other systems and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.[1]

X

Y

Z

Public Safety Canada | Sécurité publique Canada



NATIONAL CYBER SECURITY DIRECTORATE
LISTING OF INTERNATIONAL ORGANIZATIONS DEALING WITH CYBER SECURITY

OCTOBER 12 2011
RDIMS #500298
Version 1

Canada

National Cyber Security Directorate
Listing of International Organizations Dealing with Cyber Security

A

Asia Pacific Economic Cooperation (APEC) - APEC is the premier Asia-Pacific economic forum. Its primary goal is to support sustainable economic growth and prosperity in the Asia-Pacific region. APEC strives to develop a dynamic and harmonious Asia-Pacific community by championing free and open trade and investment, promote and accelerate regional economic integration, encourage economic and technical cooperation, enhance human security, and facilitate a favourable and sustainable business environment.

Asia Pacific Economic Cooperation Electronic Commerce Steering Group (APEC-ECSG) - The APEC-ECSG promotes the development and use of electronic commerce by creating legal, regulatory and policy environments in the APEC region that are predictable, transparent and consistent. It performs a coordinating role for APEC e-commerce activities, based on the principles set out in the 1998 APEC Blueprint for Action on Electronic Commerce.

Asia Pacific Economic Cooperation Telecommunication and Information Working Group (APEC-TEL) - The APEC-TEL aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing and implementing appropriate telecommunications and information policies, including relevant human resource and development cooperation strategies. This is reflected in APEC-TEL's expanded vision of promoting the transition from an Asia-Pacific Information Infrastructure into the Asia-Pacific Information Society.

Asia Pacific Economic Cooperation Counter Terrorism Task Force (APEC-CTTF) - APEC Leaders have pledged to help secure the region's people and it's economic, trade, investment and financial systems from terrorist attack or abuse and trade-based money laundering. Their commitments to undertake individual and joint actions to counter terrorism are expressed in two principle statements - the 2001 APEC Leaders Statement on Counter-Terrorism and the 2002 Statement on Fighting Terrorism and Promoting Growth - and in every subsequent annual Leaders' Declaration.

Association of South East Asian Nations (ASEAN) – ASEAN is a political and economic organization of 10 South East Asian states (Brunei, Burma, Cambodia, Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand, and Vietnam). The group's mandate is to promote economic growth as well as political and security stability in the region. On cyber security, member states work together to share information on emerging trends and issues and provide assistance on a case by case basis.

Association of South East Asian Nations Regional Forum (ARF) – ARF is an informal dialogue of 27 member states that seeks to address security issues in the Pacific region. Members of ARF include Australia, Canada, the European Union, India, New Zealand, Russia and the United States.

B

C

Council of Europe - The Council of Europe (not be confused with the EU) is a regional organization comprising of 47 member states including all EU member states, Russia and former Soviet republics. There are also 5 observer states: Canada, Japan, Mexico, the United States and the Vatican. The Council's primary contribution to cyber security policy development is its drafting of the 2001 Budapest Convention on Cybercrime, which facilitates international cooperation in prosecuting cybercrime offences such as streamlining information sharing and harmonizing domestic criminal law dealing with criminal offences on the Internet.

D

E

F

G

Group of Eight (G8) – The G8 is a grouping of seven of the world's most advanced economies (Canada, U.S., Italy, France, Japan, U.K., and Germany) and Russia. Each year, the country holding the G8 presidency convenes a series of meetings at the Heads of Government, Ministerial and officials levels to discuss topics as diverse as international peace and security, the global economy, international development, and Internet issues.

Group of Eight Roma-Lyon High Tech Crime Sub Group (HTCSG) - At the working level, there are five subgroups called the Roma-Lyon groups. These groups study and analyze issues relevant to their policy area as decided by the country holding the rotating presidency. The High Tech Crime Sub Group (HTCSG) studies issues related to cyber crime, terrorist use of the Internet, and critical infrastructure protection. The HTCSG proposes best practices to guide G8 members' policy and operational responses to these challenges.

Group of Eight Counter Terrorism Practitioner Sub Group (CTPSG) - The Counter Terrorism Practitioner Sub Group brings together counter terrorism practitioners from the G8 countries to discuss emerging trends in terrorist activity and propose common policy and operational solutions to G8 leaders in response.

H

I

International Telecommunications Union (ITU) - The ITU is the specialized agency of the United Nations which is responsible for technologies. The ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, and works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. The ITU and UNODC signed a Memorandum of Understanding in May 2011 to cooperate on cyber security.

International Telecommunications Union Development (ITU-D) - ITU-D is the ITU's capacity building branch. It assists developing countries implement international communications standards and other policies developed by the ITU. It provides both technical and policy support to developing countries with the aim of narrowing the digital divide (i.e. the communications and infrastructure gap between developed and developing countries). In the area of cyber security, the ITU-D provides assistance to developing countries to secure their networks and infrastructure.

International Telecommunications Union Global Cybersecurity Agenda (ITU-GCA) - The ITU-GCA promotes legal, technical, and policy mechanisms to aid states in deploying solutions to counter threats and vulnerabilities to their networks. The GCA has fostered such programmes such as the Child Online Protection initiative, which helps identify the risks and vulnerabilities of children in cyberspace.

International Telecommunications Union – Telecommunications Standardization (ITU-T) – ITU-T holds annual events that bring together a variety of stakeholders working in the information and communication technology sector on standardization. It offers the information and communication technology community a global platform to discuss and collaborate on emerging issues.

Internet Engineering Task Force (IETF) – IETF is the group responsible for proposing and developing technical Internet standards.

Internet Governance Forum (IGF) – Originating from the World Summit on the Information Society, the IGF is a forum which brings states, NGOs and other stakeholders to discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet. The group identifies emerging Internet governance issues, brings them to the attention of stakeholders and can make non-binding recommendations to improve and streamline Internet governance. Annual meetings have been held since its establishment in 2006.

Internet Corporation for Assigned Names and Numbers (ICANN) – ICANN is a non-profit organization dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

J

K

L

M

Meridian Process - The Meridian Process aims to provide governments worldwide with a venue to facilitate cooperation at the policy level on critical information infrastructure protection (CIIP). An annual conference and interim activities are held each year to help build trust and establish international relations within the membership to facilitate sharing of experiences and good practices on CIIP from around the world.

N

North Atlantic Treaty Organization (NATO) - NATO is a military alliance of 28 member countries. At the 2010 Lisbon summit, member states directed the Alliance to develop a common policy on cyber defence along with an implementing action plan to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimize information sharing, collaboration and interoperability.

O

Organization for Security and Cooperation in Europe (OSCE) - The OSCE is a security organization comprising of 56 states (most of Europe, former Soviet Republics, Russia, Canada, the United States) which strives to maintain peace and security in Europe with its primary focus on states in the Caucasus and Central Asia. Since 2005, OSCE activity has focused primarily on individual aspects of enhancing cyber security such as combating cyber-crime and the use of the Internet for terrorist purposes. In May 2011, Austria hosted a conference which examined current trends, the emergence of norms regulating responsible state behaviour on the Internet, and the future role of the OSCE on cyber security issues.

Organization of American States (OAS) - The OAS is a 34-member regional organization which brings together all of the independent states in the Americas. Its goal is to provide member states with "an order of peace and justice, to promote their solidarity, to strengthen their collaboration, and to defend their sovereignty, their territorial integrity, and their independence." On cyber security issues, the organization aims to promote information sharing among member states on threats, vulnerabilities, and counter-measures, largely through its Comprehensive Inter-American Strategy to Combat Threats to Cyber Security.

OAS – Inter-American Committee Against Terrorism (OAS-CICTE) - CICTE (the Spanish acronym for Inter-American Committee Against Terrorism) addresses cyber security by promoting technical assistance among member states to develop 24/7 alert, watch, and warning teams, known as Computer Security Incident Response Teams, as well as promoting member state compliance with the OAS's cyber security strategy.

OAS - Inter-American Telecommunications Commission (OAS-CITEL) - CITEL focuses on promoting the development of information and communications technologies in the Americas. It serves as a permanent forum that brings together government and the private sector for coordinating the member states' diverse political, economic, social and technical perspectives required to assist in meeting their specific infrastructure needs. CITEL's evaluations include relevant legal, regulatory and technology-related issues such as universal access to information and communications technologies, common standards, network interoperability, and compatible use of the radio spectrum.

OAS – Ministers of Justice or Attorneys General of the Americas (OAS-REMJA) - The REMJA process (an annual meeting of Ministers of Justice and Attorneys General of the Americas) is the premier policy and technical forum at the hemispheric level on matters related to the strengthening of and access to justice, and international legal cooperation in areas related to mutual legal assistance in criminal matters; extradition; penitentiary and prison policies; cybercrime and forensic sciences, among others.

Organization of Economic and Cooperation Development (OECD) - The OECD is a 34-member organization which encompasses the world's more advanced economies. It is essentially a large think tank which proposes guidelines and best practices on a variety of issues, such as international development assistance, economic competitiveness, governance, education, and the Internet.

OECD – Committee on Information and Communications Policy (ICCP) - The ICCP studies the regulation and economics of telecommunications, including the Internet, broadband and mobile as well as convergence of the broadcasting and cable sectors with more conventional telecommunications. Through its study of these "digital economy" issues, the ICCP provides insights to member and non-member states as to how telecommunications policy impacts economic and social development.

OECD – Working Party on Information Security and Privacy (WPISP) - The WPISP promotes an internationally coordinated approach to policymaking in security and protection of privacy and personal data in order to build trust among networked societies and facilitate electronic commerce. Specifically it provides policy advice in the following areas: critical information infrastructure, digital identity management and e-authentication, malware, Radio-Frequency Identification, sensor networks, the OECD Privacy Guidelines, protecting children online, and privacy law enforcement co-operation.

P

Q

R

S

T

U

United Nations General Assembly (UNGA) - The General Assembly at the UN only addresses cyber security issues when raised by a member state. There are six specialized committees that report to the UNGA. These committees generally debate tests of resolutions and initiatives before they can be presented to the General Assembly for decision. The UNGA has begun adopting an annual resolution on cyber security. The latest Resolution 65/41 passed without a vote in January 2011.

UN Disarmament and International Security Committee (First Committee) - The First Committee considers disarmament and security issues, including cyber security, that are brought forward by member states.

UN Economic and Financial Committee (Second Committee) - The Second Committee considers economic and financial issues, including cyber security, that are brought forward by member states.

UN Office on Drugs and Crime (UNODC) - The UNODC is a specialized UN Agency which is mandated to assist UN member states combat illicit drugs, crime and terrorism. It researches and analyses drug and crime issues to expand the evidence base and provide guidance on policy and operational decisions. It also provides technical expertise to member states which require such assistance. The UNODC is increasingly working on cybercrime issues, including holding technical seminars on emerging issues and to promote best practices.

V

W

World Summit on the Information Society (WSIS) - The WSIS was a series of two meetings in 2003 and 2005 whose chief aims were to bridge the digital divide and to clarify the key governance mechanisms that sustain the Internet. At the conclusion of the second meeting in Tunis, Tunisia in 2005, participating states issued two outcome documents known as the Tunis Commitment and Tunis Agenda for an Information Society which provide overarching principles for Internet governance, such as keeping the Internet open, as well as establishing the Internet Governance Forum. Since 2005, there have been annual WSIS Forum meetings where participating stakeholders exchange ideas on the future of the Internet and other emerging issues. WSIS continues to function as a secretarial body and there seems to be no desire to shut this down. WSIS actively includes a large number of civil society organizations which see cyber security as an impediment to their objectives.

[redacted]

[redacted]

[redacted]

Page 575

is withheld pursuant to section

est retenue en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

DRAFT PROGRAMME – Please follow @LondonCyber for updates

Queen Elizabeth II Conference Centre

The rapid development of a globally networked world offers enormous social and economic opportunities. In a series of panel discussion, thematic debates and a programme mixing live and virtual activities, this innovative conference aims to:

- launch a more focussed and inclusive dialogue between key cyberspace actors from across the world including government, industry and civil society
- develop a better understanding of how to protect and preserve the tremendous opportunities provided by the development of cyberspace.
- generate ideas and proposals for the 'London Agenda'

Monday 31 October

1930-2130 Welcome reception for all participants at The Science Museum

Tuesday 1 November

0800–0900 Registration at the Queen Elizabeth II Conference Centre

0930-1100 **LAUNCH OF 'ACTIVE ENGAGEMENT'.**

Cyberspace: live, inter-active and virtual sessions. Meet international business, NGOs and other active users in a programme of activities to be streamed alongside the conference.

1115-1145 **Session 1: WELCOME ADDRESS**

Opening remarks by the Foreign Secretary, William Hague accompanied by leaders of international business, civil society and government.

THE LONDON CONFERENCE ON CYBERSPACE
1 - 2 NOVEMBER 2011

1145-1300 Session 2: CYBERSPACE AND THE NETWORKED WORLD: THE VISION

Looking to 2030: What are the future trends in technology and communication techniques? How will this impact on the global community? What are the implications for democratic accountability and freedom? How will developments in cyberspace impact on prosperity, development and knowledge?

Chair: William Hague, Foreign Secretary

Keynote remarks from leaders of international business, civil society and government.

Followed by inter-active panel discussion with questions from the floor and the virtual community via social media.

1300-1400 Networking lunch including opportunities for engagement with the Blogosphere

1400-1530 Session 3: HOPES AND FEARS

Short, punchy and broad ranging perspectives from keynote speakers in an audience-focussed debate on the key cyberspace issues.

1530 - 1600 Break

1600-1835 Session 4: OPPORTUNITIES AND CHALLENGES (1)

Thematic parallel debates on 5 key issues of cyberspace

'Cyber-speed-dating' format with brief introductory pitches from leading figures followed by 15-20 minute participatory discussion.

I. Economic Growth and Development
How to realise the benefits of a secure cyberspace for international economic growth and development? Is Cyberspace a prosperity multiplier? How to strike a balance between protection of intellectual property and access, innovation and creation of markets? How to ensure transparency and predictability of regulatory and fiscal regimes, and their ability to adapt to fast-changing technologies? Government regulation and industry self-regulation – what are the ways forward?

II. Social Benefits
What are the major social benefits and how to capture this potential? How best to maximise knowledge empowerment and management? What are the potential gains for Government service delivery, democratic accountability, freedom of expression? How should governments engage to best effect? Where does responsibility, and for what, lie? How to ensure citizens are protected? What about the negative social aspects and what are the risks of unintended consequences?

s.15(1) - Int'l

s.15(1) - Subv

THE LONDON CONFERENCE ON CYBERSPACE
1 - 2 NOVEMBER 2011

III. International Security (by invitation only)
How can problems between states be prevented and managed? What *mechanisms could prevent or mitigate problems between states on cyber security* issues? What lessons can be learned from other areas of international security and conflict prevention work? How to develop and apply appropriate principles of behaviour? What are the most appropriate fora to take the debate forward?

1900-2100 Evening networking reception (tbc)

Wednesday 2 November

0900-0940 **Session 5: SEIZING THE CYBER-SPACE**

Emerging issues and mid- way reflections on conference learning to include feedback from thematic debates

0940-1000 **Session 6: THE DAY AHEAD: SCENE SETTER**

1000-1105 **Session 7: OPPORTUNITIES AND CHALLENGES (2)**

Thematic parallel debates on 5 key issues of cyberspace

'Cyber-speed-dating' format with brief introductory pitches from leading figures followed by 15-20 minute participatory discussion.

IV. Cyber Crime
How to realise the benefits of a secure cyberspace for international economic growth and development? What are the threats and opportunities for financial crime, legislation, child safety and investigation measures? How to strike a balance between protection of intellectual property and access, innovation and creation of markets? How should government regulation and industry self-regulation work together to best effect? How to ensure transparency and predictability of regulatory and fiscal regimes, and their ability to adapt to fast-changing technologies?

V. Safe and Reliable Access
How to assure safe and reliable access to cyberspace? How to ensure that global interoperability and resilience, protocols and technical standards and the security of networks and users are at the forefront? How best to promote public risk-awareness and education in secure online behaviour (particularly for vulnerable groups such as children)? How to ensure lawful access for individuals without discrimination or interference, while protecting against abuse? What is *the correct balance between regulation and self-regulation? Network* connectivity; the challenge of integrating SMS and web based systems.

1105-1135 Break

THE LONDON CONFERENCE ON CYBERSPACE
1 - 2 NOVEMBER 2011

1135-1315 Session 8: FINDING WAYS FORWARD

Thematic Debates- *further exploration of the issues raised in previous session.*

VI. Cyber Crime

In what ways can jurisdiction of online activities be improved? What would this mean for policing? What resources are needed to increase protection against cyber crime? How to reduce risk? What more can publics do to 'stay safe' and what information should governments provide?

VII. Safe and Reliable Access

Is there a need for further online privacy and data protection and how could this be implemented? How to support capacity building of individuals and states to increase resilience and reduce vulnerability? What further investments are needed in infra-structure?

1315-1430 Networking lunch

1430-1510 Session 9

Feedback from Thematic Debates including a round up of the online conversations that have taken place around the conference.

1445-1530 Session 10: AGREEING A WAY AHEAD

Summing up: Foreign Secretary's Statement and reflections and conclusions from senior representatives.

1530 Conference close

CONFIDENTIAL

BRIEFING NOTE

ECONOMIC GROWTH AND DEVELOPMENT

s.13(1)(a)

KEY ISSUES

[redacted]

- The free flow of goods and services; and
- Intellectual property protections.

Additionally, based on an analysis of the expected participants and the nature of the Conference, it is expected that these issues may also arise:

- Access to cyberspace;
- International capacity building assistance;
- Taxation of goods and services online; and
- Network neutrality.

Issue briefs on each topic, describing its strategic context, the Canadian position, and considerations for discussion, accompany this note.

There is likely to be a significant overlap in subject matter between this panel and the panels on Social Benefits and Safe and Reliable Access. Accordingly, much of the same material appears in the briefs.

THE FREE FLOW OF GOODS AND SERVICES ONLINE

Strategic Context

The free flow of goods and services online is fundamental for promoting economic prosperity and growth. As global trade increasingly moves to cyberspace, highly industrialised countries are implementing broadband or digital economy strategies to strategically position their respective countries to fully benefit from this space. In order to harness the benefits of the digital economy, it is important that governments provide an efficient and flexible policy framework that facilitates the conduct of e-transactions and online businesses that relies on a foundation of trust, transparency, and the free flow of goods and services.

In many countries, however, the state exercises considerable control over the economy, favouring certain industries and companies over others and distorting market forces. This control can extend to cyberspace, limiting the far ranging benefits of e-commerce. They view interventionist state involvement as an extension of their sovereign right to govern over their territory, irrespective of the economic consequences.

While this may have some short-term benefits, other factors being equal, history has shown that state micromanagement of the economy and protectionist trade barriers stifle long-term growth and may lead to economic hardship. There is little evidence to suggest that state control over the digital economy and commerce would engender different results.

Canadian position

As a strong trading nation, Canada's economic prosperity relies on its capacity to trade goods and services in a free and unhindered fashion. As the importance of digital marketplace increases, Canada is taking steps to ensure that cyberspace remains an open, innovative and competitive environment. For example, new telecommunications providers have entered the Canadian market [redacted]

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

Canada is taking these steps to foster competition and innovation in the digital economy. As a liberal economy, Canada's economy is best served when government is minimally involved and that excessive intrusion is detrimental to prosperity and growth. While there are some instances where the government regulates certain industries and economic sectors, this is largely done to prevent monopolies, to protect consumers, to correct negative externalities (i.e. blunt the social cost of certain transactions despite their economic benefit), or to promote domestic cultural objectives.

The liberal nature of Canada's economy is reflected in its extensive trade activities, including goods and services delivered electronically, with partners through free trade agreements (FTAs) and at the World Trade Organization. The principles and obligations within those FTAs do not distinguish between the means of delivery and therefore would apply equally to trade conducted online.

Page 582

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

INTELLECTUAL PROPERTY PROTECTIONS

Strategic Context

Intellectual property, defined as the combination of copyrights, trade-marks and patents, could be one of the most contentious issues discussed at the Conference. Certain have reputations as "havens" for services that facilitate or enable the distribution of protected works online (e.g. music, movies, and television shows), resulting in possible lost revenue for Canadian companies and economic harm. Such practices contravene a number of international agreements such as the World Trade Organisation's (WTO) Trade-Related Aspects of Intellectual Property (TRIPS) Agreement. The TRIPS Agreement establishes minimum levels of reciprocal intellectual property protection to the WTO's 153 members. These "haven" countries face international pressure to strengthen their laws to curb such activities.

In an attempt to crack down on routine violators, some states have begun adopting "graduated response" schemes to protect intellectual property in cyberspace. Under such a mechanism, also known as "three strikes," Internet users who repeatedly download intellectually protected content can face a temporary disconnection from the Internet. France, the Republic of Korea, and the United Kingdom have implemented "graduated response" schemes. This approach to intellectual property enforcement is controversial, with some international organisations (the United Nations and the Organisation for Security and Cooperation in Europe) believing it to be a disproportionate response. The U.S. has also begun seizing the domain names of websites that infringe intellectual property, but face the challenge of these sites simply reappearing abroad.

A key emerging issue is the role (if not the onus) which falls on Internet Service providers to report or enforce IP protection on behalf of the property owners. Such a policy is a hallmark of the recent legislation tabled in the U.S. Senate, the *IP PROTECT Act of 2011*.

Economic espionage, defined as state or state-affiliated entities gaining access to protected intellectual property for economic gain and not to be confused with commercial espionage where companies spy on each other, also plays a role in the online intellectual property debate. Given the sensitivity of this, states and businesses always avoid disclosing the specifics of what particular technologies were stolen and the methods used to access them.

Canadian position

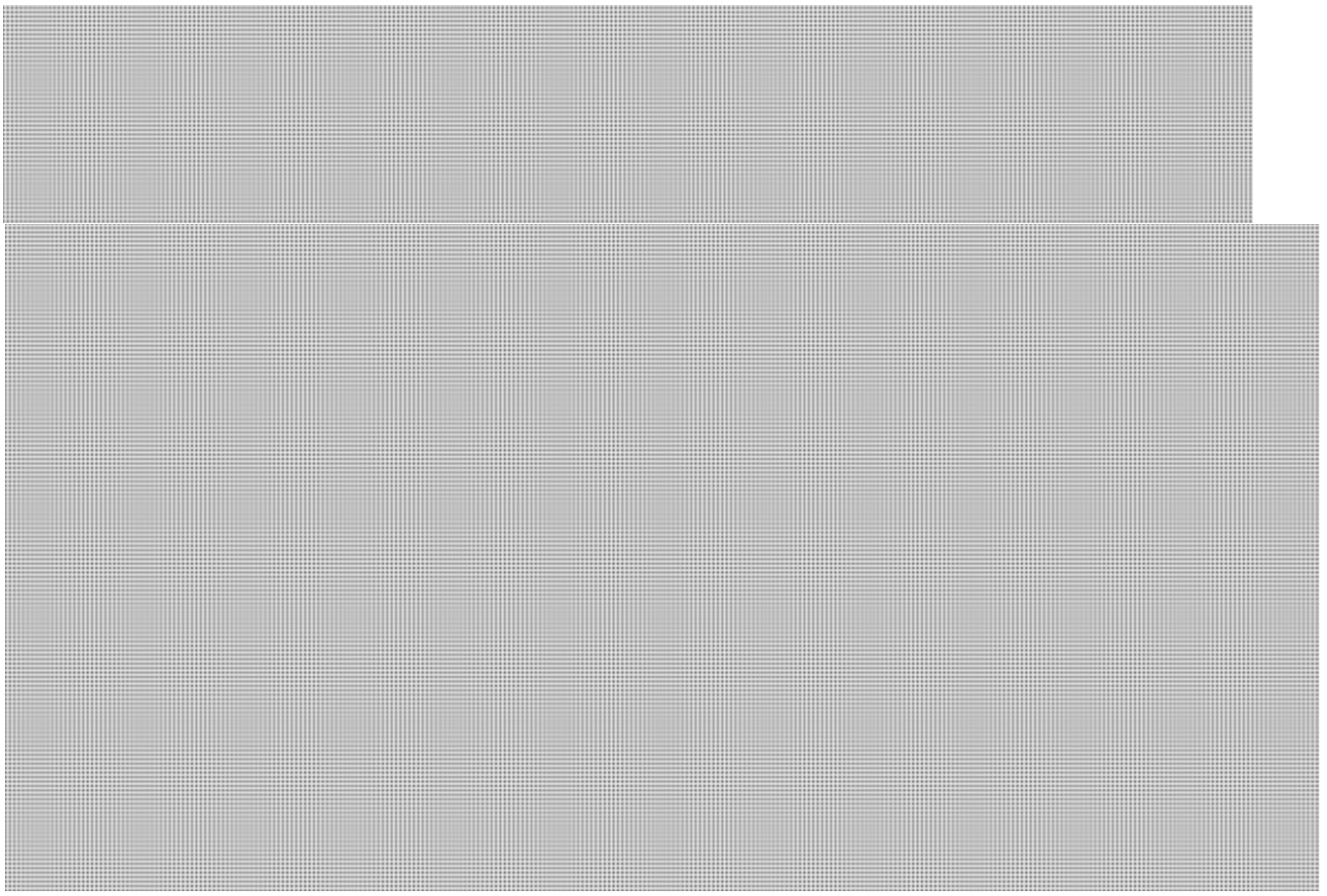
As a knowledge-based economy, intellectual property protections are increasingly important to Canada's economic prosperity; when fairly balanced, they help foster innovation, creativity, and economic growth both online and offline. Recognizing the growing importance of cyberspace for the flow of goods and services, states, businesses and individuals should uphold and respect their intellectual property laws in the online environment.

s.15(1) - Int'l

s.15(1) - Subv

To better protect intellectual property in Canada, the Government is working to modernize its intellectual property regime to bring it in line with advances in technology and international standards. On September 29, 2011, the Government introduced Bill C-11 (*Copyright Modernization Act*) which aims to modernize Canada's copyright laws in a manner that would balance the interests of creators and users in the digital age. For example, the Bill includes provisions to expand the exemptions to use protected works for non-commercial purposes while increasing penalties for those who illegally use or distribute them. The Bill also seeks to implement the World Intellectual Property Organization (WIPO) Internet Treaties, an international consensus on the standard of copyright protection needed to respond to the challenges and opportunities of the Internet and other digital technologies, which Canada signed in 1997. The WIPO Internet Treaties are in force in a number of countries, including Australia, France, the Republic of Korea, the United Kingdom, and the United States.

Internationally, Canada recently signed the Anti-Counterfeiting Trade Agreement (ACTA). The agreement seeks to implement standards of enforcement for intellectual property rights to more efficiently address the challenge of counterfeiting and piracy. ACTA identifies the role that online services providers can play, subject to due process, in the enforcement of intellectual property rights on the Internet. While ACTA largely reflects WIPO's intellectual property consensus, some civil society groups argue that a portion of ACTA's enforcement provisions are too heavy handed.



Page 585

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1) - Int'l

s.15(1) - Subv

CONFIDENTIAL

ACCESS TO CYBERSPACE

Strategic Context

Access to cyberspace confers a number of economic benefits, ranging from more efficient communications to accessing new markets. Most countries already actively champion cyberspace access, either through legislation, policy, or by setting the example of providing government services online. Additionally, a number of internationally agreed-upon documents already highlight the need for states to promote access to cyberspace, not only for economic reasons but also for social and cultural reasons. These documents include the *2005 Tunis Agenda for the Information Society* and the *2011 OECD Communiqué on Internet Policy-Making*.

States with greater control over their economy may not wish to promote online access for economic purposes as it could undermine preferred state-owned enterprises or monopolies. However, the large majority of states present at the Conference recognise the wider economic value of Internet access, and it is unlikely that this issue will become a point of contention.

What may become controversial, however, is whether access to cyberspace should be considered a human right. While this topic is slated to be addressed elsewhere during the Conference, the human rights dimension of cyberspace is likely to arise in economic discussions as rights advocates may argue that making access a right could lead to greater economic benefits, especially for those in the developing world.

Canadian position

Canada recognises the collective benefit of online access in terms of its general social, educational, and economic potential. To promote some of the enormous economic benefits and opportunities that can be derived from cyberspace, greater access to cyberspace should be encouraged.

As private companies deliver access to cyberspace in Canada, the primary role of the federal government is to ensure that the market for the delivery of online services is competitive. Recognizing its societal benefits, however, the federal government promotes access to cyberspace largely through subsidies and partnerships with provinces, businesses and community organisations.

Internationally, Canada promotes the adoption of information and communication technologies (ICTs) and access to cyberspace through Canadian International Development Agency funding and in multilateral venues such as the International Telecommunication Union. These efforts assist developing countries in developing the policies and infrastructures.

[redacted]

Issues to consider

- *Private ownership*: Most of Canada's cyber infrastructure is owned and operated by private companies or are outside the federal government's jurisdiction. Given this, the Government of Canada plays a limited role in directly providing cyberspace access to citizens and businesses.

[redacted]

PRIVACY IN CYBERSPACE

Strategic context

Advances in computing have made it easier and affordable for individuals to exchange information and for businesses to store data, creating a host of benefits for society. However, networked systems are inherently vulnerable and data breaches can cause significant harm, ranging from violations of individuals' personal security to severely damaging a country's economy.

A number of jurisdictions have struggled with applying traditional notions of privacy into a digital world. Privacy has long been recognized by liberal democratic governments as a requirement for active participation online. Accordingly, privacy Commissioners in the Western world are constantly raising awareness of the privacy implications of new technologies; in some cases they have been driving policy change by affecting legal changes to strengthen privacy. The OECD is currently reviewing its Data Protection Guidelines, the European Union has been reviewing its EU Data Protection Directive, and the United States has issued a Green Paper on privacy in 2010, a final response to which is expected soon.

The need to have privacy follow an individual as their data migrates through cyberspace, an issue known as "accountable transborder data flow", is emerging as a key international issue. Without these consistent rules, barriers to the free flow of information across international borders are likely to arise.

There are several factors competing against strong privacy. First, corporations will only meet such standards as they are required to, which is often in a different legal jurisdiction than the individual accessing those services. In some other jurisdictions, companies are required to disclose when personal information has been put at risk in order to empower individuals to take action and protect themselves; in other areas such programs do not exist. Secondly, there is a need for governments and cyber infrastructure operators to monitor data traffic to ensure the health and security of the network. Some segments of civil society are sceptical of greater government intrusion into citizens' lives argue that traffic monitoring is likely to be abused, and opens the door to violations of individuals' right to be protected from unreasonable search and seizure. Critics also suggest that these measures provide legitimacy to authoritarian governments who claim to monitor traffic for technical reasons, but use it instead to silence dissent.

Canadian position

Canada has a number of legislative measures in place to protect individual privacy online, namely:

- The *Privacy Act*, which sets specific authorities for disclosure of personal information, and the instances in which the federal government is allowed to disclose personal information within government and to third parties;
- The *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which establishes a single set of requirements that mandate private entities to

protect individuals' personal information in their custody from risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction;

- The *Charter of Rights and Freedoms*, where online privacy interests factor into the guarantee against unreasonable search and seizure under Section 8; and
- The *Criminal Code*, which criminalises, among other things, the unauthorized interception of private communication and the unauthorised use of a computer.

In addition to these existing measures, the Government of Canada seeks to strengthen Canadians' privacy protections in cyberspace. In the previous Parliament, the Government introduced Bill C-29, the *Safeguarding Canadians' Personal Information Act*. The Bill offered amendments to *PIPEDA* which would require private entities to notify clients and customers of data breaches that put their information at risk.

[redacted]

Conversely, the *Criminal Code* has provisions that specifically allow owners and operators to intercept and monitor private communication for "managing the quality of service."

[redacted]

INTERNATIONAL CAPACITY BUILDING AND ASSISTANCE

Strategic Context

The developing world has rapidly adopted new digital technologies, thanks in part to significant private sector investment in infrastructure and service delivery. However, two linked obstacles challenge progress in this regard. First, there is a need for capacity building of the physical systems to deliver these services, and the appropriate regulatory and policy framework to encourage their sustainment and future scalability. Secondly, there is a need for capacity building to ensure a baseline of necessary skills among users, who may lack the tools they need due to income, age, gender or educational background.

Currently, there are a number of multilateral financing mechanisms that developing countries may utilise to promote the adoption of ICTs, key among them are the "ICT For Development" (ICT4D) series of programs to which Canada contributes. Despite this, many developing countries lack the policy capacity to create and sustain a policy and regulatory environment that encourages private sector ICT development and that would bring their digital economies in line with international standards.

[redacted]

Canadian position

Canada recognizes the importance of cyberspace as an enabler of development and actively promotes the adoption of information and communication technologies (ICTs) in the developing world. For example, the Canadian International Development Agency (CIDA) funds the training of vulnerable groups and proprietors of micro and small enterprises to use ICTs to increase employment and generate income.

Multilaterally, Canada has widely promoted the use of ICTs for development in a variety of fora such as the International Telecommunication Union (ITU) and at the G8. At the ITU, a portion of Canada's annual contribution funds the ITU's Telecommunications Development Sector (ICT4D), which provides support to developing countries seeking to expand their telecommunications infrastructure.

[redacted]

Page 591

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

CONFIDENTIAL

TAXATION OF GOODS AND SERVICES SOLD ONLINE

Strategic Context

The taxation of goods and services online is a contentious, but niche issue in some circles. Given the multistakeholder nature of the Conference, it is possible that business attendees may want to raise the issue, arguing that sales taxes levied online can hamper economic growth and development.

[redacted]

Canadian Position

Taxation is a matter of domestic policy and leaves it to individual countries to decide how best to levy taxes in an online environment. That said, however, goods and services should not be taxed to the point where they stymie economic growth and development.

In Canada, sales tax on goods and services sold online are levied and collected by the federal and provincial governments. Both levels of government have their own rules and regulations as to each tax's applicability. As a general rule however, taxation in either jurisdiction does not distinguish between whether a good or service was sold online or offline. As such, trade barriers and protectionist measures should be discouraged.

[redacted]

Considerations for discussion: N/A

NETWORK NEUTRALITY (NET NEUTRALITY)

Strategic Context

In both domestic and international digital economy debates, the issue of network neutrality (net neutrality) is often a sticking point. Net neutrality, often erroneously conflated with Internet censorship, is defined as a policy which prohibits digital carriers from discriminating against certain forms of data traffic to promote their services instead of a competitors'. For example, under a net neutrality policy, an Internet Service Provider (ISP) would be prohibited from blocking or degrading access to services offered by another company which is already offered by the ISP. This would essentially prevent ISPs who increasingly offer music, gaming or movie content from throttling connections to outside content or services.

Net neutrality advocates argue that this promotes competition because the better and more efficient service will survive based on their own merits, not because they blocked access to competitors. ISPs have argued that they should have some degree of flexibility in managing the traffic moving across their networks, in order to help mitigate network congestion caused by certain bandwidth intensive applications and services.

Net neutrality is a technical issue stemming from national policies, which is starting to have some resonance internationally and looks to drive global management of the information grid. To date only a minority of countries, almost all in the highly industrialized liberal democratic world, have specifically defined a position in this area. Notwithstanding its technical nature, certain civil society Internet activists may want to raise the issue in order to illicit a firm response from state participants.

Canadian position

Network neutrality is a matter of domestic commercial regulation, and therefore Canada leaves it to each country to develop their own policy in this area recognising that it should ultimately promote the free flow of goods and services online.

Canada's net neutrality policy allows for imposing restrictions on end use access, as long as those restrictions and activities are transparent and designed to serve a legitimate network management purpose (e.g. blocking access to malicious content, or slowing down non real-time and bandwidth intensive applications such as peer to peer file-sharing). Domestic critics of Canada's policy have argued that the policy is vague and potentially allows ISPs to discriminate against competing services due to weak enforcement measures.

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

CONFIDENTIAL

BRIEFING NOTE

THE SOCIAL BENEFITS OF CYBERSPACE

KEY ISSUES

s.13(1)(a)

[redacted]

- Access to cyberspace;
- Capacity building assistance for developing countries;
- Privacy in cyberspace; and
- Respect for human rights.

Issue briefs on each topic, describing its strategic context, the Canadian position, and considerations for discussion, accompany this note.

There is likely to be a significant overlap in subject matter between this panel and the panels on Economic Growth and Development and Safe and Reliable Access. Accordingly, much of the same material appears in the briefs.

ACCESS TO CYBERSPACE

Strategic context

Access to cyberspace and related technologies is inherently beneficial to all. From an economic perspective, access to cyberspace is a significant driver for future economic growth, innovation, and prosperity. It also allows goods and services to be delivered more quickly and efficiently. From an educational perspective, cyberspace is the great knowledge equalizer – it offers individuals access to near infinite amounts of information. These benefits have been highlighted in a number of international documents including the *2005 Tunis Agenda for the Information Society* and the *2011 OECD Communiqué on Internet Policy-Making*.

In light of the Internet's enormous benefits, some states and civil society organisations argue that states need to make access to cyberspace, and the Internet more specifically, a fundamental right to guarantee that everyone has access to the innumerable opportunities that it affords. Greece, Finland, France, Estonia and Spain have recently declared Internet access as a human right, and a number of Special Rapporteurs on freedom of expression from various international organisations (e.g. U.N., Organisation for the Security and Cooperation in Europe) have supported this view.

Other states have been more reluctant to view cyberspace access as a right. Some view linking the human rights discourse to cyberspace as an imposition of Western values in an effort to assimilate or overrun local culture. These states are also reluctant to provide access to an instrument that may potentially destabilise their political system. Others argue that it is disingenuous to create a new right when there are a number of existing human rights obligations, such as gender and minority rights, that have yet to be fully realized.

While the international human rights dimension of cyberspace has yet to be settled, many countries agree on the benefits of providing citizens the skills, knowledge and training required. Some countries have incorporated the teaching of basic safe browsing techniques as part of their national education curriculum, while others incorporate skills development as part of worker re-training programmes. Many states, especially highly advanced economies, promote cyberspace by increasingly providing services online, making service delivery cheaper and more convenient.

Canadian position

Canada recognises the collective benefit of online access in terms of its social, educational, and economic potential: greater access to cyberspace should be encouraged.

As private companies deliver access to cyberspace in Canada, the primary role of the federal government is to ensure that the domestic market for the delivery of online services is competitive. Recognizing its benefits, however, the federal government also promotes access to cyberspace largely through subsidies and partnerships with provinces, businesses and community organisations.

[redacted]

Issues to consider

- *Private ownership*: Most of Canada's cyber infrastructure is owned and operated by private companies or are outside the federal government's jurisdiction. Given this, the Government of Canada plays a limited role in directly providing cyberspace access to citizens and businesses.

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

s.21(1)(a)

s.21(1)(b)

CONFIDENTIAL

CAPACITY BUILDING ASSISTANCE FOR DEVELOPING COUNTRIES

Strategic context

Information and communication technologies (ICTs) offer those in the developing world the ability to improve their lives by overcoming asymmetrical access to and use of information and knowledge, a principle driver of social and economic inequality. The expansion of the Internet, the growth of mobile phone use, and the emergence of social media are reshaping the way people access and share information. For developing countries, the digital economy is an essential tool to support public sector service delivery by promoting transparency and accountability, while enabling the private sector to access new markets.

Unfortunately, two linked obstacles challenge progress in this regard. First, there is a need for capacity building of the physical systems to deliver these services, and the appropriate regulatory and policy framework to encourage their sustainment and future scalability. Secondly, there is a need for capacity building to ensure a baseline of necessary skills among users, who may lack the tools they need due to income, age, gender or educational background.

Currently, there are a number of multilateral financing mechanisms that developing countries may utilise to promote the adoption of ICTs, key among them are the "ICT For Development" (ICT4D) series of programs. Despite this, many developing countries lack the policy capacity to create and sustain a policy and regulatory environment that encourages private sector ICT development and that would bring their economies in line with international standards.

Canadian position

Canada recognizes the importance of cyberspace as an enabler of development and actively promotes the adoption of information and communication technologies (ICTs) in the developing world. For example, the Canadian International Development Agency (CIDA) funds the training of vulnerable groups and proprietors of micro and small enterprises to use ICTs to increase employment and generate income.

Multilaterally, Canada has widely promoted the use of ICTs for development in a variety of fora such as the International Telecommunication Union (ITU) and at the G8. At the ITU, a portion of Canada's annual contribution funds the ITU's Telecommunications Development Sector (ICT4D), which provides support to developing countries seeking to expand their telecommunications infrastructure.

Page 598

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

PRIVACY IN CYBERSPACE

Strategic context

Advances in computing have made it easier and affordable for individuals to exchange information and for businesses to store data, creating a host of benefits for society. However, networked systems are inherently vulnerable and data breaches can cause significant harm, ranging from violations of individuals' personal security to severely damaging a country's economy.

A number of jurisdictions have struggled with applying traditional notions of privacy into a digital world. Privacy has long been recognized by liberal democratic governments as a requirement for active participation online. Accordingly, privacy Commissioners in the Western world are constantly raising awareness of the privacy implications of new technologies; in some cases they have been driving policy change by affecting legal changes to strengthen privacy. The OECD is currently reviewing its Data Protection Guidelines, the European Union has been reviewing its EU Data Protection Directive, and the United States has issued a Green Paper on privacy in 2010, a final response to which is expected soon.

The need to have privacy follow an individual as their data migrates through cyberspace, an issue known as "accountable transborder data flow", is emerging as a key international issue. Without these consistent rules, barriers to the free flow of information across international borders are likely to arise.

There are several factors competing against strong privacy. First, corporations will only meet such standards as they are required to, which is often in a different legal jurisdiction than the individual accessing those services. In some other jurisdictions, companies are required to disclose when personal information has been put at risk in order to empower individuals to take action and protect themselves; in other areas such programs do not exist. Secondly, there is a need for governments and cyber infrastructure operators to monitor data traffic to ensure the health and security of the network. Some segments of civil society are sceptical of greater government intrusion into citizens' lives argue that traffic monitoring is likely to be abused, and opens the door to violations of individuals' right to be protected from unreasonable search and seizure. Critics also suggest that these measures provide legitimacy to authoritarian governments who claim to monitor traffic for technical reasons, but use it instead to silence dissent.

Canadian position

Canada has a number of legislative measures in place to protect individual privacy online, namely:

- The *Privacy Act*, which sets specific authorities for disclosure of personal information, and the instances in which the federal government is allowed to disclose personal information within government and to third parties;
- The *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which establishes a single set of requirements that mandate private entities to

protect individuals' personal information in their custody from risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction;

- The *Charter of Rights and Freedoms*, where online privacy interests factor into the guarantee against unreasonable search and seizure under Section 8; and
- The *Criminal Code*, which criminalises, among other things, the unauthorized interception of private communication and the unauthorised use of a computer.

In addition to these existing measures, the Government of Canada seeks to strengthen Canadians' privacy protections in cyberspace. In the previous Parliament, the Government introduced Bill C-29, the *Safeguarding Canadians' Personal Information Act*. The Bill offered amendments to *PIPEDA* which would require private entities to notify clients and customers of data breaches that put their information at risk.

[redacted]

Conversely, the *Criminal Code* has provisions that specifically allow owners and operators to intercept and monitor private communication for "managing the quality of service."

[redacted]

RESPECT FOR HUMAN RIGHTS

Strategic context

Cyberspace has emerged as an extraordinary tool for ordinary citizens to exercise, and in some cases claim for the first time, their basic rights and freedoms enshrined in the *Universal Declaration of Human Rights,* the *International Covenant on Civil and Political Rights*, and the *International Covenant on Economic, Social and Cultural Rights*. While an unintended consequence, cyberspace has nonetheless become an enabler of rights, often granting a degree of freedom not always present outside of the online world.

[redacted]. The U.S., for example, has reinforced its commitment to defending fundamental rights and freedoms on the Internet in a number of policy pronouncements (the May 2011 *International Strategy for Cyberspace*; speeches by the Secretary of State).

Aside from merely promoting freedom, some states are trying to make censorship more difficult. The U.S. Congress is considering legislation to prevent repressive governments from using American technology to suppress their citizens' basic rights and freedoms on Internet. Similarly, the E.U. is considering amending its export control regime to prohibit the export of software or hardware "for use in connection with a violation of human rights, democratic principles or freedom of speech."

International human rights law recognises that rights and freedoms are not absolute and are subject to certain restrictions to not impede the rights of others. These restrictions may only be enforced if they are applied in a transparent, necessary, and proportionate manner. For example, in the Western world, hate speech and child pornography are generally accepted areas where expression can be curtailed and are subject to judicial review

[redacted]

Canadian position

Human rights protections apply in cyberspace and states should uphold their domestic and international human rights obligations.

Domestically, the rights most often raised when discussing cyberspace (freedom of expression, association, privacy and equality) are all constitutionally entrenched in Canada's *Charter of Rights and Freedoms*. The *Charter* extends to all levels of government action, and therefore any action in cyberspace would be subject to the *Charter*. *Charter* rights are not absolute, and are subject to only such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society. Such limits in Canada include, *inter alia*, hate speech and child pornography. While both are subject to having their content seized and removed upon judicial review, there are no specific legal provisions in Canada that require the state to block access to websites.

Internationally, Canada is a party to a number of international human rights conventions, notably, the *International Covenant on Civil and Political Rights* (ICCPR), the *International Covenant on Economic, Social and Cultural Rights* (ICESCR), the *Convention on the Elimination of All forms of Discrimination against Women* (CEDAW).

[redacted]

Canada has pledged to support the application of rights and freedoms on the Internet in a number of fora. For example, it joined allies in supporting a "Joint Statement on Freedom of Expression on the Internet" at the United Nations Human Rights Council in June 2011. In addition, at the 2011 G8 Summit, the Prime Minister joined G8 leaders in encouraging "the use of the Internet as a tool to advance human rights and democratic participation throughout the world."

[redacted]

CONFIDENTIAL

BRIEFING NOTE

TACKLING CYBERCRIME

KEY ISSUES

s.13(1)(a)

[redacted]

- *Council of Europe Convention on Cybercrime* (Budapest Convention);
- International cooperation;
- Cybercrime capacity building assistance;
- Minimum codes of conduct; and
- Public awareness of cybercrime.

Issue briefs on each topic, describing its strategic context, the Canadian position, and considerations for discussion, accompany this note.

THE NATURE AND SCOPE OF "CYBERCRIME"

Generally the concept of "computer crime" refers to crimes specifically directed against computers, networks, data and their users (e.g. "hacking", hostile software etc.), whereas "computer-related crime" extends to the broader category of other offences (fraud, identity crime etc.) that can be committed using computer systems. The terms "computer crime", "computer-related crime" and "cybercrime" are all commonly used, but there is no universal consensus as to what the terms mean or what should be made the subject of criminal offences, domestic investigative powers, and international cooperation obligations.

For example, there is wide consensus that criminal law and international cooperation mechanisms should be used to suppress the dissemination of child pornography. Some countries, however, consider issues such as religious freedom, promoting separatist movements, and anti-state content to also be "cybercrime".

CONFIDENTIAL

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION)

Strategic Context

The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the only widely-recognised attempt to deal with cybercrime issues and contains the most accepted typology for cybercrime. The treaty is uncharacteristically specific, precisely describing which actions are prohibited in cyberspace, the extent of personal and corporate liability, and search and seizure of computer data. It also provides specific mechanisms to facilitate law enforcement cooperation in cyberspace through a 24/7 assistance network. Given its high level of specificity, only 31 countries are parties to the Convention.

While the Convention is trumpeted as the gold standard to combat cybercrime among Western countries, a number of states have been reluctant join largely on the grounds that some of its core elements, such as the 24/7 information sharing network, violate national sovereignty. It is also on sovereignty grounds that certain countries reject provisions in the Convention that allows Parties to access stored computer data with consent of the data's host or where it is publicly available.

Some countries also view it as politically unacceptable to accede to a largely European-centric treaty, having been negotiated between members and observers of the Council of Europe. These countries, largely in the developing world, believe that a global cybercrime instrument, negotiated through a United Nations process, would be more representative of a global consensus.

Canadian position

Canada actively promotes the Budapest Convention as a key instrument to effectively combat cybercrime. Canada signed the treaty in 2001 but has not yet ratified. The Government sought to implement elements of the Convention which were not already part of Canadian law in the last Parliament as part of Bill C-51 (*Investigative Powers of the 21st Century Act*). However, the Bill died on the Order Paper when the last federal election was called in March, 2011.

Despite having not yet ratified the Budapest Convention, Canada's *Criminal Code* addresses the vast majority of crimes that occur in, or are facilitated by, cyberspace. Most of these provisions were written in a technologically neutral manner; for example, the methods that criminals use to buy and sell stolen credit card numbers online are not criminalised given that theft and identity fraud are inherently criminal acts. For example, the *Code* has provisions criminalizing:

- the possession and distribution of child pornography (s. 163);
- the unlawful interception of private communications (s. 184), possession of an illegal device for surreptitious interception of private communications (s.191), and limitations on the disclosure of intercepted communications (s.193);
- possession of a device to obtain telecommunication facility or service (s. 327);

- the unauthorized use of a computer (s. 342.1);
- the possession of a device to illegally obtain a computer service (s. 342.2);
- the theft of identity or the fraudulent use of someone's identity (s. 380, s. 402.1, s. 402.2, and s. 403);
- mischief to data (s. 430(1.1));
- the trafficking of controlled drugs and substances (*Controlled Drugs and Substances Act*); and
- the infringement of intellectual property (*Copyright Act*, *Trade-marks Act*, and the *Patent Act*).

INTERNATIONAL COOPERATION

Strategic Context

In the abstract, all states agree that greater cooperation is required to prevent and prosecute cybercrime. However, states have significant disagreements over the definition of cybercrime. This definitional dichotomy has serious repercussions on international cooperation. Countries using a narrow definition of cybercrime may be reluctant to share information or evidence with states with a broader definition as it could potentially be used for illegitimate purposes, such as cracking down on dissent, in violation of domestic or international law.

Jurisdictional issues can also pose a significant impediment to effective international cooperation on cybercrime, especially the way in which information travels in cyberspace. For example, investigative and enforcement measures are strictly limited to the territorial jurisdiction of the state. In essence, this prevents a state from gathering data held in cyberspace outside of its jurisdiction without the consent of the state in which the data is held. This can potentially lead to long, formal, and arduous processes to obtain consent and can undermine investigations.

There are two international instruments which aim to facilitate cooperation. First, the *U.N. Convention against Transnational Organised Crime* (Palermo Convention) which facilitates law enforcement cooperation when crimes are committed by a group (i.e. three or more people) and are transnational in nature. A significant amount of criminal activity online fits this definition, facilitating the cooperation of approximately 160 States Parties on cybercrime enforcement. However, given the lack of international consensus on a definition of cybercrime, cooperation under the Palermo Convention can be challenging.

Second, the *Council of Europe Convention on Cybercrime* (Budapest Convention) establishes specific mechanisms for cooperation, such as the requirement for reciprocal frameworks for legal assistance, the harmonization of computer-related offences, and the establishment of a 24/7 contact network. Only 31 countries are parties to the Budapest Convention given its high level of specificity. While Canada is a signatory, it has yet to ratify.

Canadian position

International cooperation on cybercrime issues is necessary to effectively deter cyber criminals and hold them to account. To this end, Canada actively advocates that countries sign the Budapest Convention or adopt its provisions as a model for domestic cybercrime legislation.

Canada facilitates international cooperation on cybercrime in a number of ways. As a Party to the Palermo Convention, Canada provides legal and investigative assistance to

other Parties as required. As a signatory to the Budapest Convention, Canada has identified points of contact at the Royal Canadian Mounted Police to facilitate cooperation as part of the global 24/7 global cybercrime network. At the G8, Canada contributes to the Roma/Lyon High Tech Crime Sub Group, which seeks to bridge operational and policy gaps that hinder effective cybercrime cooperation.

Despite these efforts, effective cooperation on cybercrime remains challenging due to jurisdictional barriers, different evidence gathering standards, and lack of consensus on the definition of cyber-related offences.

CYBERCRIME CAPACITY BUILDING ASSISTANCE

Strategic Context

The rapidly evolving cybercrime landscape means that countries must continuously adapt their investigative methods, update their legal frameworks and cooperate internationally. This poses a substantial challenge even for developed countries with the resources for State-based programmes and in which most of the major private-sector entities are located. It is a much greater challenge for developing countries, in which even basic legal and law enforcement infrastructure may be weak or absent.

The need for technical assistance is dealt with in other crime treaties such as the 2000 *Palermo Convention* which addresses transnational organised crime. The usual pattern in such instruments is that developed countries obtain enhanced legal and law enforcement frameworks, and developing countries receive in exchange the financial resources and expertise needed to meet the new requirements. The need for technical assistance is one of the underlying reasons many developing (G-77) states now seek a global legal instrument at the UN.

To reduce this pressure, the United States and like-minded countries have begun to emphasize the availability of such assistance more immediately. A G-77 proposal to create a direct technical assistance mandate for the UN Office on Drugs and Crime at the April 2011 session of the Commission on Crime Prevention and Criminal Justice enjoyed wide support, and work on this is now commencing.

[redacted]

Canadian position

Capacity building assistance can play a key role in mitigating the effects of cybercrime, and that donor countries should provide assistance in a focused and sustainable manner.

In its development assistance, Canada has not focused on cybercrime assistance given its niche appeal and its recent emergence as a global challenge. However, its funding of certain multilateral institutions, such as the International Telecommunication Union's Development Branch, has provided support for cybercrime initiatives. This support

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

CONFIDENTIAL

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

generally involves policy and legislative support to provide local authorities with an effective framework to address cybercrime.

Bilaterally, Canada has provided capacity building assistance on cybercrime through the Royal Canadian Mounted Police, which has provided training on data retrieval for evidence-gathering purposes.

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

CONFIDENTIAL

DOMESTIC MINIMUM CODES OF CONDUCT

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

Strategic Context

The idea of minimum codes of conduct for cyber space users has been gaining traction internationally. These codes of conduct would be voluntary and would essentially guide private sector actions in cyberspace to ensure a basic level of security. For example, a code may include provisions whereby signatories aim to keep all identifiable and financial information on their clients encrypted. This would prevent the most basic incidents of cybercrime where financial information obtained through cyber intrusions are used to steal someone's identity.

Some countries, such as Australia, already have a voluntary code for Internet Service Providers (ISPs) that provides guidance on how to prevent and mitigate malicious activity on their networks. For example, ISPs can inform customers that their computers have been compromised and notify Australian authorities of possible malicious activity.

Much of the discussion on minimum codes of conduct focuses on the role of ISPs, given their importance in the distribution of cyber services. However, these codes can extend beyond cyberspace providers and include the banking, electricity and finance sectors to ensure baseline security standards to mitigate and prevent cybercrime. Such features could include the encryption of individuals' credit card information stored with businesses, or timely patch deployment to fix network vulnerabilities in a particular sector.

[redacted]

Canadian position

[redacted]

Despite not having a formal code of conduct, the Canadian telecommunications industry had voluntarily adopted certain practices, such as disclosing subscriber information without a court order, to assist in child pornography investigations. This voluntary initiative was made mandatory with the passage of Bill C-22, *An Act Respecting the*

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

CONFIDENTIAL

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

Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service, which obtained Royal Assent on March 23, 2011.

PUBLIC AWARENESS OF CYBERCRIME

Strategic Context

Recent high profile cyber intrusions and data breaches have heightened the public's awareness of cybercrime. Despite this greater awareness, individuals and businesses have been slow to take the appropriate steps required to prevent falling victim to cybercrime. Additionally, there is a significant lack of understanding amongst businesses and individuals of some of the basics of cybercrime – notably how cybercrime is defined – leading to overreactions which hamper public awareness and prevention efforts.

In order to effectively identify, investigate and prosecute cybercrime, the public should have a measured understanding of the challenges that cybercrime poses, and the simple and routine measures to mitigate the most basic cybercrime. Some countries have incorporated the teaching of basic safe browsing techniques as part of their national education curriculum. By addressing these issues early, individuals will have a better understanding of cyberspace's inherent risks and that they have the knowledge and strategies to protect themselves against cyber criminals.

The private sector and civil society organisations also have an important role in raising awareness of cybercrime. They can both complement state-led efforts by providing tools and techniques for safer access to cyberspace – something which they do already.

Canadian position

States, businesses and civil society have an active role to play in raising cybercrime awareness, and that they should work together to mitigate the effects of cybercrime.

Canada, through Public Safety Canada, raises awareness on cyber security issues through the annual Cyber Security Month held in October. The awareness month is coordinated with Australia, the United Kingdom and the United States and aims to remind individuals on how to protect themselves and to guard against cybercrime.

While the federal government plays an active role in promoting cyber security, it doesn't require that cyber security awareness becomes part of the educational curriculum as it is in some countries. Doing so would impose on provincial and territorial jurisdiction. Nevertheless, the federal government works with private sector and community groups to raise awareness about the importance of safe browsing techniques, updating critical software, and network security (i.e. protecting a wireless network) in partnership with the provinces and territories.

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

Issue to consider

- *Jurisdictional issues*: Should discussion move to the incorporation of cyber security public awareness into the education curriculum, Canada should mention that, as a federated country, the responsibility for education in Canada rests with provincial governments. Notwithstanding, Canada works with the private sector and civil society to inform individuals about cybercrime, and measures they can take to protect themselves.

CONFIDENTIAL

BRIEFING NOTE

SAFE AND RELIABLE ACCESS

s.13(1)(a)

KEY ISSUES

[redacted]

- Protecting and defending systems of national importance;
- Global interoperability;
- Information sharing on the source of malicious activity;
- Privacy in cyberspace; and
- Public awareness and education.

Issue briefs on each topic, describing its strategic context, the Canadian position, and considerations for discussion, accompany this note.

There is likely to be a significant overlap in subject matter between this panel and the panels on Economic Growth and Development and Social Benefits. Accordingly, much of the same material appears in the briefs.

PROTECTING AND DEFENDING SYSTEMS OF NATIONAL IMPORTANCE

Strategic context

All countries, to a certain extent, agree with the need to protect and defend systems of national importance whether physical or digital. The divergence of views largely rests on the interpretation of sovereignty, and what constitutes sovereignty in cyberspace.

[redacted]

Countries on the other side of the sovereignty spectrum see an important role for the state, but also recognise that much of cyberspace is privately owned and operated. While the state plays a supporting role in protecting critical infrastructure, their primary focus is safeguarding networks of national importance, not all networks within a state's jurisdiction. This more minimalist approach recognises that protecting and defending systems of national importance is not the exclusive purview of the state.

On a practical level however, many countries are shoring up their defences in the event of a major cyber attack. States, both on a bilateral and multilateral level (e.g. NATO), have begun to develop doctrine and response mechanisms should ever a cyber incident amount to an armed attack as defined in the traditional military sense. There is, however, a lack of consensus on how actions in cyberspace conform to traditional notions of self-defence, proportionality, and distinction in the military sphere. On a more fundamental level, there is a lack of understanding of what "cyber warfare" actually means and whether military responses are appropriate or legal. Unsurprisingly, this has led to heightened tensions, which countries are looking to diffuse though confidence building measures (e.g. meetings among senior officials, information sharing).

[redacted]

Canadian position

Canada takes a more minimalist approach to cyberspace, recognising that the private sector, provinces, territories, and municipalities share responsibilities in helping Canada protect its critical networks. Under the *Emergency Management Act*, the Minister of Public Safety is responsible for leading the overall national effort to strengthen the

resilience of critical infrastructure. To this end, the federal government works closely with critical infrastructure owners to assist in protecting them from a range of cyber threats. Beyond Public Safety and its mechanisms to protect national critical infrastructure, Communications Security Establishment Canada has a mandate to provide advice, guidance, and services to help ensure the protection of electronic information and of information infrastructures of importance to Canada.

In terms of defending its critical infrastructure, Canada is currently exploring information sharing mechanisms which would allow the federal government to share threat information with infrastructure owners. Through NATO, Canada has been actively involved in the development of the organisation's cyber defence policy,

GLOBAL INTEROPERABILITY

Strategic context

Access to cyberspace and related technologies are inherently beneficial to everyone around the world. From an economic perspective, access to cyberspace will be a significant driver for future economic growth, competition, innovation, and prosperity. From an educational perspective, cyberspace is the great knowledge equalizer – it offers individuals access to near infinite amounts of information. These benefits exist due to the simple fact that technical standards cyberspace standards are largely universal, allowing anyone with the requisite equipment to connect with others. The Internet, for example, works because its architecture is globally interoperable: a website or service can be accessed from anywhere in the world with little or no alteration to its content.

[redacted]

On the whole, these efforts limit cyberspace interoperability, and create a precedent for the further fracturing of cyberspace, which would prevent individuals from fully benefiting from its innumerable opportunities.

In addition to the fracturing of cyberspace, certain countries seek to exert greater policy control over some of cyberspace's more technical issues. Since the advent of the Internet and cyberspace, a number of non-state technical experts have set global standards to ensure interoperability. As cyberspace mostly existed in the developed world, this approach remained uncontroversial as technical considerations were balanced with state-based policy objectives to ensure that cyberspace is open, accessible, and resilient. Once developing countries became more connected, they sought to exert more influence over certain technical aspects to make cyberspace more reflective of their local and cultural realties. Consequently these technical changes, such as the inclusion of non-Latin script for web addresses, were introduced.

[redacted]

Canadian position

Canada recognises cyberspace's global interoperability as integral to maintaining the benefits that it affords. As such, Canada has taken a position in a number of international fora, similar to that of our allies, that the technical aspects of cyberspace are best left to technical experts with a limited operational role for states. This allows cyberspace to remain a neutral platform and restrains the role of politics, to the extent possible, from threatening cyberspace's global interoperability.

INFORMATION SHARING ON THE SOURCE OF MALICIOUS ACTIVITY

Strategic context

Cyberspace is the accumulation of a myriad of interconnected computer-based systems, ranging from cellular technology to the Internet's backbone, to transmit information. Being man-made, however, the architecture that sustains cyberspace, the hardware, the software and the protocols, have vulnerabilities that can be exploited for personal, criminal, or national gain. When the Internet was designed over fifty years ago, security was not a significant issue as it was largely the purview of technology experts and researchers who knew each other. Furthermore, the main objective of the system was not to necessarily have secure communication, but to have a communication system in the event that all others failed. As the Internet has evolved, it has gone far beyond the trusted networks of researchers and into the public domain, making it more relevant from an economic and social perspective, but much less secure.

The exponential increase in security vulnerabilities requires better domestic and international cooperation to address the corresponding malicious activity which seeks to undermine or exploit the digital architecture. Currently, however, there are very few structured mechanisms with which security researchers, businesses, technology vendors, security software companies, and national Computer Emergency Response Teams (CERTs) can share information on security vulnerabilities and malicious activity. All information sharing is done on an ad-hoc basis, if at all as some businesses, vendors, or states have a disincentive to report malicious activity due to the business or reputational costs that would ensue. In the public sector, when governments detect vulnerabilities or significant malicious activity patterns, they may be incapable of sharing that information due to classification requirements.

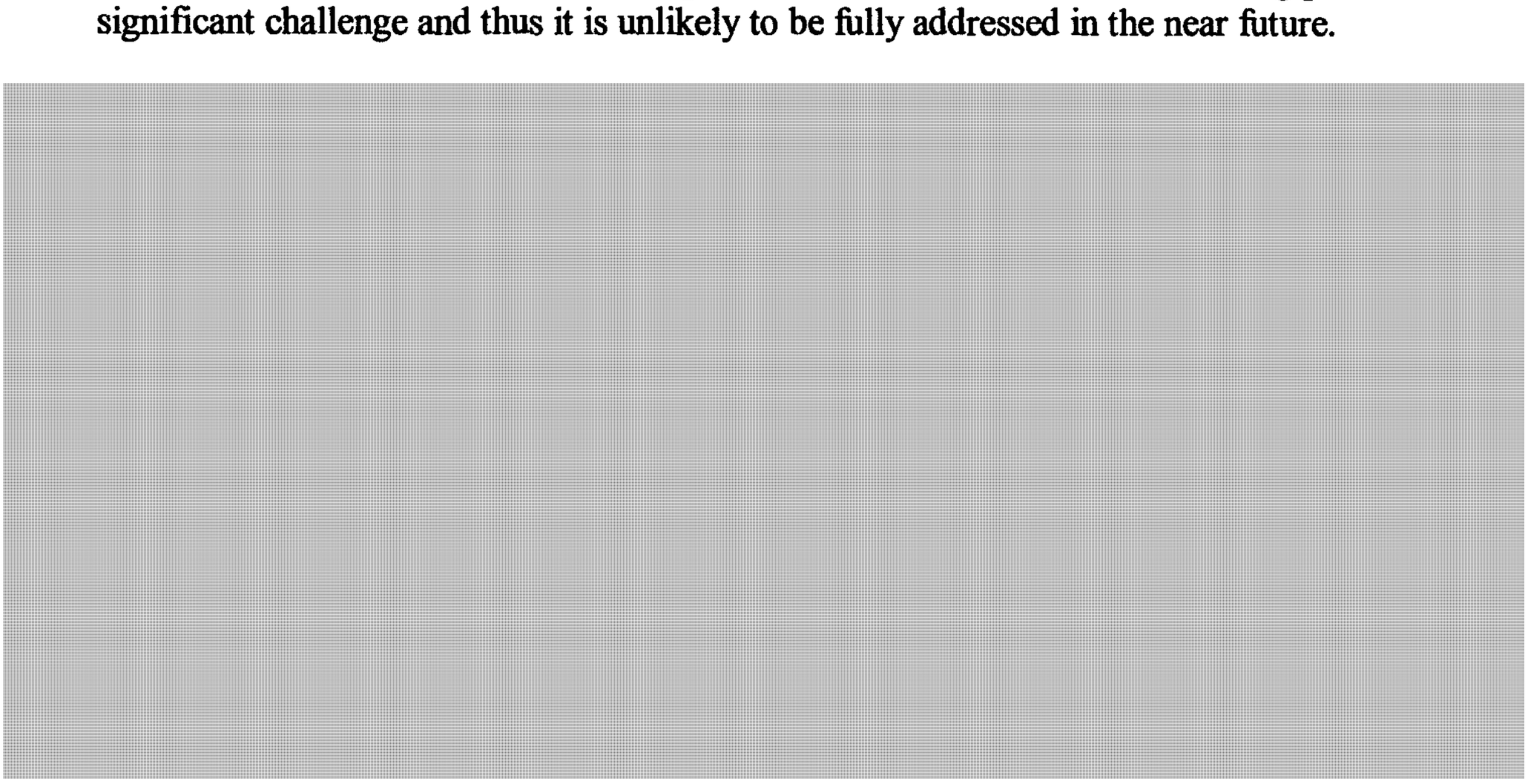
Certain countries are beginning to address the need to share malicious activity patterns to improve situational awareness. However, much of this activity is done between countries or between countries and select businesses (e.g. defence contractors, telecommunications providers) that already have a high degree of trust given the sensitivity of the material being shared, and tend to only address malicious activity that poses a threat to national security.

Canadian position

As previously stated, most of the information sharing on malicious activity occurs on an ad-hoc and voluntary basis, and Canada is no exception. Canada's national CERT, the Canadian Cyber Incident Response Centre (CCIRC), distributes malicious activity information to Canadian businesses to help them protect themselves. Canadian companies, however, are under no obligation to disclose to CCIRC whether they have been subject to malicious activity. Similarly, companies are under no obligation to disclose that they have been a victim of malicious activity to anyone else, such as their clients or shareholders.

Canada, through Public Safety Canada and Industry Canada, is currently examining the possibility of greater information sharing between and within the private sector and

government. For example, representatives from Industry Canada, Public Safety, and the private sector meet as part of the Canadian Secure Telecommunications Advisory Committee to study information sharing barriers. However, information sharing poses a significant challenge and thus it is unlikely to be fully addressed in the near future.



PRIVACY IN CYBERSPACE

Strategic context

Advances in computing have made it easier and affordable for individuals to exchange information and for businesses to store data, creating a host of benefits for society. However, networked systems are inherently vulnerable and data breaches can cause significant harm, ranging from violations of individuals' personal security to severely damaging a country's economy.

A number of jurisdictions have struggled with applying traditional notions of privacy into a digital world. Privacy has long been recognized by liberal democratic governments as a requirement for active participation online. Accordingly, privacy Commissioners in the Western world are constantly raising awareness of the privacy implications of new technologies; in some cases they have been driving policy change by affecting legal changes to strengthen privacy. The OECD is currently reviewing its Data Protection Guidelines, the European Union has been reviewing its EU Data Protection Directive, and the United States has issued a Green Paper on privacy in 2010, a final response to which is expected soon.

The need to have privacy follow an individual as their data migrates through cyberspace, an issue known as "accountable transborder data flow", is emerging as a key international issue. Without these consistent rules, barriers to the free flow of information across international borders are likely to arise.

There are several factors competing against strong privacy. First, corporations will only meet such standards as they are required to, which is often in a different legal jurisdiction than the individual accessing those services. In some other jurisdictions, companies are required to disclose when personal information has been put at risk in order to empower individuals to take action and protect themselves; in other areas such programs do not exist. Secondly, there is a need for governments and cyber infrastructure operators to monitor data traffic to ensure the health and security of the network. Some segments of civil society are sceptical of greater government intrusion into citizens' lives argue that traffic monitoring is likely to be abused, and opens the door to violations of individuals' right to be protected from unreasonable search and seizure. Critics also suggest that these measures provide legitimacy to authoritarian governments who claim to monitor traffic for technical reasons, but use it instead to silence dissent.

Canadian position

Canada has a number of legislative measures in place to protect individual privacy online, namely:

- The *Privacy Act*, which sets specific authorities for disclosure of personal information, and the instances in which the federal government is allowed to disclose personal information within government and to third parties;
- The *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which establishes a single set of requirements that mandate private entities to

s.15(1) - Int'l

protect individuals' personal information in their custody from risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction;

s.15(1) - Subv

- The *Charter of Rights and Freedoms*, where online privacy interests factor into the guarantee against unreasonable search and seizure under Section 8; and
- The *Criminal Code*, which criminalises, among other things, the unauthorized interception of private communication and the unauthorised use of a computer.

In addition to these existing measures, the Government of Canada seeks to strengthen Canadians' privacy protections in cyberspace. In the previous Parliament, the Government introduced Bill C-29, the *Safeguarding Canadians' Personal Information Act*. The Bill offered amendments to *PIPEDA* which would require private entities to notify clients and customers of data breaches that put their information at risk.

s.21(1)(c)

[redacted]

Conversely, the *Criminal Code* has provisions that specifically allow owners and operators to intercept and monitor private communication for "managing the quality of service."

[redacted]

PUBLIC AWARENESS AND EDUCATION

Strategic context

Recent high profile cyber intrusions and data breaches have heightened the public's awareness of some of the inherent risks of operating in cyberspace. This may leave certain segments of society weary of engaging in this new domain, preventing them from fully benefiting from everything that cyberspace has to offer. Additionally, there is a significant lack of understanding amongst businesses and individuals of some of the basics of cyber security, leading to overreactions and panic that hamper public awareness efforts.

In order to build greater confidence, the public should have a measured understanding of the challenges that cyberspace poses, and that simple and routine measures can often mitigate the most basic risks. Some countries have incorporated the teaching of basic safe browsing techniques as part of their national education curriculum. By addressing these issues early, individuals will have a better understanding of cyberspace's inherent risks and have the knowledge and strategies to protect themselves against cyber risks.

The private sector and civil society organisations also have an important role in raising awareness of cyber crime – they can both complement state-led efforts by providing tools and techniques for safer access and use of cyberspace. Many businesses already do these things by providing services that enhance user safety in cyberspace (e.g. offering malware protection), although clients do not always implement security updates in a timely manner. In other cases, however, many businesses (e.g. financial institutions) assume some, if not all, of the liability for protecting individuals online, effectively allowing individuals to outsource security measures to others.

These efforts, compounded with effective anti-cybercrime and privacy regimes, can give people the confidence required for safe and reliable access in cyberspace.

Canadian position

States, businesses and civil society have an active role to play in raising awareness of the inherent challenges of engaging in cyberspace, and that they should work together to mitigate them.

Canada, through Public Safety Canada, raises awareness on cyber security issues through the annual Cyber Security Month held in October. The awareness month is coordinated with Australia, the United Kingdom and the United States and aims to remind individuals on how to protect themselves and to guard against cybercrime.

While the federal government plays an active role in promoting cyber security, it doesn't require that cyber security awareness becomes part of the educational curriculum as it has in some countries due to jurisdictional requirements. Despite this, the federal government works with, private sector and community groups to raise awareness about the importance of safe browsing techniques, updating critical software, and network security (i.e. protecting a wireless network).

Page 624

is withheld pursuant to sections

est retenue en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

CONFIDENTIAL

BRIEFING NOTE

INTERNATIONAL SECURITY

s.13(1)(a)

KEY ISSUES

[redacted]

- Confidence and security building measures;
- The role of international and regional security organisations; and
- Effectiveness of international law.

Issue briefs on each topic, describing its strategic context, the Canadian position, and considerations for discussion, accompany this note.

Only government delegations will be allowed to attend this panel session.

CONFIDENCE AND SECURITY BUILDING MEASURES

Strategic context

Confidence and security building measures (CSBMs) are agreements (not necessarily treaties) between two or more states to exchange information with the aim of reducing tensions and anxiety between parties. This in turn makes state behaviour more predictable and lessens the chance of escalation in the event of a security incident. Common CSBMs include "hotlines" to ensure quick communication between senior leaders in the event of an incident, verification and monitoring arrangements to gauge an understanding of a potential adversary's capabilities, and regional communication centers to assist parties in crisis management. CSBMs are largely a product of the Cold War and traditional arms control regimes, as they allow parties to monitor each others' military capabilities and reduce the risk of misunderstandings that can potentially lead to hostilities.

Given the emergence of cyberspace as a new domain, there is a great deal of uncertainty with regards to states' capabilities, command structures, doctrine, and posture. This uncertainty compounds the already heightened sense of vulnerability to cyber attacks in some circles: the challenge with attributing cyber attacks and the low barriers to entry makes it impossible to use traditional Cold War deterrence mechanisms to fend off a potential attacker. While these concerns may be overblown, they are real and increase the potential for escalation, especially given the fact that some countries, notably the U.S., have publicly asserted that a devastating cyber attack could result in a kinetic response. These heightened tensions have led some states and non-governmental organisations to call for the application of traditional CSBMs to cyberspace with the hopes of lessening suspicions.

s.13(1)(a)

To date, little research has been done to examine the viability of CSBMs in cyberspace.

[redacted] Multilaterally, a U.N. Group of Governmental Experts (GGE) was established in 2009 to examine cyber risks and vulnerabilities with the view of increasing cooperation mechanisms to mitigate possible threats. Brazil, China, France, Germany, India, Israel, South Korea, Russia, the U.K. and the U.S. are all represented in this group.

While CSBM efforts aim to reduce tensions between countries, levels of mistrust are quite high given the exponential increase in the detection of cyber intrusions. Many governments are therefore shoring up their defences in the event of a major cyber attack and to defend against espionage. States, both on a bilateral and multilateral level (e.g. NATO), have begun to develop doctrine and response mechanisms should ever a cyber incident amount to an armed attack as defined in the traditional military sense. Some have also publicly stated that they engage in "active defence" (i.e. offensive measures) to disrupt hostile activity in cyberspace even when it does not amount to an armed attack.

s.13(1)(a)

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

s.13(1)(a)

s.21(1)(a)

s.21(1)(b)

CONFIDENTIAL

[redacted]

Canadian position

Canada believes that CSBMs can be a helpful resource to reduce tensions in cyberspace, but that some of the traditional mechanisms that have made CSBMs successful in the past (i.e. verification and monitoring mechanisms) may not currently be feasible. By way of comparison, it took a full fifteen years for CSBMs to be considered as a viable option during the Cold War, and much longer for significant measures to become operational. Furthermore, many of the successful arms control CSBMs were treaty-based, a path that Canada and allies are reluctant to take given the difficulty in keeping parties bound to any possible and appropriate text.

[redacted]

Canada has been actively involved in the development of NATO's cyber defence policy, [redacted]

CONFIDENTIAL

s.13(1)(a)

THE ROLE OF INTERNATIONAL AND REGIONAL SECURITY ORGANISATIONS

Strategic context

The increasing prominence of the international security dimensions of cyberspace has prompted certain states to raise the issue in a number of international for a, especially in light of the potential destructive power of a cyber attack. Russia, China, India, Brazil, and South Africa have sought to raise the issue in a number of international deliberative bodies to set firmer ground rules on where state actions in cyberspace fit in the conduct of state relations. Specifically, Russia has promoted the idea of an international treaty on cyberspace that would specifically set out what states could and could not do in this new domain, and has floated the idea of having these discussions within the auspices of the United Nations.

While all states can agree that there should be more defined "rules of the road" to avoid destabilising international peace and security via cyberspace, there is considerable disagreement as to which venues are more appropriate.

t This stands in sharp contrast to allies' rough definition of a cyber attack, largely considered to be an attack launched in cyberspace to disable a communication or command and control system.

On such forum is the Association of South Eastern Nations' Regional Forum (ARF) a body set up to specifically address security issues and reduce tensions among states. Historically, the ARF has tended to shy away from issuing binding commitments and has a reputation as a venue that states use to float new ideas. The Organisation for Security and Cooperation in Europe works in a similar fashion, also making it a more appropriate venue for discussion on security dimension of cyberspace.

Canadian position

Canada has not yet voiced a preference as to which fora should address cyberspace's security dimension.

In an alliance context, Canada has been actively involved in the development of NATO's cyber defence policy,

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

CONFIDENTIAL

APPLICATION OF INTERNATIONAL LAW

Strategic context

There are a number of contentious issues in regards to the applicability of existing laws and norms in cyberspace. Presently, there is a degree of uncertainty in terms of applying existing legal principles (e.g. jurisdiction), mechanisms (e.g. mutual legal assistance in criminal matters), and particular bodies of law (e.g. international humanitarian law (IHL)) in cyberspace. The novel nature of this space makes it difficult for international policy makers and lawyers to transpose core legal concepts to this new domain. For example, under international law, states may only use force against another state if authorised by the U.N. Security Council or in self defence in response to an armed attack, generally understood to be along the lines of one state launching a kinetic attack on another. In the cyber world however, it is unclear a cyber attack would ever reach the threshold of an armed attack, making it difficult to ascertain whether the use of force in self defence would be legally justified.

Despite these difficulties, a number of states have determined that the existing body of international law should apply to cyberspace as they offer a basic set of rules that allow states to roughly predict and interpret each others' actions. The U.S. has explicitly and publicly mentioned that they believe that IHL applies in cyberspace and that non-cyber methods may be used in response to a critical cyber event.

Other countries, such as Russia and China, seek new binding instruments to apply specifically to cyberspace. They argue that the old rules do not necessarily fit this new domain, and that the potential of a devastating cyber attack requires tailored rules. While states may alter their behaviour according to cyberspace's new realities, it is questionable whether new binding instruments for cyberspace would make hostile activity less likely to occur. Indeed, given the nature of cyberspace, it would be nearly impossible to verify if countries who agreed to be bound by the rules would actually follow them. Furthermore, international treaty negotiations are time consuming and resource intensive, largely making this course of action incompatible with cyberspace's dynamism.

Canadian position

Given that much of the current international system relies on these instruments and customs (e.g. sovereignty, state responsibility, non-intervention, proportionality), it is likely that Canada will support their application to cyberspace as they provide the clearest and safest way of interpreting state actions. The intention is to allow Canada to maintain its ability to act freely domestically and internationally, while being able to predict and interpret state actions.

Page 631

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

CONFIDENTIAL

RUSSIAN AND CHINESE EFFORTS TO PROMOTE AN INTERNATIONAL CODE OF CONDUCT FOR INFORMATION SECURITY

ISSUE

On September 12, 2011, China, Russia, Tajikistan and Uzbekistan tabled a draft *International Code of Conduct for Information Security* (Code of Conduct) as a document of the 66th United Nations (UN) General Assembly. It is not a resolution for the current General Assembly but the tabling states hope to compel deliberations and have drafted it in such a way that it could be raised at a future UN meeting.

BACKGROUND

Countries and international organizations are increasingly jockeying to promote their interests in the plethora of international venues where discussions on cyberspace and cyber security are occurring. Given that a number of countries, to say nothing of corporations and civil society, have very divergent views on how cyberspace and its components should function and what the role of the state should be, international consensus on issues related to cyber security has been difficult, if not impossible to achieve.

The discussion of the economic, social, technical, and security dimensions of cyberspace by international bodies can only be expected to grow. Moreover, these discussions are also frequently occurring in organizations lacking a specific mandate in the field, a situation aggravated by the ubiquitous nature of cyberspace, and by the lack of clear laws and authorities.

CONSIDERATIONS

The draft Code of Conduct is largely a compilation of language that has been promoted, in particular by China and Russia, at a number of international venues including the World Summit on the Information Society and the Association of South East Asian Nations Regional Forum.

s.15(1) - Int'l

s.15(1) - Subv

s.15(1) - Int'l

s.15(1) - Subv

CONFIDENTIAL

TALKING POINTS

[redacted]

Pages 634 to / à 638

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1) - Int'l

s.15(1) - Subv

Meeting on January 19, 2012, with Mr. Jamie Shea, Deputy Assistant Secretary General, Emerging Security Challenges, North Atlantic Treaty Organization and Officials from the NATO Cyber Incident Response Centre

ISSUE

- On January 19, 2012, you will be meeting with Mr. Jamie Shea, Deputy Assistant Secretary General, Emerging Security Challenges (**TAB B**), followed by a meeting with officials from the NATO Cyber Incident Response Centre (**TAB C and D**). These meetings will be largely an information exchange as NATO is focused on cyber defence, not cyber security. NATO is an important partner organization for the Department of National Defence/Canadian Forces (DND/CF) and Department of Foreign Affairs and International Trade (DFAIT) in advancing international security and defence issues.

STRATEGIC OBJECTIVES

- Obtain a greater understanding of how NATO works with member states on cyber defence. Lessons learned could inform Public Safety Canada's engagement.

- Obtain a greater understanding of the work of the NATO Cooperative Cyber Defence Centre of Excellence and NATO's efforts to establish cyber defence collaboration with the private sector.

- Sensitize NATO officials that in the Canadian context, national cyber security is principally the responsibility of Public Safety Canada.

- Identify some of the accomplishments of the Government of Canada's efforts in implementing *Canada's Cyber Security Strategy* (**TAB E – Backgrounder**).

BACKGROUND

In 2010, at the Lisbon Summit, leaders of NATO member states agreed to a revision to the Alliance's seminal policy document, the Strategic Concept (**TAB F**). This update, only the fifth since NATO was established, is entitled *Active Engagement, Modern Defence* and signalled several clear shifts in transatlantic defence policy. It directly addressed threats from cyberspace and concluded that cyber attacks represent a risk to Allies' security. In extreme circumstances, cyber attacks against member states could provoke a NATO response. The Lisbon Declaration promotes the development of Allies' cyber defence capabilities and commits the alliance to assisting individual Allies, upon request, to optimise information-sharing, collaboration and interoperability

In June 2011, following on the Strategic Concept, NATO updated its "Policy on Cyber Defence" and also developed an evergreen "Cyber Defence Action Plan" (**both at TAB G**). These documents set forth the elements of the Alliance's cyber defence efforts for enhancing NATO's own cyber defence and security posture, as well as promote the cyber defence efforts of member states. and governance that will ." The Government of Canada was thoroughly consulted on the development of both the Policy and Action Plan on Cyber Defence.

STRATEGIC CONSIDERATIONS

NATO has become very engaged with cyber security issues. Its approach is broadly similar to that of the United States, in that it blurs the difference between civilian and military programs. The different Canadian approach means NATO will be a complement to other Canadian efforts rather than a primary venue. Several cyber programs under consideration at NATO, such as emergency management, incident response and information sharing, fall firmly within the mandate of Public Safety Canada.

It is also expected that issues may come up in your conversations with Alliance officials which, in a Canadian context, fall to the DND/CF or DFAIT.

There has been close coordination domestically between Public Safety Canada, DFAIT, and DND/CF on Canadian input to NATO cyber policy development, including in drafting the recent Strategic Concept. The two departments have also collaborated to support NATO incident management exercises. The Canadian separation of roles and responsibilities has not been an impediment, but NATO officials should be made aware that some aspects of cyber security programs and policy development, which they see as firmly within the 'military' sphere, are not seen that way in Canada, including critical infrastructure protection.

TALKING POINTS ARE ON FOLLOWING PAGE

Meeting on January 19, 2012, with Mr. Jamie Shea, Deputy Assistant Secretary General, Emerging Security Challenges, North Atlantic Treaty Organization and Officials from the NATO Cyber Incident Response Centre

TALKING POINTS

Learn about cyber security in the NATO context

- Questions of jurisdiction, whether in a federal context for Canada, or a national context for NATO, are a challenge in advancing cyber security. Has NATO had to deal with specific jurisdictional challenges with member states while working to further enhance cyber security? If so, what was the general approach in managing the varied roles and responsibilities of the jurisdictions involved?

- Public Safety Canada is exploring ways to clarify national responsibilities to manage cyber security incidents. I would be interested in hearing if NATO has any useful lessons learned with respect to defining responsibilities among a number of jurisdictions in managing cyber security incidents.

- My department coordinates federal efforts to discuss and establish cooperation mechanisms to enhance cyber security with the private sector in Canada. Could you give me a sense of what work the Emerging Security Challenges Division is undertaking to establish cyber defence mechanisms with private sector?

Learn about NATO's Cyber Defence Centre of Excellence

- In my discussions on cyber security I continue to hear the recurring themes of raising awareness, education, and information sharing. Does NATO work with member states to raise awareness among stakeholder and encourage information sharing and cooperation on cyber defence?

- I would like to hear more about how the NATO Cooperative Cyber Defence Centre of Excellence furthers the efforts of NATO and its member states to secure their networks and information systems.

Sensitize NATO to Canadian Roles and Responsibilities

- Like all of the Allies, we deal with issues in such a way that reflects our domestic legal and policy structures. Overall responsibility for cyber security in Canada rests with Public Safety Canada. My Department also manages many of the key cyber security program areas that NATO deals with such as emergency management, critical infrastructure protection, and incident response.

- I work very closely with my colleagues at the Department of Foreign Affairs and International Trade and Department of National Defence/Canadian Forces, who deal with some of the operational aspects of defending military networks, and could, potentially, be called upon to provide a military response to a cyber attack.

- For the moment, the bulk of our efforts in Canada are directed at supporting the programs and structures put in place under the Cyber Security Strategy we released in October 2010.

Implementation of *Canada's Cyber Security Strategy*: Roles and Responsibilities

- Public Safety Canada is leading the Government of Canada's efforts to enhance national cyber security posture. We lead federal engagement efforts with all stakeholders including other levels of government in Canada, critical infrastructure sectors, the private sector, and international partners.

- In addition, Public Safety Canada is leading the federal Government's outreach efforts to Canadians through a public awareness campaign and through the development of a website where Canadians can go for educational information on how to improve their personal cyber security.

- Public Safety Canada supports the work of the Department of National Defense and Canadian Forces on cyber security issues through exercises, lessons learned, and policy development. We also work closely with the Department of Foreign Affairs and International Trade on the foreign policy aspects of *Canada's Cyber Security Strategy*

- Our departments have a strong working relationship on security and defence issues and we look forward to continuing our engagement with NATO on cyber security and cyber defence issues.

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

Responsive Only

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

Jamie Shea

2010 -

Jamie Shea is Deputy Assistant Secretary General for Emerging Security Challenges

Personal

- Married, two children. Born 11 September 1953 in London (British citizen).

Previous NATO positions:

April 2003 - Aug. 2005	Deputy Assistant Secretary General for External Relations, Public Diplomacy Division
Oct. 2000 - Mar. 2003	Director of Information and Press
July 1993 - Sep. 2000	Spokesman of NATO and Deputy Director of Information and Press.
Jan. 1991 - July 1993	Deputy Head and Senior Planning Officer, Policy Planning Unit and Multilateral Affairs Section of the Political Directorate, NATO. Speechwriter to the Secretary General of NATO. Drafter of NATO Ministerial communiqués and policy planning of Ministerial meetings.
Nov. 1988 - Jan. 1991	Assistant to the Secretary General of NATO for Special Projects; most notably speechwriting, ghostwriting of articles, press releases, book chapters and official communiqués; advising Secretary General on political and military issues and on his public communications strategy.
Feb. 1985 - Nov. 1988	Head of External Relations Conferences and Seminars.
Sep. 1982 - Feb. 1985	Head of Youth Programmes.
Oct. 1980 - Sep. 1982	Administrator in Council Operations Section of Executive Secretariat.

Current external, academic positions:

- Professor, Collège d'Europe, Bruges

- Lecturer, Brussels School of International Studies, University of Kent
- Associate Professor of International Relations, American University, Washington DC; Director of the Brussels Overseas Study Programme
- Adjunct Associate Professor of International Relations, James Madison College, Michigan State University - Director of the MSU Summer School in Brussels.
- External Advisor, Post-graduate curriculum development, University of Sussex.
- Chair of Transatlantic Programme, Royal Holloway College, University of London.
- Member of the Academic Advisory Council, Vesalius College, Brussels

Other professional and academic pursuits:

- Regular lecturer and conference speaker on NATO and European security affairs and on public diplomacy and political communication and lobbying.
- Associate Editor, Europe's World, Brussels-based journal on international affairs.
- External examiner, candidates for PhD degree, London School of Economics, University of St Andrews, Department of War Studies, King's College, University of London, University of Kent, Canterbury and University of Iceland

Associations and memberships:

- Member of the Advisory Board, Security and Defence Programmes, Chatham House
- Member of the Policy Council, World Economic Forum, Geneva
- Founder and Member of Board, Security and Defence Agenda, Brussels
- Member of Advisory Council, European Policy Centre, Brussels
- Board Member, Geneva Centre for Security Policy
- External Associate, Centre for Defence and Security Studies, University of Manitoba, Winnipeg, Canada.
- Member of the Advisory Board, Centre d'Etudes et de Prospectives Stratégiques, Paris.
- Member of the Centre for European Policy Studies, Brussels.
- Associate Member, Institut Royal des Relations Internationales, Brussels.
- Member of the Advisory Council, Académie Diplomatique Internationale, Paris
- Member, Policy Forum, London
- Member of Advisory Board, Centre for Defence Studies, Tallinn, Estonia
- Member of the Advisory Board, LSE Ideas Transatlantic Project
- European Communicator of the Year (PR Week) 1999
- International Who's Who and Debretts Director of Public Figures.

Education:

- D.Phil. In Modern History from Oxford University (Lincoln College) 1981.
- Thesis: "European Intellectuals and the Great War 1914-1918".

- B.A. Hons. In Modern History and French from Sussex University 1977; First Class.

Lieutenant General Kurt Herrmann

Director, NCSA

Lieutenant General Kurt Herrmann was born in Wetzlar, Germany in 1950. He joined the German Air Force (GAF) in 1969 and was commissioned at the Air Force Officer School at Fürstenfeldbruck and Neubiberg (Bavaria) in March 1971. After pursuing an education in aeronautical and space engineering at the Air Force Technical Academy (later the Federal Armed Forces University, Munich), he studied computer science at the Technical University in Munich and received his diploma in 1977.

In early assignments he served as Technical Officer, Aircraft Electronics, for the F-104G "Starfighter" and as deputy squadron leader of the Electronics and Weapons Unit of a Fighter Bomber Wing. Later on, he became a Software Engineering Officer for the TORNADO PA-200.

Following a two-year course at the Federal Armed Forces Command and Staff College in Hamburg (1981-1983), he was assigned as squadron leader of a Phantom RF-4E electronics and reconnaissance systems unit (1983-1985), as ACOS Logistics, GAF Communications and Electronics Command (1985-1987), and as Assistant Branch Chief for Automated Data Processing as well as secretary of a study group for Command, Control and Information Systems in the Air Staff of the Federal Ministry of Defence (MOD, 1987-1990).

Further on, he served as General Staff Officer (Operations) in the "Forces Programmes Section" of the SHAPE Policy Division (1990 -1992) and as Assistant Branch Chief military-political affairs in Armed Forces Staff at the Federal MOD in Bonn (1993-1994). Promoted to the rank of Colonel he became the Commander of GAF Service Regiment 5 (1994-1996). Already in March 1996 he returned to the MOD and assumed the position of a Branch Chief for Strategic Optical and Radar Reconnaissance Systems at the Armed Force Staff Intelligence Division (1996-1998). During the whole period of this assignment, he also was the GAF Chief of Staff's representative for intelligence. Mid November 1998, he took up an assignment as the Deputy Commander and Chief of Staff, 1st GAF Air Division in Karlsruhe, holding this position until September 2000.

In October 2000, Lieutenant General Herrmann was appointed Inspector General, Air Force, at the GAF Office in Cologne. The following year, he was promoted to the rank of Brigadier General. In his second, dual hatted function as General GAF Concepts and Development he worked in close cooperation with the GAF Chief of Staff at the Federal MOD in Bonn.

In January 2002, he became the first commander of the German Armed Forces Joint Strategic Reconnaissance Command and occupied this position until the end of November 2004. From October 2004 until March 2005 Lieutenant General Herrmann studied the Russian Language at the Federal Foreign Language Training Centre in Hürth. Subsequently, by end of May 2005, he took over the position of Head NATO Military Liaison Mission (MLM) in Moscow, Russian Federation, then already promoted to the rank of Major General.

On return to Germany, Lieutenant General Herrmann assumed the position of the Deputy Commanding General of the German Joint Support Command in Cologne, on 1 July 2008. He was promoted to his current rank in April 2009. Lieutenant General Herrmann was awarded the German Federal Distinguished Service Medal and the Bundeswehr Cross of Honour in Gold. He is married to Ursula since 1972. They have two adult sons, both serving as officers in the German Air Force.

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

"Strategic Concept
For the Defence and Security of The Members of the North Atlantic Treaty Organisation"

Adopted by Heads of State and Government in Lisbon

Active Engagement, Modern Defence

Preface

We, the Heads of State and Government of the NATO nations, are determined that NATO will continue to play its unique and essential role in ensuring our common defence and security. This Strategic Concept will guide the next phase in NATO's evolution, so that it continues to be effective in a changing world, against new threats, with new capabilities and new partners:

- It reconfirms the bond between our nations to defend one another against attack, including against new threats to the safety of our citizens.
- It commits the Alliance to prevent crises, manage conflicts and stabilize post-conflict situations, including by working more closely with our international partners, most importantly the United Nations and the European Union.
- It offers our partners around the globe more political engagement with the Alliance, and a substantial role in shaping the NATO-led operations to which they contribute.
- It commits NATO to the goal of creating the conditions for a world without nuclear weapons – but reconfirms that, as long as there are nuclear weapons in the world, NATO will remain a nuclear Alliance.
- It restates our firm commitment to keep the door to NATO open to all European democracies that meet the standards of membership, because enlargement contributes to our goal of a Europe whole, free and at peace.
- It commits NATO to continuous reform towards a more effective, efficient and flexible Alliance, so that our taxpayers get the most security for the money they invest in defence.

The citizens of our countries rely on NATO to defend Allied nations, to deploy robust military forces where and when required for our security, and to help promote common security with our partners around the globe. While the world is changing, NATO's essential mission will remain the same: to ensure that the Alliance remains an unparalleled community of freedom, peace, security and shared values.

***

Core Tasks and Principles

1. NATO's fundamental and enduring purpose is to safeguard the freedom and security of all its members by political and military means. Today, the Alliance remains an essential source of stability in an unpredictable world.

2. NATO member states form a unique community of values, committed to the principles of individual liberty, democracy, human rights and the rule of law. The Alliance is firmly committed to the purposes and principles of the Charter of the United Nations, and to the Washington Treaty, which affirms the primary responsibility of the Security Council for the maintenance of international peace and security.

3. The political and military bonds between Europe and North America have been forged in NATO since the Alliance was founded in 1949; the transatlantic link remains as strong, and as important to the preservation of Euro-Atlantic peace and security, as ever. The security of NATO members on both sides of the Atlantic is indivisible. We will continue to defend it together, on the basis of solidarity, shared purpose and fair burden-sharing.

4. The modern security environment contains a broad and evolving set of challenges to the security of NATO's territory and populations. In order to assure their security, the Alliance must and will continue fulfilling effectively three essential core tasks, all of which contribute to safeguarding Alliance members, and always in accordance with international law:

    a. ***Collective defence***. NATO members will always assist each other against attack, in accordance with Article 5 of the Washington Treaty. That commitment remains firm and binding. NATO will deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole.
    b. ***Crisis management***. NATO has a unique and robust set of political and military capabilities to address the full spectrum of crises – before, during and after conflicts. NATO will actively employ an appropriate mix of those political and military tools to help manage developing crises that have the potential to affect Alliance security, before they escalate into conflicts; to stop ongoing conflicts where they affect Alliance security; and to help consolidate stability in post-conflict situations where that contributes to Euro-Atlantic security.
    c. ***Cooperative security***. The Alliance is affected by, and can affect, political and security developments beyond its borders. The Alliance will engage actively to enhance international security, through partnership with relevant countries and other international organisations; by contributing actively to arms control, non-

proliferation and disarmament; and by keeping the door to membership in the Alliance open to all European democracies that meet NATO's standards.

5. NATO remains the unique and essential transatlantic forum for consultations on all matters that affect the territorial integrity, political independence and security of its members, as set out in Article 4 of the Washington Treaty. Any security issue of interest to any Ally can be brought to the NATO table, to share information, exchange views and, where appropriate, forge common approaches.

6. In order to carry out the full range of NATO missions as effectively and efficiently as possible, Allies will engage in a continuous process of reform, modernisation and transformation.

The Security Environment

7. Today, the Euro-Atlantic area is at peace and the threat of a conventional attack against NATO territory is low. That is an historic success for the policies of robust defence, Euro-Atlantic integration and active partnership that have guided NATO for more than half a century.

8. However, the conventional threat cannot be ignored. Many regions and countries around the world are witnessing the acquisition of substantial, modern military capabilities with consequences for international stability and Euro-Atlantic security that are difficult to predict. This includes the proliferation of ballistic missiles, which poses a real and growing threat to the Euro-Atlantic area.

9. The proliferation of nuclear weapons and other weapons of mass destruction, and their means of delivery, threatens incalculable consequences for global stability and prosperity. During the next decade, proliferation will be most acute in some of the world's most volatile regions.

10. Terrorism poses a direct threat to the security of the citizens of NATO countries, and to international stability and prosperity more broadly. Extremist groups continue to spread to, and in, areas of strategic importance to the Alliance, and modern technology increases the threat and potential impact of terrorist attacks, in particular if terrorists were to acquire nuclear, chemical, biological or radiological capabilities.

11. Instability or conflict beyond NATO borders can directly threaten Alliance security, including by fostering extremism, terrorism, and trans-national illegal activities such as trafficking in arms, narcotics and people.

12. Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.

13. All countries are increasingly reliant on the vital communication, transport and transit routes on which international trade, energy security and prosperity depend. They require greater international efforts to ensure their resilience against attack or disruption. Some NATO countries will become more dependent on foreign energy suppliers and in some cases, on foreign energy supply and distribution networks for their energy needs. As a larger share of world consumption is transported across the globe, energy supplies are increasingly exposed to disruption.

14. A number of significant technology-related trends – including the development of laser weapons, electronic warfare and technologies that impede access to space – appear poised to have major global effects that will impact on NATO military planning and operations.

15. Key environmental and resource constraints, including health risks, climate change, water scarcity and increasing energy needs will further shape the future security environment in areas of concern to NATO and have the potential to significantly affect NATO planning and operations.

Defence and Deterrence

16. The greatest responsibility of the Alliance is to protect and defend our territory and our populations against attack, as set out in Article 5 of the Washington Treaty. The Alliance does not consider any country to be its adversary. However, no one should doubt NATO's resolve if the security of any of its members were to be threatened.

17. Deterrence, based on an appropriate mix of nuclear and conventional capabilities, remains a core element of our overall strategy. The circumstances in which any use of nuclear weapons might have to be contemplated are extremely remote. As long as nuclear weapons exist, NATO will remain a nuclear alliance.

18. The supreme guarantee of the security of the Allies is provided by the strategic nuclear forces of the Alliance, particularly those of the United States; the independent strategic nuclear forces of the United Kingdom and France, which have a deterrent role of their own, contribute to the overall deterrence and security of the Allies.

19. We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. Therefore, we will:

- maintain an appropriate mix of nuclear and conventional forces;
- maintain the ability to sustain concurrent major joint operations and several smaller operations for collective defence and crisis response, including at strategic distance;
- develop and maintain robust, mobile and deployable conventional forces to carry out both our Article 5 responsibilities and the Alliance's expeditionary operations, including with the NATO Response Force;
- carry out the necessary training, exercises, contingency planning and information exchange for assuring our defence against the full range of conventional and emerging security challenges, and provide appropriate visible assurance and reinforcement for all Allies;
- ensure the broadest possible participation of Allies in collective defence planning on nuclear roles, in peacetime basing of nuclear forces, and in command, control and consultation arrangements;
- develop the capability to defend our populations and territories against ballistic missile attack as a core element of our collective defence, which contributes to the indivisible security of the Alliance. We will actively seek cooperation on missile defence with Russia and other Euro-Atlantic partners;
- further develop NATO's capacity to defend against the threat of chemical, biological, radiological and nuclear weapons of mass destruction;
- develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations;
- enhance the capacity to detect and defend against international terrorism, including through enhanced analysis of the threat, more consultations with our partners, and the development of appropriate military capabilities, including to help train local forces to fight terrorism themselves;
- develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning;
- ensure that the Alliance is at the front edge in assessing the security impact of emerging technologies, and that military planning takes the potential threats into account;

- sustain the necessary levels of defence spending, so that our armed forces are sufficiently resourced;
- continue to review NATO's overall posture in deterring and defending against the full range of threats to the Alliance, taking into account changes to the evolving international security environment.

Security through Crisis Management

20. Crises and conflicts beyond NATO's borders can pose a direct threat to the security of Alliance territory and populations. NATO will therefore engage, where possible and when necessary, to prevent crises, manage crises, stabilize post-conflict situations and support reconstruction.

21. The lessons learned from NATO operations, in particular in Afghanistan and the Western Balkans, make it clear that a comprehensive political, civilian and military approach is necessary for effective crisis management. The Alliance will engage actively with other international actors before, during and after crises to encourage collaborative analysis, planning and conduct of activities on the ground, in order to maximise coherence and effectiveness of the overall international effort.

22. The best way to manage conflicts is to prevent them from happening. NATO will continually monitor and analyse the international environment to anticipate crises and, where appropriate, take active steps to prevent them from becoming larger conflicts.

23. Where conflict prevention proves unsuccessful, NATO will be prepared and capable to manage ongoing hostilities. NATO has unique conflict management capacities, including the unparalleled capability to deploy and sustain robust military forces in the field. NATO-led operations have demonstrated the indispensable contribution the Alliance can make to international conflict management efforts.

24. Even when conflict comes to an end, the international community must often provide continued support, to create the conditions for lasting stability. NATO will be prepared and capable to contribute to stabilisation and reconstruction, in close cooperation and consultation wherever possible with other relevant international actors.

25. To be effective across the crisis management spectrum, we will:

- enhance intelligence sharing within NATO, to better predict when crises might occur, and how they can best be prevented;

- further develop doctrine and military capabilities for expeditionary operations, including counterinsurgency, stabilization and reconstruction operations;
- form an appropriate but modest civilian crisis management capability to interface more effectively with civilian partners, building on the lessons learned from NATO-led operations. This capability may also be used to plan, employ and coordinate civilian activities until conditions allow for the transfer of those responsibilities and tasks to other actors;
- enhance integrated civilian-military planning throughout the crisis spectrum,
- develop the capability to train and develop local forces in crisis zones, so that local authorities are able, as quickly as possible, to maintain security without international assistance;
- identify and train civilian specialists from member states, made available for rapid deployment by Allies for selected missions, able to work alongside our military personnel and civilian specialists from partner countries and institutions;
- broaden and intensify the political consultations among Allies, and with partners, both on a regular basis and in dealing with all stages of a crisis – before, during and after.

Promoting International Security through Cooperation

Arms Control, Disarmament, and Non-Proliferation

26. NATO seeks its security at the lowest possible level of forces. Arms control, disarmament and non-proliferation contribute to peace, security and stability, and should ensure undiminished security for all Alliance members. We will continue to play our part in reinforcing arms control and in promoting disarmament of both conventional weapons and weapons of mass destruction, as well as non-proliferation efforts:

    - We are resolved to seek a safer world for all and to create the conditions for a world without nuclear weapons in accordance with the goals of the Nuclear Non-Proliferation Treaty, in a way that promotes international stability, and is based on the principle of undiminished security for all.
    - With the changes in the security environment since the end of the Cold War, we have dramatically reduced the number of nuclear weapons stationed in Europe and our reliance on nuclear weapons in NATO strategy. We will seek to create the conditions for further reductions in the future.
    - In any future reductions, our aim should be to seek Russian agreement to increase transparency on its nuclear weapons in Europe and relocate these weapons away from the territory of

NATO members. Any further steps must take into account the disparity with the greater Russian stockpiles of short-range nuclear weapons.

- We are committed to conventional arms control, which provides predictability, transparency and a means to keep armaments at the lowest possible level for stability. We will work to strengthen the conventional arms control regime in Europe on the basis of reciprocity, transparency and host-nation consent.
- We will explore ways for our political means and military capabilities to contribute to international efforts to fight proliferation.
- National decisions regarding arms control and disarmament may have an impact on the security of all Alliance members. We are committed to maintain, and develop as necessary, appropriate consultations among Allies on these issues.

Open Door

27. NATO's enlargement has contributed substantially to the security of Allies; the prospect of further enlargement and the spirit of cooperative security have advanced stability in Europe more broadly. Our goal of a Europe whole and free, and sharing common values, would be best served by the eventual integration of all European countries that so desire into Euro-Atlantic structures.

    - The door to NATO membership remains fully open to all European democracies which share the values of our Alliance, which are willing and able to assume the responsibilities and obligations of membership, and whose inclusion can contribute to common security and stability.

Partnerships

28. The promotion of Euro-Atlantic security is best assured through a wide network of partner relationships with countries and organisations around the globe. These partnerships make a concrete and valued contribution to the success of NATO's fundamental tasks.

29. Dialogue and cooperation with partners can make a concrete contribution to enhancing international security, to defending the values on which our Alliance is based, to NATO's operations, and to preparing interested nations for membership of NATO. These relationships will be based on reciprocity, mutual benefit and mutual respect.

30. We will enhance our partnerships through flexible formats that bring NATO and partners together – across and beyond existing frameworks:

    - We are prepared to develop political dialogue and practical cooperation with any nations and relevant organisations across the globe that share our interest in peaceful international relations.
    - We will be open to consultation with any partner country on security issues of common concern.
    - We will give our operational partners a structural role in shaping strategy and decisions on NATO-led missions to which they contribute.
    - We will further develop our existing partnerships while preserving their specificity.

31. Cooperation between NATO and the United Nations continues to make a substantial contribution to security in operations around the world. The Alliance aims to deepen political dialogue and practical cooperation with the UN, as set out in the UN-NATO Declaration signed in 2008, including through:
    - enhanced liaison between the two Headquarters;
    - more regular political consultation; and
    - enhanced practical cooperation in managing crises where both organisations are engaged.

32. An active and effective European Union contributes to the overall security of the Euro-Atlantic area. Therefore the EU is a unique and essential partner for NATO. The two organisations share a majority of members, and all members of both organisations share common values. NATO recognizes the importance of a stronger and more capable European defence. We welcome the entry into force of the Lisbon Treaty, which provides a framework for strengthening the EU's capacities to address common security challenges. Non-EU Allies make a significant contribution to these efforts. For the strategic partnership between NATO and the EU, their fullest involvement in these efforts is essential. NATO and the EU can and should play complementary and mutually reinforcing roles in supporting international peace and security. We are determined to make our contribution to create more favourable circumstances through which we will:

    - fully strengthen the strategic partnership with the EU, in the spirit of full mutual openness, transparency, complementarity and respect for the autonomy and institutional integrity of both organisations;
    - enhance our practical cooperation in operations throughout the crisis spectrum, from coordinated planning to mutual support in the field;
    - broaden our political consultations to include all issues of common concern, in order to share assessments and perspectives;
    - cooperate more fully in capability development, to minimise duplication and maximise cost-effectiveness.

33. NATO-Russia cooperation is of strategic importance as it contributes to creating a common space of peace, stability and security. NATO poses no threat to Russia. On the contrary: we want to see a true strategic partnership between NATO and Russia, and we will act accordingly, with the expectation of reciprocity from Russia.

34. The NATO-Russia relationship is based upon the goals, principles and commitments of the NATO-Russia Founding Act and the Rome Declaration, especially regarding the respect of democratic principles and the sovereignty, independence and territorial integrity of all states in the Euro-Atlantic area. Notwithstanding differences on particular issues, we remain convinced that the security of NATO and Russia is intertwined and that a strong and constructive partnership based on mutual confidence, transparency and predictability can best serve our security. We are determined to:

    - enhance the political consultations and practical cooperation with Russia in areas of shared interests, including missile defence, counter-terrorism, counter-narcotics, counter-piracy and the promotion of wider international security;
    - use the full potential of the NATO-Russia Council for dialogue and joint action with Russia.

35. The Euro-Atlantic Partnership Council and Partnership for Peace are central to our vision of Europe whole, free and in peace. We are firmly committed to the development of friendly and cooperative relations with all countries of the Mediterranean, and we intend to further develop the Mediterranean Dialogue in the coming years. We attach great importance to peace and stability in the Gulf region, and we intend to strengthen our cooperation in the Istanbul Cooperation Initiative. We will aim to:

    - enhance consultations and practical military cooperation with our partners in the Euro-Atlantic Partnership Council;
    - continue and develop the partnerships with Ukraine and Georgia within the NATO-Ukraine and NATO-Georgia Commissions, based on the NATO decision at the Bucharest summit 2008, and taking into account the Euro-Atlantic orientation or aspiration of each of the countries;
    - facilitate the Euro-Atlantic integration of the Western Balkans, with the aim to ensure lasting peace and stability based on democratic values, regional cooperation and good neighbourly relations;
    - deepen the cooperation with current members of the Mediterranean Dialogue and be open to the inclusion in the Mediterranean Dialogue of other countries of the region;
    - develop a deeper security partnership with our Gulf partners and remain ready to welcome new partners in the Istanbul Cooperation Initiative.

Reform and Transformation

36. Unique in history, NATO is a security Alliance that fields military forces able to operate together in any environment; that can control operations anywhere through its integrated military command structure; and that has at its disposal core capabilities that few Allies could afford individually.

37. NATO must have sufficient resources – financial, military and human – to carry out its missions, which are essential to the security of Alliance populations and territory. Those resources must, however, be used in the most efficient and effective way possible. We will:
    - maximise the deployability of our forces, and their capacity to sustain operations in the field, including by undertaking focused efforts to meet NATO's usability targets;
    - ensure the maximum coherence in defence planning, to reduce unnecessary duplication, and to focus our capability development on modern requirements;
    - develop and operate capabilities jointly, for reasons of cost-effectiveness and as a manifestation of solidarity;
    - preserve and strengthen the common capabilities, standards, structures and funding that bind us together;
    - engage in a process of continual reform, to streamline structures, improve working methods and maximise efficiency.

An Alliance for the 21st Century

38. We, the political leaders of NATO, are determined to continue renewal of our Alliance so that it is fit for purpose in addressing the 21st Century security challenges. We are firmly committed to preserve its effectiveness as the globe's most successful political-military Alliance. Our Alliance thrives as a source of hope because it is based on common values of individual liberty, democracy, human rights and the rule of law, and because our common essential and enduring purpose is to safeguard the freedom and security of its members. These values and objectives are universal and perpetual, and we are determined to defend them through unity, solidarity, strength and resolve.

Pages 661 to / à 676

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Meeting on January 19, 2012, with Mr. Yves Brodeur, Permanent Representative of Canada to the North Atlantic Council

ISSUE

- You may meet with Mr. Yves Brodeur, the Permanent Representative of Canada to the North Atlantic Council (**TAB C**), to discuss objectives in meeting with the North Atlantic Treaty Organization (NATO).

STRATEGIC OBJECTIVES

- Seek an assessment from the Ambassador of the political priority and sense of direction given to cyber security by NATO and its member states.

- Leave Canadian officials with a greater understanding of ongoing efforts to implement *Canada's Cyber Security Strategy*.

STRATEGIC CONSIDERATIONS

NATO continues to adapt to emerging threats to security and defence. At times the efforts of NATO to address emerging threats can venture into areas traditionally dealt with by public safety and emergency management organizations. Canada's approach to cyber security, as outlined in *Canada's Cyber Security Strategy*, will be managed differently from the current 'military' approach that NATO is undertaking. It will be important to highlight that emergency management, national incident response, and critical infrastructure protection all fall under the purview of Public Safety Canada. Critical Infrastructure Policy has provided background material regarding their engagement with NATO, should the Ambassador indicate an interest (**TAB B**).

As a courtesy to the Ambassador, you may want to outline the objectives for your meetings with NATO, which are:

- Obtain a greater understanding of how NATO works with member states on cyber defence. Lessons learned could inform Public Safety Canada's engagement.

- Obtain a greater understanding of the work of the NATO Cooperative Cyber Defence Centre of Excellence and NATO's efforts to establish cyber defence collaboration with the private sector.

- Sensitize NATO officials that in the Canadian context, cyber security is principally the responsibility of Public Safety Canada, and not the Department of National Defence/Canadian Forces (DND/CF).

- Identify some of the accomplishments of the Government of Canada's efforts in implementing *Canada's Cyber Security Strategy* (**TAB D – Backgrounder**).

TALKING POINTS ARE ON THE FOLLOWING PAGE

Meeting on January 19, 2012, with Mr. Yves Brodeur, Permanent Representative of Canada to the North Atlantic Council

TALKING POINTS

Possible questions to ask Mr. Brodeur

- What is your assessment of NATOs efforts in cyber security? Where do you see this effort going? Is this an issue you hear about from your colleagues?

- How is Canada perceived in this space by allies?

- What are NATO's expectations for partner countries? What does this mean for Canada?

- As you may know, emergency management, national incident response, critical infrastructure protection and public awareness all fall under the purview Public Safety Canada. Furthermore, *Canada's Cyber Security Strategy* focuses overwhelmingly on those issues, rather than on military aspects.

- The Canadian Cyber Incident Response Centre, which is housed within Public Safety Canada, acts as Canada's national CERT (Computer Emergency Readiness Team) in providing assistance and mitigation advice to domestic partners and coordinating the national response to any cyber security incident.

Objectives for the meeting with Mr. Shea and NCIRC

- As you know, I will be meeting with Mr. Jaime Shea, Deputy Assistant Secretary General for Emerging Security Challenges. My objectives for that meeting are to:

    - Obtain a greater understanding of how NATO works with member states on cyber defence. Lessons learned could inform Public Safety Canada's engagement with stakeholders.

    - Obtain a greater understanding of the work of the NATO Cooperative Cyber Defence Centre of Excellence and NATO's efforts to establish cyber defence collaboration with the private sector/

    - Sensitize NATO officials that in the Canadian context, cyber security is principally the responsibility of Public Safety Canada, and not the Department of National Defence/Canadian Forces (DND/CF).

    - Identify some of the accomplishments of the Government of Canada's efforts in implementing *Canada's Cyber Security Strategy*.

Yves Brodeur – Ambassador and Permanent Representative of Canada to the North Atlantic Council

Mr. Brodeur was born in Montréal in 1953. He joined the Department of External Affairs and International Trade in 1982 after completing his studies in Architecture at l'Université Laval in Québec and having worked in that field.

Mr. Brodeur served abroad as Second Secretary and Vice-Consul in Ankara from 1983 to 1985; First Secretary at the Organization for Economic Co-operation and Development (OECD) in Paris from 1989 to 1993; Counsellor (political) and Head of the Political Affairs Section at the Permanent Mission of Canada to the European Union in Brussels from 1996 to 2000; and Director of Communications and Spokesperson at the North Atlantic Treaty Organization (NATO) from 2001 to 2003. He served as Ambassador to the Republic of Turkey with accreditation to the Republic of Azerbaijan and the Republic of Georgia from 2005 to 2007.

In Ottawa, Mr. Brodeur served in the Media Relations Office from 1982 to 1983, as an analyst in the Political and Strategic Analysis Secretariat from 1985 to 1987, as well as in the South, South-East Asia Relations Division in 1987. From 1993 to 1995, he served at the Privy Council Office as Policy Advisor, Foreign Affairs and Defence. He was Chief of Staff to the Deputy Minister of Foreign Affairs from 1988 to 1989 and Departmental Spokesperson and Press Secretary to the Minister of Foreign Affairs from 1995 to 1996. He also served as Director of the Media Relations Office and from 2003 to 2005 was Director General of the Communications Bureau. He then served as Assistant Deputy Minister for the Afghanistan Task Force from October, 2007 to July 2009. Mr. Brodeur recently served as Assistant Deputy Minister of the International Security Branch and Political Director from August 2009 until his appointment to NATO.

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

Meeting on January 19, 2012, with Mr. Andrea Servida, Deputy Head of Unit, Information Society and Media Directorate General, and Mr. Stephen Purser, Head, Technical Competency Department, European Network and Information Security Agency

ISSUE

- On January 19, 2012, you will be meeting with Mr. Andrea Servida, Deputy Head of Unit, Cyber Security, Directorate General of Information Society and Media, and Mr. Stephen Purser, Head, Technical Competence Department, European Network and Information Security Agency. This meeting will provide an opportunity to tap into European experience and programs to help deliver on Canadian objectives for cyber security.

STRATEGIC OBJECTIVES

- Obtain a greater understanding of how the EU manages cyber security across multiple jurisdictions. This may inform how Public Safety Canada can assess different approaches to engage stakeholders.

- Obtain an understanding of how the European Commission and the European Network and Information Security Agency (ENISA) work together and with the private sector. This may offer lessons learned for Public Safety Canada to engage more effectively with domestic stakeholders.

- Leave counterparts with a greater understanding of the accomplishments achieved thus far in implementing *Canada's Cyber Security Strategy*.

- Indicate Canada's support of promoting norms in cyberspace and of European efforts to undertake cyber security awareness month.

BACKGROUND

To date, Canada has had only incidental contact with the European Union (EU) on cyber security. By contrast, the United States has established a strong transatlantic relationship and has even participated in joint exercises.

Typically within the EU, security and defence issues remain the purview of member states. However, with the broader economic and societal role of cyberspace, the EU has seen cyber security as a fundamental enabler of the common market and information society. The Directorate General of the Information Society and the Media responsible for managing European efforts to secure cyberspace; it reports to Ms. Neelie Kroes, the Commissioner for the Digital Agenda.

The overall aim of the EU's Digital Agenda is to deliver sustainable economic and social benefits from a digital single market based on fast Internet and interoperable applications. Online trust and security is the key to achieve this vision statement, as the EU recognizes that in order to realize social and economic benefits they need to ensure that consumer confidence in European networks and information systems remains high.

ENISA's mission is to deliver Network and Information Security within the EU. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of network and information security to benefit citizens, consumers, businesses and governments in the EU. It does this by helping the European Commission, Member States and the business community address, respond to and prevent network and information security problems. The Agency also provides technical guidance to the European Commission on developing European legislation in the field of network and information security.

It should be clearly noted that the Council of Europe (host body for the Budapest Convention on Cybercrime) is <u>not at all connected</u> to the EU, although it is often erroneously confused with the "Council of the European Union" or with the "European Council," both of which are EU organizations.

STRATEGIC CONSIDERATIONS

In November 2010, the United States and the EU established a cyber security working group which was tasked with:

- expanding incident management response capabilities jointly and globally,
- engaging the private sector by sharing good practices on collaboration with industry and pursuing specific engagement on key issue areas such as fighting botnets, securing industrial control systems, and enhancing the resilience and stability of the Internet;
- joint awareness raising activities, harmonizing messages across the Atlantic, as well as a developing a roadmap towards synchronised annual awareness efforts;
- continuing EU/U.S. cooperation to remove and block online child pornography;
- advancing the Council of Europe *Convention on Cybercrime*, including a programme to expand accession to all EU Member States, and a capacity-building program to assist states outside the region.

This working group also staged a joint EU-U.S. cyber incident management exercise in November 2011 to test for weaknesses in national and international responses. In line with these EU-U.S. efforts, ENISA has since published a feasibility study (**TAB E**) evaluating the merits of establishing a European "Cyber Security Awareness month". The report was quite positive and saw good potential for collaborating with the U.S. to leverage existing efforts.

International partners continue to seek Canada's ratification of the Council of Europe *Convention on Cybercrime* (Budapest Convention), which Canada signed in 2001. It is expected that officials from the European Commission will inquire as to what Canada's

intentions are with respect to the Budapest Convention. Although the current Government has indicated its desire to provide law enforcement agencies with the investigative tools required for modern technology, such legislation has not yet been introduced in the House of Commons, although it is expected to be soon.

ENISA recently issued a report entitle, *Cyber security: future challenges and opportunities* (**TAB F**). The report highlights key gaps ENISA needs to address to further secure international information and communication technology systems. These gaps include: threat identification, risk awareness, early warning and response, critical information infrastructure protection, consistent policy implementation, actions against cybercrime, international cooperation, and information exchange.

It would be informative to seek the views of your European colleagues as to whether their efforts to secure European information systems and networks could be applied more broadly around the world.

TALKING POINTS ARE ON THE FOLLOWING PAGE

Meeting on January 19, 2012, with Mr. Andrea Servida, Deputy Head of Unit, Information Society and Media Directorate General, and Mr. Stephen Purser, Head, Technical Competency Department, European Network and Information Security Agency

TALKING POINTS

- Public Safety Canada is the Government of Canada's lead department responsible for coordinating the implementation of *Canada's Cyber Security Strategy*.

- I understand that the ENISA provides technical guidance to support European efforts to enhance network and information security but I would like to better understand the relationship between your organizations.

- I would imagine that you face a number of challenges in working with national governments and private sectors that operate under different legal regimes. Has this hindered your ability to push jurisdictions to enhance cyber security? What mechanisms have you found work best in establishing partnerships with all of your various stakeholders?

- I would like to highlight that Public Safety Canada would be fully supportive of European efforts to establish a 'Cyber Security Awareness Month.' We feel that it would complement efforts in North America to reach out to the public and raise awareness of the threats and risks of online behaviour, but also to highlight ways in which the public can take steps to secure their online experiences.

- Have incidents in Europe, such as the DigiNotar event in the Netherlands, spurred greater political awareness in Europe on the importance of cyber security?

Andrea Servida

Deputy Head of Unit, European Commission, Information Society and Media Directorate General

He has joined the European Commission in 1993 and in January 2006 he became Deputy Head of the Unit "Internet; Network and Information Security" in the Information Society and Media Directorate-General. Besides co-managing the Unit, whose competences span from Internet governance to ".eu", he is in charge of defining and implementing the strategy and policy on network and information security, which includes the activity on critical information infrastructure protection.

He also contributes to the Commission policy-making activities in electronic signature, privacy & data protection and cyber-crime. Until 2005, he has worked in the Information Society Technologies Thematic Priority of FP6 with management responsibilities for the research activities on security and dependability technologies and applications.

In the 5th Framework Programme, he has been in charge of shaping up and co-ordinating at the Programme level the initiative on Dependability in Information Society (called DEPPY), including the preparation and management of related Cross Programme Actions calls for proposals and evaluation. This initiative focused on large scale information infrastructures and on extensively deployed networked embedded systems.

Before joining the European Commission he has worked in industry for nearly eight years as a project manager of a number of international R&D projects on decision support systems for environmental, civil and industrial emergency and risk management. He graduated with Laude in Nuclear Engineering at Politecnico di Milano and carried out PhD studies on fuzzy sets and artificial intelligence at Queen Mary and Westfield College, University of London.

Pages 688 to / à 691

are withheld pursuant to section

sont retenues en vertu de l'article

19(1)

of the Access to Information

de la Loi sur l'accès à l'information

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

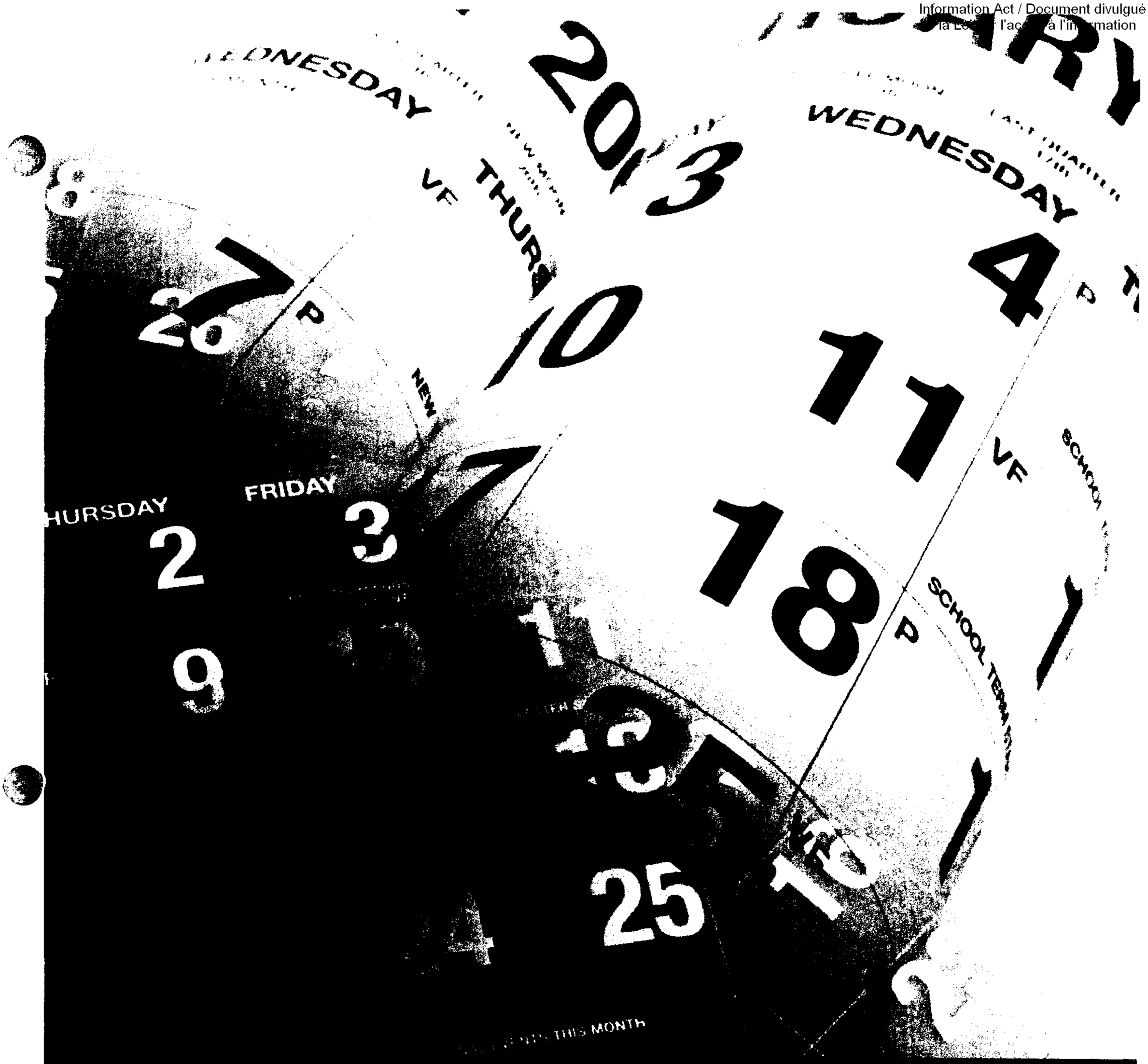
- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.



European Month of Network and Information Security for All – *A feasibility study*

November 2011

enisa
European Network and Information Security Agency

1. Executive summary

As part of its ongoing awareness raising mission, ENISA assesses the establishment and organisation of a European Month of Network and Information Security for All.

This concept was inspired by similar projects that have been held successfully in other places around the world for some years now. ENISA suggests that this project will significantly raise the awareness of EU citizens on Network and Information Security (NIS) issues. The particularities of the European territory compared to other areas of the world indicate that a significant amount of effort will be required in order for this idea to deliver its full potential across Europe. To this effect, one of the most critical elements for the success of this activity is to develop an effective structure and coordination scheme among participating entities.

This year, ENISA has been asked to assess the feasibility and explore various options on how such a campaign can become an effective instrument to raising awareness about NIS challenges and in particular:

- generate awareness about NIS,
- achieve long-lasting behavioural change,
- modify perception of risks,
- involve relevant stakeholders,
- disseminate security-relevant information.

To this end, a virtual working group was created to:

- gather information with regard to Member States' experiences on organising national security events held for one or more days or an entire week;
- compile these results and produce a European overview (as-is);
- assess feasibility by developing a coordination scheme and model;
- identify and eventually develop awareness material to be used during such a campaign.

The following did not qualify to be included in this analysis:

- any event organised under Safer Internet Day;
- programmes funded by the Structural Funds of the European Union and/or the European Commission;
- any event organised within an international project or international commemoration (e.g. International Youth Day);
- any conference, summit or forum organised for professionals only.

The report covers two main parts:

- the overview of the security-related days/weeks currently organised at national level across Europe;
- the organisational insights and patterns for delivering a European Month of Network and Information Security for All on annual basis.

The first part of the study looks at the current state of play in Europe. The main findings are:

- half of the Member States hold either a security day(s) or week(s);
- the majority focus was around security week(s) rather than day(s);
- the proportion of campaigns encompassing general users versus those targeting business users is almost the same;
- a wide variety of key messages are promoted across the different European countries;
- most of the events are organised in October and November, although many are organised in February and April;
- all supporting material and communication is produced in the official language of the countries concerned;
- printed materials (41 %) and electronic messages (36 %) are featured in many cases;
- websites are the most prominent channels of communication used (12 out of 15 Member States);
- all Member States used a variety of techniques that were fun, exciting and motivating;
- the public sector has been involved in the organisation of all the events that have been reviewed;
- messages should be tailored specifically to the audience and each intermediary;
- the wide variety of delivery channels used clearly demonstrates that there is no particular delivery method that has proven to be successful across all sectors and countries;

- the use of websites as a communication vehicle is followed by the use of magazines, brochures, documents, annual reports and other printed material (seven Member States) and events and meetings (seven Member States). Video clips and TV/radio/webcasts are two other common delivery channels.

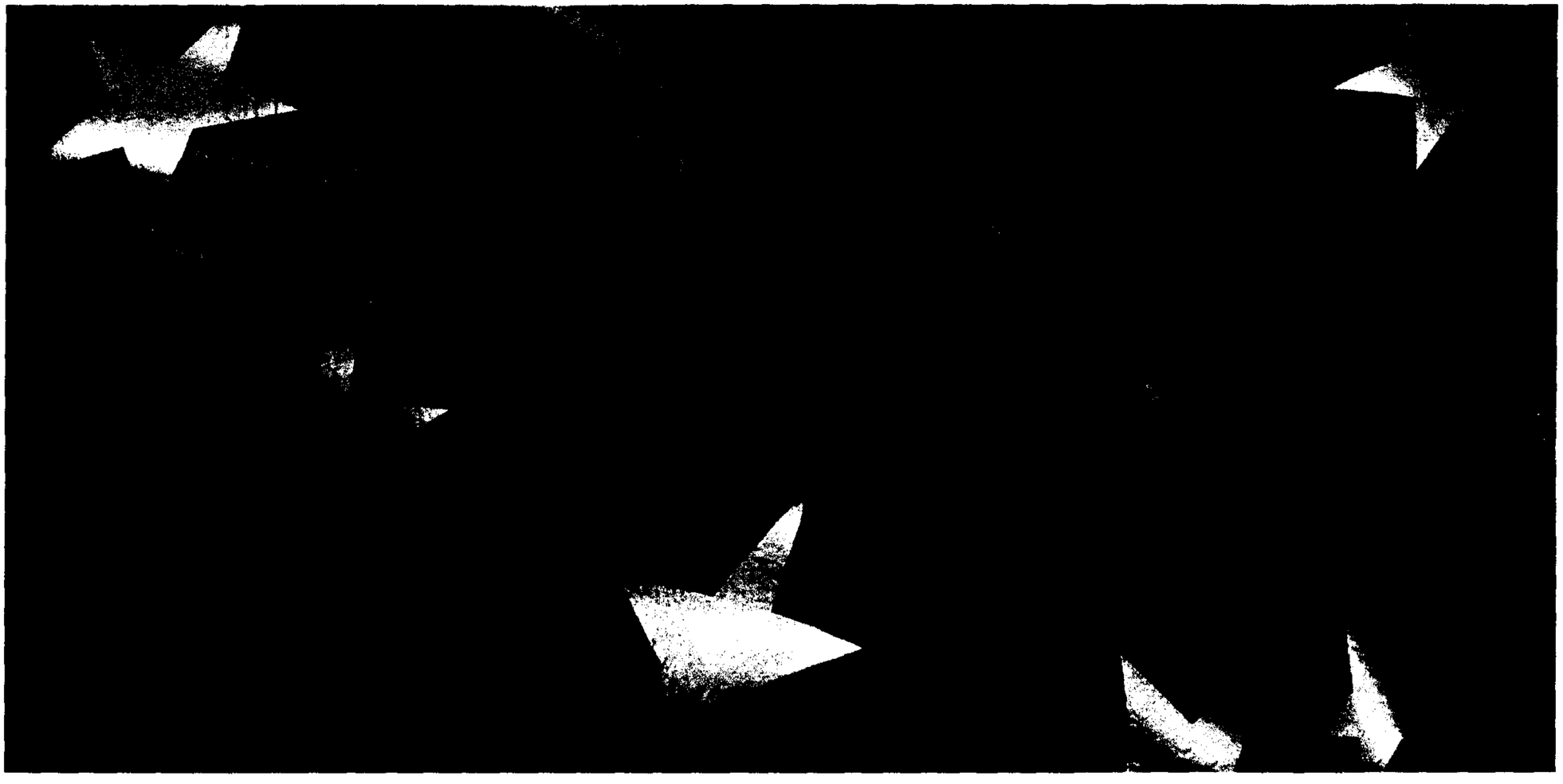
The second part assesses the feasibility of delivering the European Month of Network and Information Security for All. The main findings are:

- leveraging on European and worldwide experiences would be essential – in particular Insafe could provide useful information of the success and challenges their previous campaigns and competitions have encountered;
- the implementation in coordination with the United States, where the cybersecurity month is established, is a supplemental model to jump-start the activities in Europe;
- engaging with relevant parties such as Member States and intermediaries is one of the most critical elements of this project;
- the involvement of the private sector would be required in order to deliver the full potential of this idea;
- an aim should be to broaden the scope of national security events to make them a solely international event;
- using appropriate communication channels and vocabulary will be critical for addressing multicultural aspects;
- branding will be key for the success of the 'European security month';
- a roadmap will be needed to provide a mechanism to help forecast developments and a framework to help plan and coordinate these developments. Member States might consider implementing one or more identified activities according to the level of engagement and information security awareness maturity of their country;
- alternative methods to jump-start the 'European security month' have been identified;
- one method appears to meet most of the requirements in relation to the organisation of a yearly security month across Europe. This method foresees three different phases: the production of a feasibility study; various activities and options of involvement and engagement of actors at national, European and global level; the implementation of a 'European security month' in all EU countries. The main features are:
  - the number and type of actors involved simultaneously;
  - the different type of proposed activities;
  - the various options of involvement and engagement open to the actors;
  - the timeframe foreseen for implementing coordinated annual awareness efforts.
- a structure would be essential to coordinate such a campaign across all Member States; the general principle of subsidiarity would apply;
- a decision-maker and someone to undertake the planning is essential, as well as national groups which should work to implement the 'European security month' activities at national level.

The analysis carried out in the study lead to the conclusion that organising a European Month of Network and Information Security for All is feasible especially because of the existing good practices and experiences of the Member States. This will be an annual activity, conducted in collaboration with the Member States and featuring a variety of national/European cybersecurity awareness raising initiatives and competitions.

Cyber security: future challenges and opportunities

enisa
European Network and Information Security Agency



Cyber security: future challenges and opportunities

Authors:
Prof. Udo Helmbrecht
Dr. Steve Purser
Maj. Ritter Kjejnstrup

Contact details
For contacting ENISA or for general enquiries about this publication, please use the following details:
E-mail: info@enisa.europa.eu
Internet: http://www.enisa.europa.eu

Contents

Executive Summary ____ 4
Introduction ____ 6
The Evolving Threat Landscape ____ 8
Mitigating the Threats – A Fragmented Approach ____ 12
Ensuring a Coherent Pan-European Approach ____ 14
ENISA's Role ____ 16
- Identification and analysis of emerging trends and threats 17
- Awareness of NIS risks and challenges 18
- Early warning and response 18
  - Early warning 18
  - CERTs in Europe 19
  - CERT for EU institutions 19
- Critical Information Infrastructure Protection 20
  - *Cyber exercises* 20
- Adequate and consistent policy implementation 21
- Supporting the community in the fight against cybercrime 22
  - Cybercrime centre 22
- International cooperation 23
- *Information exchange* 24
- Building communities 24
- The future 25

Conclusion ____ 26

Executive Summary

Our society has become irreversibly dependent on Information and Communication Technologies (ICTs). Unfortunately, whilst these technologies have brought many benefits, the increased adoption of them has also been accompanied by the development of a new set of cyber threats which are developing in ever more rapid, sophisticated and sinister ways.

This means that the protection of critical infrastructure, and the applications that run on top of it, is not just about technology and security, it is closely connected to the European Union's competitiveness and prosperity.

Any future approach to securing Europe's ICT systems must be coherent across geographical borders and pursued with consistency over time. This is not the case at the present time, where different approaches to securing information and systems are developed independently in different Member States and in different communities. However, without a coordinated global approach to major incidents on the internet, Member States could find themselves in a situation where local systems cannot function correctly due to issues that are outside their control.

ENISA believes international coordination is essential to achieve a holistic approach to network and information security. This includes cooperation throughout Europe as well as worldwide in both the public and private sectors. In many ways, it is this global dimension that distinguishes cyber security from what we have referred to in the past as information security.

The EU institutions and bodies should provide the support and the framework for Member States to achieve a coordinated global approach.

One of ENISA's tasks is to bridge the gap between policy and operational requirements; it does so by being an impartial European platform for information sharing amongst EU Member States, and also globally.

The main contributions of ENISA to enhancing cyber security are in the following areas:

- *Identification and analysis of emerging trends and threats*
- *Awareness of network and information security risks and challenges*
- *Early warning and response*
- *Critical information infrastructure protection*
- *Adequate and consistent policy implementation*
- *Actions against cybercrime*
- *International cooperation*
- *Information exchange*
- *Building communities*

There are a number of areas where the current approach to improving cyber security in the EU could sensibly be extended. For example, there is a clear need to collect and analyse data relating to information security in a cross-border context which could reveal trends that are not visible at present. Also, the coming into force of the Lisbon Treaty is an opportunity to improve the level of dialogue between communities in the area of network and information security. A proactive approach to building these new cross-border communities will bring great benefits both in terms of the effectiveness of its approach and efficiency in use of its resources.

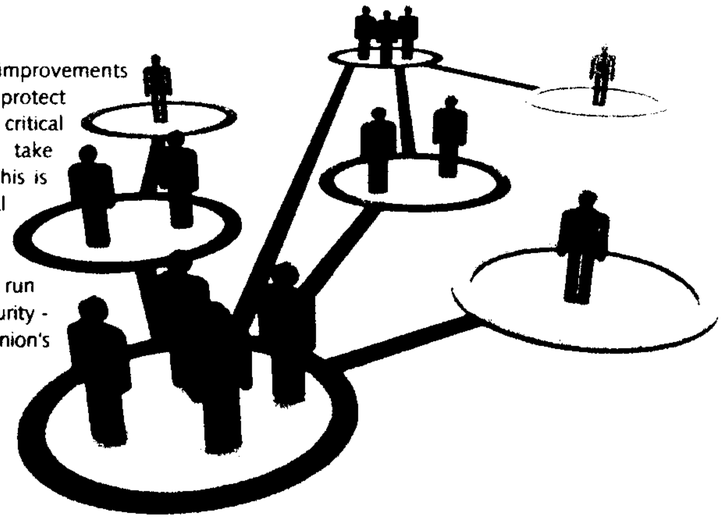
It is important that our efforts to protect and facilitate the development and prosperity of the European Information Society do not lose momentum. These efforts are addressed on many fronts with multiple stakeholders – all are increasing in numbers and scope along with the pervasiveness and economic importance of ICTs. It is important that ENISA is modernised and further developed to allow the Agency to respond to these changes and provide support and expertise for stakeholders across Europe.

Introduction

Information and Communication Technologies (ICTs) have become the backbone of our economy and society. In today's world, geographically separated societies are interconnected by information technology – and are irreversibly dependent on it. Unfortunately, whilst it has brought many benefits, the increased adoption of information technology has also been accompanied by the development of a new set of threats. These threats reflect the global nature of the systems they target and their mitigation often requires international collaboration. In many ways, it is this global dimension that distinguishes cyber security from what we have referred to in the past as information security. The propagation and implications of threats such as malware (and botnets in particular) mean they are no longer just an issue for people to deal with individually, but are increasingly a social and civic responsibility.

European Commission Vice President Neelie Kroes has put forward the Digital Agenda for Europe, with the objective of improving the quality of life through, for example, better health care, safer and more efficient transport solutions, a cleaner environment, new media opportunities and easier access to public services and cultural content.[1] This is a major step towards the creation of the Digital Society. However, cyber-attacks complicate the deployment of ICT solutions used by citizens in their day-to-day lives, such as online payment and e-government services. ICT is increasingly used in crime and politically motivated attacks. For example Germany saw an increase of 8.1% in criminal acts associated with the internet during 2010, as noted by the German Minister of the Interior.[2]

To fully achieve the potential for improvements through ICTs, it is necessary to better protect citizens, businesses, governments and critical infrastructure from criminals who take advantage of modern technologies. This is also recognised in both the Digital Agenda and the Internal Security Strategy.[3] The protection of critical infrastructure, and the applications that run on top of it,[4] is not just about cyber security - it is closely connected to the European Union's competitiveness and prosperity.



1 COM(2010) 245 final/2
2 http://www.dw-world.de/dw/article/0,,15093336,00.html
3 COM(2010) 673 final
4 An insecure application running on secure infrastructure is still insecure. A secure application running on insecure infrastructure can still be secure as long as we can ensure availability and performance

The Evolving Threat Landscape

The development of information technology in the past 40 years has been rapid. However, it is not only ICT that has developed and become increasingly pervasive, so have the threats against it.

This is a major challenge for all of those involved in securing the European information society and protecting European citizens and their fundamental rights. Not only are new technologies and business models continuously being introduced, the use of old technologies is being extended in ways that were never envisaged when they were first developed. A good example of this is SCADA[5] industrial control systems, which were initially designed to be independent without connectivity to other systems, but are now increasingly being connected to the internet. SCADA systems were targeted in the Stuxnet[6] attack which is described below.

At the same time, new business models seriously push existing concepts and regulation to their limits. Cloud computing and other technologies where data is decentralised and spread out over virtual and physical locations is a prime example. Our concepts of data, data protection and data sharing are often difficult to apply in these settings, which is problematic given the rate of uptake of these new technologies. An illustrative example of this is the difficulty experienced by a Danish municipality in rolling out Google Apps[7] to teachers. The Danish Data Protection Agency challenged the municipality's initial assessment that confidential and sensitive data about students and parents can be processed in Google Apps. Among other issues, the Data Protection Agency had concerns about the physical location of data as well as the municipality's ability to maintain control with the cloud solution provider (Google).[8] In this case there is a potential conflict between the benefits of the new business model, such as economies of scale and standardized services, and the possible negative impact on citizens' rights to privacy and data protection. ENISA is currently looking at the use of such new technologies. The Agency has highlighted some of the possible risks and provided guidance on how these risks could be mitigated. As part of their recommendations to the municipality, the Danish Data Protection Agency recommends the use of ENISA's cloud security risk assessment.[9]

As well as issues created by the fast pace of development, we are faced with deliberate attempts to cause harm. These include increasingly complex attacks, which may benefit from the backing of rogue states and organised crime, such as for example the Stuxnet attack. This, and four other recent attacks, are described below. Each of them highlights different aspects of the types of threats we are facing and their consequences. They all illustrate the seriousness and global dimension of network and information security (NIS) issues.

- *Stuxnet: malware which targets industrial software at, for example, nuclear facilities. It was specially created to attack the SCADA systems that these facilities use. Developing Stuxnet required special knowledge of the control systems as well as substantial resources to develop. Thus we have highly capable and resourceful attackers that go after critical infrastructure. The major concern about Stuxnet however is not the technical mechanisms that the software implements, but the fact that the target has changed – the ability to interrupt or modify the operations of industrial control systems could result in the loss of life.*

5 http://en.wikipedia.org/wiki/SCADA
6 http://en.wikipedia.org/wiki/Stuxnet
7 http://en.wikipedia.org/wiki/Google_Apps
8 http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/
9 http://www.enisa.europa.eu/act/application-security/rm/files/deliverables/cloud-computing-risk-assessment

- *Since 2008 the EU Emission Trading Scheme has been the subject of several attacks. At the beginning of January 2011 close to 30 million euro-worth of emissions allowances were stolen from the national registries.*[10] *This was a cross-border attack with serious financial impact.*

- *In March 2011, the security firm RSA*[11] *issued a statement that there had been an attack against their infrastructure which they categorised as an Advanced Persistent Threat (APT). This means that for some time they had been under a sophisticated attack which seems to have had the purpose of extracting specific information on their SecurID two-factor authentication products, probably as preparation for future attacks.*

- *In April 2011, Sony's online gaming platform, the PlayStation Network, was taken offline after it was attacked and information about more than 100 million users was stolen.*[12] *It is still not known how much the attack will cost Sony, but it is likely to be considerable and one estimate is as high as $2 billion.*[13] *This shows how an attack on one company can seriously affect and undermine the trust of users across the globe. More generally, it illustrates how attacks can affect entire businesses.*

- *Diginotar, an SSL certificate authority, recently suffered a cyber-attack which has led to its subsequent bankruptcy. Fox IT reports that the first traces of the cyber-attack date from the 17th of June 2011. The attacker was able to create fraudulent SSL certificates for hundreds of sites, including Google and Skype. Fake SSL certificates can be used to intercept encrypted web browsing, machine-to-machine communications (web services) and to fake electronic signatures. DNSSEC also relies on SSL certificates to validate the link between IP addresses and domain names.*

(footnote: http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html)

Of course, it is not only threats that are evolving. The countermeasures to tackle them have also changed. These developments include improvements to networking best practices; more focused policies, regulations and directives; increased insight into multi-sector implications of security issues; and the recognition of the importance of having a global perspective on NIS. It is important to maintain and adapt these efforts to improve NIS to keep pace with the continuous evolution and increasing pervasiveness of ICTs.

10 http://en.wikipedia.org/wiki/European_Union_Emission_Trading_Scheme
11 http://www.rsa.com/node.aspx?id=3872
12 http://www.ft.com/cms/s/2/e13be04a-80af-11e0-85a4-00144feabdc0.html#axzz1MiIfb8HH
13 http://www.reuters.com/article/2011/05/05/us-sony-insurance-idUSTRE74472120110505

Mitigating the Threats - A Fragmented Approach

Despite the above mentioned improvements, it is essential to achieve a holistic approach to cyber security, including cybercrime, on a pan-European level. Much of the current debate (and flow of information) on cyber security is taking place within specialised communities. Military communities are discussing subjects such as cyber war and cyber-defence; law and enforcement communities are analysing threats and solutions related to cybercrime; and intelligence communities are concerned with cyber espionage. In the information society, we are concerned with the way in which new threats affect infrastructure, applications and data related to internal market activities, both within the public and private sectors.

This document adopts the following classification of areas that are typically considered to fall into the general category of cyber security:

Cybercrime: Criminality is on a new scale on the internet. In conventional crime the perpetrator has to be at the scene of the crime. In a bank robbery he has to enter the bank. On the internet the time and place of the crime are not dependent on each other. If I am phishing, I can take money illegally from a person's bank account at any place in the world and at any time. This also means that I may find myself in different legal systems. It may be impossible for the prosecution authorities in country A to arrest a criminal in country B.

Cybercrime often also allows organised crime to scale up its illegal operations.

Cyber espionage: Espionage has been around for a long time and will continue to be present as long as there are national state interests and intelligence services.

However, whereas in the past the spy had to run the risk of having his cover blown at the crime scene, today he can spy unseen from afar using technology (for example Trojan horses[14]).

Cyber security: This refers to the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment.

Cyber warfare: In the past, troops from opposing countries confronted each other on a battlefield, and "rules" for warfare were written if not always followed. The Geneva Convention,[15] for example, describes rules for the protection of people who do not take part in the fighting.

Outside these rules, terrorist organisations seek to achieve mainly political aims by operations which, under state legislation, are assessed as criminal acts.

With internet technology it is possible for an individual, group or state to carry out remotely controlled, often covert, cyber attacks on critical infrastructures[16] of a state. Therefore the line between soldier, terrorist and criminal becomes blurred.

These terms are not mutually independent and there are many overlaps of scope when discussions take place, especially at a more detailed level, where similar issues and problems are discussed by many communities in both the public and private sectors. Unfortunately, information and experiences are often not shared across communities. This represents a significant challenge for Europe over the next decade and can also be seen as an opportunity. A truly effective approach to dealing with the issues underlying all these related areas will require close collaboration between different communities and a corresponding alignment of approaches.

Finally, our efforts to protect the European information society must not be restricted by definitions of words and artificial barriers to communications, which our adversaries are not subject to - and which they may actually benefit from if our responses are not coordinated across sectors and national borders.

14 http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
15 http://en.wikipedia.org/wiki/Geneva_convention
16 http://en.wikipedia.org/wiki/Critical_infrastructure

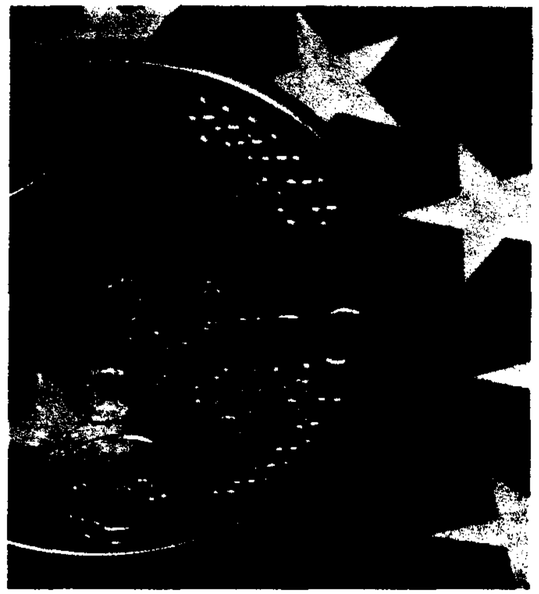
Ensuring a Coherent Pan-European Approach

Any future approach to securing Europe's ICT systems must be coherent across geographical borders and pursued with consistency over time. This is not the case at the present time, where different approaches to securing information and systems are developed independently in different Member States and in different communities. In such an environment, the principle of the weakest link applies; for example weaknesses in one Member State could easily be used to compromise other Member States. Thus, in a global networked environment, there will only be an optimal response if issues that transcend national boundaries are managed and controlled correctly. Without a coordinated global approach to major incidents on the internet, Member States could find themselves in a situation where local systems cannot function correctly due to issues that are outside their control.

At a more technical level, there is evidence that the approaches we have defined to date need to be improved. As an example, it is clear that it makes little sense to separate the protection of infrastructure from the applications which run on top of it. Those who choose to attack systems do not make the distinction between the two – they simply exploit the weakest link. For example, with botnets[17] home users' computers can be infected with malicious software, such as a Trojan horse.[18] The computers can then be remotely controlled to attack governmental websites and online services. An example of this was seen in the 2007 cyber-attacks against Estonia.[19]

The EU institutions should provide the support and the framework for Member States to achieve a coordinated global approach. These efforts to improve NIS must involve the private sector: as users of ICTs, as implementers of ICT based business models, as producers of technologies and as operators of services and infrastructure. Last but not least, citizens must be involved and not left to fend for themselves.

17 http://en.wikipedia.org/wiki/Botnet
18 http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
19 http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia



ENISA's Role

ENISA is working together with the Member States to secure Europe's information society. A significant part of this effort is concerned with protecting our infrastructure and applications, and ensuring that we are prepared for incidents when they do happen by reinforcing incident response capabilities across Europe. The focus of ENISA is on cross-border issues, helping Member States to identify dependencies and to decide on the most appropriate way to deal with them.

The Agency achieves this in a number of different ways. By acting as a neutral European platform for information sharing - and for establishing and maintaining networks and communities - we promote dialogue and help Member States to align their approaches to specific issues. This role is also important in a more general context where ENISA facilitates dialogue between European actors and their international counterparts.

The Agency also provides expertise and advice to a variety of stakeholders, particularly in the area of development and implementation of standards and good practices. As such, the Agency plays an important role in bridging the gap between policy and operational requirements. Finally, we are active in the area of risk assessment and management, particularly where emerging threats are concerned.

Where cyber security is concerned, the main contribution of ENISA is in the following areas:

- *Identification and analysis of emerging trends and threats*
- *Awareness of NIS risks and challenges*
- *Early warning and response*
- *Critical information infrastructure protection*
- *Supporting the international CERT community*
- *Adequate and consistent policy implementation*
- *Actions against cybercrime*
- *International cooperation*
- *Information exchange*
- *Building communities*

Identification and analysis of emerging trends and threats

These are explored in more detail below.

On the one hand we are increasingly aware of how sensitive and how vulnerable to attack our IT infrastructures are and on the other hand we lack adequate information by which to be able to recognise and react to dangers in due time. An example of this is botnets.[20] This is a very complex problem to solve because there are so many parties involved – the owners of infected PCs, ISPs, the victims of extortion or click fraud[21], law enforcement, software vendors etc. To make the most of the limited funds available for fighting botnets it is essential to have accurate assessments of the relative size and impact of different botnets. However, the current estimates of the extent of infected machines and botnet activities vary wildly by up to a factor of seven.[22] More generally, we need to move from a situation in which we are making decisions based on information about attacks to a situation in which we are able to refer to discrete data.

ENISA can support the European Commission and Member States by providing them with information on trends, emerging threats and by providing guidance on risk management and appropriate preventative and response measures. For example, ENISA has produced a report on Botnets entitled "Botnets: Measurement, Detection, Disinfection and Defence" which is a comprehensive report on how to assess botnet threats and how to neutralise them.[23] At the moment ENISA does not collect and analyse data on cyber-attacks. However, this could be useful as it would enable ENISA to identify pan-European trends and to report these back to the Member States. ENISA can also facilitate dialogue on NIS across communities and with different international counterparts. We believe that this dialogue is a critical precursor to any long-term action plan for protecting information services that benefit EU citizens.

20 http://en.wikipedia.org/wiki/Botnets
21 http://en.wikipedia.org/wiki/Click_fraud
22 http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence
23 Ibid

Awareness of NIS risks and challenges

Much of the work that ENISA carries out on a daily basis can be considered as awareness raising. Most of this activity is directly associated with the different work packages that constitute ENISA's annual work programme. For instance, we are examining whether the Computer Emergency Response Team (CERT) community could function as a channel for communicating with businesses and citizens across Europe about NIS issues.

In addition to this ongoing effort, the Agency undertakes specific projects that are concerned with awareness raising as an activity its own right. At present, the Agency is exploring the possibility of a European Cyber Security Awareness Month, which would bring stakeholders together to support and reinforce NIS awareness across Europe. In parallel, we are also working together with certain Member States to see to what extent it is possible to introduce the basic elements of information security into the school curriculum. Achieving this vision would put Europe amongst the leaders in terms of correctly preparing the next generation for dealing with the cyber security issues of tomorrow.

Early warning and response

Early warning

It is critical to have a proactive approach to threats in order to be able to anticipate, counter and attribute them. This approach much be a collaborative effort and cannot be limited only to the boundaries of an industry or of a country. Information collection on attacks, techniques, methods and vulnerabilities needs to be constant and vigilant. ENISA has devised a high-level roadmap for a development of a European Information Sharing and Alert System (EISAS).[24] The Agency has the expertise to support the Member States in implementing it and developing the interoperability services enabling national Information Sharing and Alert Systems (ISAS) to be functionally integrated into EISAS.

CERTs in Europe

Since 2005 ENISA has run a programme dedicated to reinforcing national and governmental CERTs. The goals of this programme are to support the EU Member States in establishing and developing their national and governmental CERTs according to an agreed baseline set of capabilities, and to generally support and reinforce CERT cooperation by making available good practice.

ENISA seeks to reinforce this type of cooperation by analysing barriers to cross-border cooperation and proposing measures to tackle them. The ultimate goal of these activities is to help CERTs to improve the effectiveness and the efficiency of their response mechanisms, particularly where cross-border incidents are concerned.

A recent development here is the work that ENISA is doing to facilitate dialogue between CERTs and other communities such as law enforcement, which is important for the fight against cybercrime. As part of this work, the Agency is currently exploring ways in which we can collaborate with Europol.

CERT for EU institutions

The Digital Agenda for Europe[25] is a flagship initiative under the EU 2020 Strategy.[26] Key Action 6 of the Agenda is to: "Present in 2010 measures aimed at a reinforced and high level Network and Information Security Policy."[27] One of the measures identified is the implementation of a CERT for the EU institutions.

A CERT for the EU institutions will deliver strong value as it would, among other things; increase protection against attacks and facilitate swifter reaction to threats; ensure efficiency through shared resources; protect EU competitiveness; and be consistent with EU policy.

24 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/?searchterm=eisas
25 http://ec.europa.eu/information_society/digital-agenda/index_en.htm
26 http://ec.europa.eu/europe2020/index_en.htm
27 COM(2010) 245 final/2

ENISA, in its position as an independent, experienced and – above all other things – trusted body in Europe is uniquely positioned to play the key role in the coordination of the incident response capabilities of the European institutions.

The first steps towards establishing such a CERT have already been taken by the setting up of a pre-configuration team in the summer of 2011.[28] ENISA is supporting the establishment of the EU institutional CERT and has representatives both within the pre-configuration team and the steering committee.

Critical Information Infrastructure Protection

As the communication on Critical Information Infrastructure Protection (CIIP) 'Achievements and next steps: towards global cyber-security' shows, we have, on a pan-European level, already made several important first steps to improve our cyber security. ENISA is facilitating much of this activity, and will continue to do so. In the future, we hope to increase our contribution on the basis of the new mandate for the Agency because, as the communication recognises, "strengthening and modernising ENISA will help the EU, Member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cyber security challenges."[29]

Cyber exercises

In 2010, ENISA facilitated the first pan-European cyber security exercise. This exercise took place in November and involved all 27 Member States and three EFTA countries (Switzerland, Norway and Iceland). Of these participants, 22 acted as players and eight as observers. One of the most important conclusions of this exercise was that procedures to handle cyber incidents do not yet exist on a pan-European level and that there is a need to improve response collaboration across Europe.[30] Following on from this work, ENISA has recently been asked to facilitate the planning of the first EU-US cyber security exercise, which will happen before the end of 2011.

This exercise represents an important development in international cooperation and ENISA appreciates that the Agency's expertise is being called upon to support this effort. Despite the fact that such a project is a great challenge for the Agency, we are confident that we can work together with the Member States and the USA to enhance transatlantic cyber security and cooperation.[31]

Adequate and consistent policy implementation

The cross-border nature of threats today means that there is a need for alignment of European and international legislative frameworks and procedures as well as collaboration models to ensure adequate policy implementation. More importantly, operational measures need to be designed to be capable of delivering results in a cross-border environment.

ENISA is supporting the Member States in the implementation of article 13a of the telecommunications directive.[32] This is important because it is the first attempt to collect data on security breach notifications at the pan-European level. In addition to supporting the Member States with implementation, we are also working on the broader concept. In particular, we are looking into how this data could sensibly be used to provide Member States with a more complete understanding of security breach trends at the pan-European level. By necessity, we consider this as a long-term goal, as it is critical that Member States fully support any model for exploiting the data that has been provided and that they agree on an overall concept for the use of such data.

28 IP/11/694
29 COM(2011) 163 final
30 http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/view?searchterm=cyber+europe+report
31 MEMO/11/246
32 http://www.enisa.europa.eu/media/news-items/agency-initiative-to-implement-art.-13-of-telecom-package?searchterm=article+13a

Supporting the community in the fight against cybercrime

In the recently released organised crime threat assessment from Europol it is noted that the internet is "a facilitator for organised crime". They note that "A new criminal landscape is emerging marked increasingly by highly mobile and flexible groups, operating in multiple jurisdictions and criminal sectors, and aided, in particular by widespread, illicit use of the Internet."[33]

Improving the capability for dealing with cyber-attacks is one of the objectives of the EU Internal Security Strategy, which states that "Europe is a key target for cybercrime because of its advanced Internet infrastructure, the high number of users, and its Internet-mediated economies and payment systems."[34]

ENISA acknowledges the importance of the fight against cybercrime as well as the need for a strong collaboration between CERTs and law enforcement. Since its inception, ENISA has sought to foster a good working relationship with relevant communities in both areas. ENISA already acts as a facilitator and information broker for CERTs.[35] The Agency does not, itself, respond to cybercrime, but can assist bodies that do.

ENISA will continue to work together with the CERT community as well as law and enforcement agencies to assist CERTs in their efforts against cybercrime and to work for better protection and resilience of ICT in Europe. For this reason, ENISA appreciates the European Commission's proposal to extend its task list by giving the Agency a role in supporting the fight against cybercrime.

Cybercrime centre

ENISA supports the establishment of a cybercrime centre, as called for in the Internal Security Strategy[36] and recognises the importance of setting up a structured approach to information exchange between this centre and ENISA. ENISA can help the centre set up a dialogue with the CERT community and provide the centre with access to its other stakeholder communities as needed. Furthermore, ENISA can act as a centre of expertise on tools, methods and trends.

The cooperation between the cybercrime centre and ENISA will initially focus on improving awareness about trends and emerging threats, as well as concerns and possible barriers to collaboration and information exchange across sectors and national borders. With the different knowledge, focus and expertise of the centre and the Agency, the exchange of methods and information will help in improving skill sets and achieving a more holistic approach to preventing and tackling cybercrime.

International cooperation

The cross-border nature of threats and the associated mitigation mechanisms make it essential to focus on strong international cooperation. This requires major efforts at national level, at pan-European level and globally. There should be close cooperation with international partners to prevent and to respond to cyber incidents.

At the EU-US summit[37] in November 2010, held in Lisbon, it was agreed to set up a working group on cyber security and cybercrime to evaluate and coordinate opportunities for enhanced collaboration. ENISA will contribute to three Expert Sub-Groups (ESGs). These are looking at Public Private Partnerships, Cyber Incident Management and Awareness Raising.

ENISA expects that international coordination in the area of information security will grow in importance throughout the next decade as countries become increasingly dependent on ICT functions that are offered and maintained in locations outside national boundaries. The recent phenomenon of cloud computing is highly illustrative of this trend.

33 http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA_2011.pdf
34 COM(2010) 673 final
35 And for Computer Security Incident Response Teams (CSIRTs)
36 http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf
37 MEMO/10/597

Information exchange

Information exchange is a fundamental component of any global initiative to improve security. Without effective information exchange mechanisms, European Member States will not be in a position to correctly assess global threats and may therefore put in place procedures and mechanisms that do not address the most important risks.

Similarly, poor information exchange mechanisms are likely to result in a duplication of effort and a slower implementation of approaches, processes and technology for mitigating the key risks once they are understood.

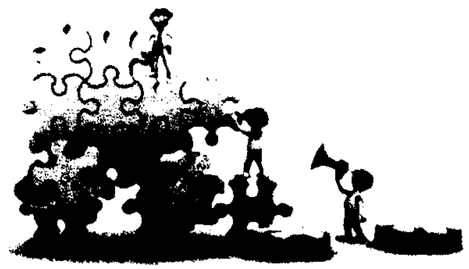
ENISA has significant experience in promoting the exchange of information related to information security between Member States. In the area of CIIP for instance, the approach has been to work together with Member States in order to identify lessons learned from national approaches and to enable Member States to learn from each other. As a concrete example, one of the preparation activities in the cyber security exercise was the exchange of experience at the national level on preparedness exercises.

Building communities

Given the global nature of ICT, and the growing and ever more sophisticated forms of cyber security threats, international coordination and appropriate networks are indispensable. This includes cooperation throughout Europe as well as globally in both the public and private sectors.

Much of our critical information infrastructure is owned and operated by the private sector. As such, addressing threats and strengthening security in the digital society is a shared responsibility – of individuals as much as of private and public bodies. A good example of an initiative to build bridges between the public and private sector is the EP3R (European Public-Private Partnership for Resilience) initiative. Since 2009 ENISA has facilitated and supported the activities of the working groups in the EP3R on security and resilience objectives, baseline requirements, as well as good policy practices and measures.

With the Lisbon Treaty in force the EU is better placed to take a more holistic approach to cyber security and to exploit synergies in our efforts to improve it. ENISA's mission is to support the Member States and the EU institutions in improving dialogue between communities in the area of NIS. The Agency could sensibly be considered as an interface between different operational communities in general. The objective would be to ensure that the overall approach to improving information security throughout Europe is both coherent and efficient, by identifying synergies and eliminating duplication of work.



The Future

ENISA was established in 2004 with the purpose of contributing to a high level of network and information security "for the benefit of citizens, consumers, business and public sector organisations in the European Union, thus contributing to the smooth functioning of the internal market," as set out in the founding regulation of the Agency.[38] Since then, the challenges related to NIS have evolved alongside technology and market developments. Therefore, the decision has been taken to modernise and further develop ENISA as an efficient body which serves as the EU's centre of expertise in NIS. The intention is to agree on a new mandate for the Agency, which reflects the constantly evolving NIS environment and will give the Agency more flexibility to interact with and respond to the needs of stakeholders across Europe.

38 Regulation (EC) No 460/2004

Conclusion

ICT developments bring with them considerable benefits for modern society – they are a key economic driver and contribute to the competitiveness of the European economy. Such developments however are accompanied by associated risks, and controlling such risks is essential if we are to realise the true benefits.

The success of the EU Internal Security Strategy "is dependent on the combined efforts of all EU actors, but also on cooperation with the outside world. Only by joining forces and working together to implement this strategy can Member States, EU institutions, bodies and agencies provide a truly coordinated European response to the security threats of our time "[40]

ENISA's role is to support the Commission and Member States in facilitating dialogue on Network and Information Security across communities and with different international counterparts. As the European Agency for Network and Information Security, ENISA already plays an important role in supporting the EU institutions and the Member States in securing the ICT infrastructure of the future. In particular, by acting as a neutral European platform for information sharing and for establishing and maintaining networks and communities, the Agency promotes dialogue and helps Member States to align their approaches to specific issues. The Agency also provides advice to stakeholders, bridging the gap between policy and operational requirements.

There are a number of areas where the current approach to improving cyber security in the EU could sensibly be extended. For example, there is a clear need to collect and analyse data relating to information security in a cross-border context which could reveal trends that are not visible at present. Also, the coming into force of the Lisbon Treaty is an opportunity to improve the level of dialogue between communities in the area of network and information security. A proactive approach to building these new cross-border communities will bring great benefits both in terms of the effectiveness of its approach and efficiency in use of its resources.

It is important that our efforts to protect and facilitate the development and prosperity of the European Information Society do not lose momentum. These efforts are addressed on many fronts with multiple stakeholders – all are increasing in numbers and scope along with the pervasiveness and economic importance of ICTs. It is important that ENISA is modernised and further developed to allow the Agency to respond to these changes and provide support and expertise for stakeholders across Europe.

40 COM(2010) 673 final p. 16

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu

Meeting on January 20, 2012, with Mr. Marc Lortie, Canada's Ambassador to France and Mr. Kim Butler, French Plenipotentiary Minister

ISSUE

- You will be meeting with Mr. Marc Lortie, Canada's Ambassador to France (**TAB C**), and Mr. Kim Butler, French Plenipotentiary Minister (**TAB D**), to discuss cyber security in Canada and in France.

STRATEGIC OBJECTIVES

- Seek an assessment of France's political positioning of cyber security, and how cyber security efforts are perceived in France.

- Convey your objectives in meeting with Mr. Patrick Pailloux of the *Agence nationale de la sécurité des systèmes d'information* (ANSSI).

- Leave these officials with a greater understanding of the accomplishments and challenges associated with the implementation of *Canada's Cyber Security Strategy* (**TAB E – Backgrounder**).

STRATEGIC CONSIDERATIONS

France has made cyber security a cornerstone of its national security policy as defined in its 2008 *Livre blanc sur la défence et la securité nationale* (White Paper on Defence and National Security). Since then, the French Government established the *Agence nationale de la sécurité des systèmes informatique* (ANSSI, the National Agency for the Security of Information Systems) as the primary agency responsible for national cyber security and in 2011, launched its first cyber security strategy.

France has advanced cyber capabilities and is understood to be innovative in the development of policies and legislation to strengthen its national cyber security. This meeting will be an opportunity to apprise an important ally of Canada's accomplishments and challenges on cyber security. Likewise it would be informative to know whether French officials have conveyed their primary cyber security concerns to the Ambassador or Embassy officials, and how France aim to address them. Despite France's significantly different political and legislative system, French efforts could inform Canada's approach to key cyber security challenges, such as information sharing between the private and public sectors.

National Security Operations has provided briefing material in the instance the Ambassador raises the *Criminal Code* listing of the Mujahedin-E-Khalq (**TAB B**).

TALKING POINTS ARE ON THE NEXT PAGE

Meeting on January 20, 2012, with Mr. Marc Lortie, Canada's Ambassador to France and Mr. Kim Butler, French Plenipotentiary Minister

TALKING POINTS

Possible questions to ask Ambassador Lortie and Minister Butler

- Given your interactions with French officials, what do they convey as their top cyber security concerns and where do Internet policy issues fall on the French agenda?

- Have French officials kept you abreast of how they are implementing France's cyber security strategy, released in early 2011?

- I understand that, in general, the private sector in France has traditionally been more welcoming of government intervention than industry in Canada. We intend to get a better sense of how the French government works with French industry to address cyber security issues.

- Do you have a sense of what effort the French Government has made to facilitate or improve information sharing between the private and public sectors in France?

Objectives for the meeting with Mr. Pailloux

- As you know, I will be meeting with Mr. Patrick Pailloux, Director General, *Agence nationale de la sécurité des systèmes d'information* (ANSSI). My objectives for the meeting are to:

    - Leave him with a greater understanding of the accomplishments associated with the implementation of *Canada's Cyber Security Strategy*.

- Obtain a greater understanding of the roles and responsibilities of the respective French organizations involved in ensuring the security and resiliency of information systems and networks in France.

- Obtain a greater understanding of the unique relationships and challenges that France faces in advancing national cyber security efforts especially in working with the private sector.

- Signal Canada's desire for targeted collaboration with France on cyber security issues, notably on the promotion of international norms for cyberspace.

Marc Lortie – Ambassador of Canada to France

Marc Lortie, a career diplomat, was born in Beauport, Québec in 1948.

He obtained a specialized B.A. in Political Science (International Relations) at Laval University. He joined the Department of External Affairs in 1971. He served abroad in Tunisia (1973-75) and Washington (1979-83). He was seconded to the Prime Minister's Office in 1985 where he was in charge of relations with the international media until 1987 when he was named Press Secretary.

In 1989, he returned to the diplomatic service and served in Paris as Minister-Counsellor for Political Affairs and as Personal Representative of the Prime Minister for La Francophonie. He was named Canadian Ambassador to Chile in 1993 and served in that position until 1997 when he was nominated Fellow at the Centre for International Affairs at Harvard University.

Mr. Lortie returned to Ottawa in September 1998 when he was appointed sherpa for the third Summit of the Americas. In 2001, Mr. Lortie was appointed Assistant Deputy Minister for the Americas. He was Ambassador of Canada to Spain from 2004 to 2007. He arrived in Paris in September 2007.

BIOGRAPHY

Kim Perry Butler

Minister Plenipotentiary, Embassy of Canada, Paris

Kim Butler was appointed Minister Plenipotentiary at the Embassy of Canada in Paris in September 2010.

Kim joined the Federal Government in 1986 and has held a variety of positions with increasing responsibilities including Consul General of Canada at Minneapolis, Senior Adviser to the Deputy Minister of Industry, Director General and Federal Co-Chair of the Canada-Ontario Infrastructure Program, Corporate Comptroller and, Senior Director of Financial Policy and Systems. From 2007 to 2010, he served as Director General of the North American Bureau .

Kim is a graduate of the Government of Canada's Accelerated Executive Development Program and has completed the Public Executive Program at Queen's University. He holds a Bachelor of Commerce Honours degree from the University of Ottawa.

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

Meeting on January 20, 2012, with Mr. Patrick Pailloux, Director General, Agence nationale de la sécurité des systèmes d'information

ISSUE

- Meeting with Mr. Patrick Pailloux, Director General (**TAB B**), *Agence nationale de la sécurité des systèmes d'information* (ANSSI, unofficially translated as the National Agency for the Security of Information Systems).

- Mr. Pailloux presented at the East-West Institute's first cyber security summit in Dallas in 2010. More recently, Mr. Pailloux spoke at the London Conference on Cyberspace in November 2011.

STRATEGIC OBJECTIVES

- Obtain a greater understanding of how French organizations work together to achieve national cyber security policy objectives.

- Obtain a greater understanding of the unique relationships and challenges that France faces in advancing national cyber security efforts especially in working with the private sector. This is particularly important given the closer relationship that the French state maintains with the private sector compared to that between the private sector and federal government in Canada.

- Leave counterparts with a greater understanding of the accomplishments achieved thus far in the implementation of *Canada's Cyber Security Strategy* (**TAB C – Backgrounder**).

- Signal Canada's desire for targeted collaboration with France on cyber security issues, [redacted]

BACKGROUND

France has made cyber security a cornerstone of its national security policy as outlined in the 2008 *Livre blanc sur la défence et la securité nationale* (White Paper on Defence and National Security). In 2009, the French Government established the ANSSI as the primary government agency responsible for national cyber security and in 2011, launched its first cyber security strategy (**TAB D**). Furthermore, in 2011, France made the Internet part of the focus of the G8 Leader's Declaration. [redacted] It would be informative to hear if, over the course of the year, how France's policy positions have evolved.

s.15(1) - Int'l

s.15(1) - Subv

The ANSSI appears to combine functions which, in Canada, reside with the Communications Security Establishment Canada (CSEC), Public Safety Canada, and the Chief Information Officer Branch of the Treasury Board Secretariat. ANSSI's mandate is to:

- detect and react early to cyber attacks, by creating an operational center for cyber defence, with continuous 24/7 surveillance of sensitive government networks, and appropriate defence mechanisms;

- prevent threats by supporting the development of trusted products and services for governmental entities and economic actors (what we address in Canada as the supply chain);

- provide reliable advice and support to governmental entities and operators of critical infrastructure; and

- keep companies and the general public informed about information security threats and the related means of protection through an active communication program.

Every week, the ANSSI prepares two high level briefings for the *Secrétaire general de la défense et la securité nationale* (i.e. the national security advisor to the Prime Minister of France). The ANSSI also administers the government's secure networks and acts as the government's Computer Emergency Readiness Team.

A 2009 report by the Internet security firm McAfee identified France, along with China, Israel, Russia and the United States (U.S.), as having the most advanced offensive cyber capabilities. The 2008 White Paper asserted France's primary cyber security objective was to become a global power in this area to protect its sovereignty. While France's military Joint Staff is largely in charge of these capabilities, it is unclear whether ANSSI plays a role in conducting offensive actions.

In 2006, France ratified the Council of Europe *Convention on Cybercrime* (Budapest Convention), the only piece of international law that specifically addresses cyber issues. Canada signed the Convention in 2001, but has yet to pass the requisite legislation for ratification.

STRATEGIC CONSIDERATIONS

Despite a general understanding of France's cyber capabilities and the role of the ANSSI, other elements of the organisational structure of France's cyber security apparatus remain unclear. For example, while ANSSI seems to act as the focal point for cyber security issues, the military is understood to play a significant role in establishing French cyber security policy. Better understanding the unofficial arrangements of France's cyber security organisational structure could help international coordination in the event of an international cyber incident or to promote shared cyber interests internationally.

France's cyber security strategy places a heavy emphasis on the need for the French government and private sector to protect information on their respective networks, but pays little attention to cybercrime. Using *Canada's Cyber Security Strategy* as a point of reference, France's strategy focuses largely on pillars one and two, and seems to only passingly address law enforcement considerations to combat cybercrime. If possible, it would be useful to better understand France's approach towards cybercrime.

On certain Internet economy and governance issues, France has taken a 'top down' policy approach, arguing that the state must play a more assertive role in developing regulations to mitigate unwanted behaviour in cyberspace.

It would be valuable to understand whether France's approach extends to cyber security, and whether, for example, the government would mandate standardised cyber security regulations for the private sector.

TAKING POINTS FOLLOW ON THE NEXT PAGE

s.15(1) - Int'l

s.15(1) - Subv

Meeting on January 20, 2012, with Mr. Patrick Pailloux, Director General, Agence nationale de la sécurité des systèmes d'information

TALKING POINTS

- Since launching *Canada's Cyber Security Strategy* in October 2010, the Government of Canada has strengthened its cyber security through:
  - updating Canada's legislative framework (e.g. the Anti-Spam bill);
  - streamlining the Canadian Cyber Incident Response Centre;
  - launching a national cyber security public awareness campaign; and
  - establishing relationships with provincial and territorial governments and key critical infrastructure sectors to improve their capabilities to protect their cyber systems.

- Canada's approach has been based on partnerships and consensus building, rather than regulation or government intervention

- Notwithstanding these achievements, many challenges lie ahead. These include establishing concrete policies and procedures to deal with major international cyber security incidents, improvements to information sharing regimes between private and public sector entities, and promoting international norms for cyberspace.

- States need to work together to find innovative ways to enable the benefits of cyberspace while deterring those activities that undermine national security, economic stability, and user confidence.

- I would like to get a better sense of how the French Government works with private sector organizations in operationalizing addressing cyber security threats and vulnerabilities.

Possible questions to ask French interlocutors

- How do Internet policy issues fit into the French policy agenda?

- In terms of information sharing, do critical infrastructure and private sector organizations share information willingly and in a timely fashion with you? What are the biggest challenges that you face with respect to sharing and obtaining information from affected entities both within France and with the international community?

- Can you please elaborate on the roles and responsibilities of ANSSI? How does your Agency work with other government departments with a responsibility for cyber security, such as the defence forces, law enforcement and computer emergency response teams?

- In terms of information sharing, do critical infrastructure entities and the private sector share information willingly and in a timely fashion with your organization? What are the biggest challenges that you face with respect to sharing and obtaining information from affected entities both within France and with the international community?

- Do you believe that government should set mandatory industry regulations for cyber security standards? If so, what would these regulations include?

- I would like to get a sense of what you took away from the London International Cyber Conference. What steps do you see as critical to promoting international norms for cyberspace?

Patrick Pailloux – Chief Executive Officer – Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

A former Polytechnique (1986) and École nationale supérieure des télécommunications student, M. Patrick Pailloux was part of the regional direction of France Télécom Île de France from 1991 to 1995. Following this he was sector Chief and Department Chief of the Ministère de la Défense information systems from 1995 to 2003. On July 8, 2009, he was appointed as the Chief Executive Officer of Agence nationale de la sécurité des systèmes d'information (ANSSI).

He is also a member of the executive board of the European Network and Information Security Agency (ENISA).

BACKGROUNDER: CANADA'S CYBER SECURITY EFFORTS

Canada's Cyber Security Strategy has achieved several notable accomplishments in its first year. With respect to Pillar 1 of the Strategy, "secure Government systems," achievements include:

- the creation within Public Safety (PS) of the Government's first policy capacity to lead national cyber security efforts;
- strengthening of Government network and security measures, in particular with further investment in the security capability and a major revision of the Government's *Information Technology Incident Management Plan*;
- the transfer of incident response coordination for Government of Canada systems to the Communications Security Establishment Canada in June 2011, thereby further leveraging Government's internal capabilities to secure its systems and clarifying roles and mandates; and
- the creation of Shared Service Canada, which will consolidate and streamline the delivery of Government IT services, complementing the Strategy by facilitating improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," achievements include:

- initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors, noting that such dialogue was absent one year ago;
- substantial expansion to engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure* and fora such as the newly created Canadian Security Telecommunications Advisory Council; and
- streamlining the mandate of PS' Canadian Cyber Incident Response Centre to focus on national issues and on supporting the provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has progressed as follows:

- to mark the one-year anniversary of the October 2010 launch of the Strategy, PS' Communications Directorate, as the federal lead for cyber security communications, launched a national public awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the Government passed anti spam legislation to create new penalties against unsolicited commercial messages and new authorities for those penalties to be enforced; and
- the Royal Canadian Mounted Police (RCMP) established the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

Défense et sécurité des systèmes d'information

Stratégie de la France

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence Nationale de la Sécurité des Systèmes d'Information

Prologue

Sans doute n'en avons-nous pas encore pris collectivement la mesure : dans le *Livre blanc sur la défense et de la sécurité nationale* présenté par le Président de la République en juin 2008, la sécurité des systèmes d'information émergeait, avec la dissuasion, comme un domaine dans lequel la souveraineté de la France devrait s'exprimer pleinement.

Le cyberespace peut pourtant apparaitre bien éloigné du champ de la défense et de la sécurité nationale. En vingt ans, les technologies du numérique ont fusionné nos vies personnelles et professionnelles, porté la compétitivité des entreprises à un niveau inédit, rapproché les administrations des usagers et favorisé la transparence de la vie des institutions de notre pays.

Le cyberespace, nouvelle tour de Babel, est un lieu de partage des cultures du monde, de diffusion des idées et d'informations en temps réel, un lieu d'échanges entre personnes. L'exclusion du numérique condamne les individus à l'isolement, les entreprises à la décroissance et les nations à la dépendance.

Dans le monde matériel, les destructions causées par les guerres ou le terrorisme comme les exactions des criminels sont visibles et souvent médiatisées. Dans le cyberespace, monde immatériel, les conséquences des attaques informatiques contre les systèmes d'information des États, des entreprises ou contre les ordinateurs des citoyens ne sont le plus souvent visibles que des spécialistes et restent ignorées du grand public.

Le cyberespace, nouvelles Thermopyles, est devenu un lieu d'affrontement : appropriation de données personnelles, espionnage du patrimoine scientifique, économique et commercial d'entreprises victimes de leurs concurrents ou de puissances étrangères, arrêt de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, compromission d'informations de souveraineté et même, dans certaines circonstances, perte de vies humaines sont aujourd'hui les conséquences potentielles ou réelles de l'imbrication entre le numérique et l'activité humaine.

Devant l'irruption du cyberespace dans le champ de la sécurité nationale et à la mesure des enjeux, le Gouvernement a décidé de doter la France d'une capacité structurée de défense et de sécurité. Il a ainsi créé en 2009 l'Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité au service des pouvoirs publics, des entreprises et des citoyens. Le Président de la République a décidé en juillet dernier de confier à l'Agence, en complément de sa mission de sécurité, une mission de défense des systèmes d'information.

L'objectif de ce document est de préciser les grandes lignes de la stratégie poursuivie par la France depuis la publication du *Livre blanc sur la défense et la sécurité nationale* afin de garantir, dans le cyberespace, la sécurité de nos compatriotes, de nos entreprises et de la Nation.

Francis DELON

Secrétaire général de la défense et de la sécurité nationale

Les mots suivis d'un astérisque sont définis dans le glossaire

Credits Photos

couverture	Jean Mottershead (CC BY-NC-ND 2.0), ou libres de droits
page 11	Ruby MV (CC BY-NC-SA 2.0)
page 12	Simon BISSON (CC BY-NC-ND 2.0)
page 13	MrFenwick (CC BY-NC-ND 2.0)
page 14	Runran (CC BY-SA 2.0)

Sommaire

Prologue

Synthèse

Quatre objectifs stratégiques

- Être une puissance mondiale de cyberdéfense
- Garantir la liberté de décision de la France par la protection de l'information de souveraineté
- Renforcer la cybersécurité des infrastructures vitales nationales
- Assurer la sécurité dans le cyberespace

Sept axes d'effort

- Anticiper, analyser
- Détecter, alerter, réagir
- Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines
- Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales
- Adapter notre droit
- Développer nos collaborations internationales
- Communiquer pour informer et convaincre

Glossaire

Synthèse

Parmi les menaces majeures auxquelles la France sera confrontée dans les quinze prochaines années, le *Livre blanc sur la défense et la sécurité nationale* de 2008 a retenu l'attaque informatique de grande envergure contre les infrastructures nationales. Ce constat a conduit le Gouvernement à décider de renforcer significativement les capacités nationales en matière de cyberdéfense. La création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en 2009, a été la première étape de cet engagement.

Exposée dans le présent document, la stratégie nationale en matière de défense et de sécurité des systèmes d'information incarne l'ambition affichée par le *Livre blanc*.

Elle repose sur quatre objectifs.

1. Être une puissance mondiale de cyberdéfense

Tout en conservant son autonomie stratégique, la France doit effectuer l'effort nécessaire pour appartenir au premier cercle très restreint des nations majeures dans le domaine de la cyberdéfense. Nous bénéficierons ainsi de l'effet démultiplicateur des coopérations tant au plan opérationnel que pour la mise en place d'une stratégie unifiée face à des menaces communes.

2. Garantir la liberté de décision de la France par la protection de l'information de souveraineté

Les autorités gouvernementales comme les acteurs de la gestion des crises doivent disposer des moyens de communiquer en toute situation et en toute confidentialité. Les réseaux qui répondent à ce besoin doivent être étendus, notamment à l'échelon territorial.

La confidentialité de l'information qui transite par ces réseaux nécessite la réalisation de produits de sécurité maîtrisés. Nous devons conserver les compétences nécessaires à leur conception et optimiser leurs modes de développement et de production.

3. Renforcer la cybersécurité des infrastructures vitales nationales

Le fonctionnement de notre société dépend de manière croissante des systèmes d'information et des réseaux, notamment d'Internet. Une attaque réussie contre un système d'information critique ou contre l'Internet français peut entraîner des conséquences humaines ou économiques graves. Il importe que l'État, en liaison étroite avec les équipementiers et les opérateurs concernés, travaille à garantir et à améliorer la sécurité de ces systèmes critiques.

4. Assurer la sécurité dans le cyberespace

Les menaces qui pèsent sur les systèmes d'information touchent tout à la fois les administrations, les entreprises et les citoyens.

L'administration doit être exemplaire et améliorer la protection de ses systèmes d'information et des données qui lui sont confiées.

S'agissant des entreprises et des particuliers, un travail d'information et de sensibilisation doit être engagé.

En matière de lutte contre la cybercriminalité, la France encouragera le renforcement du droit et l'entraide judiciaire internationale.

Pour atteindre ces objectifs, sept axes d'effort sont retenus :

1. Mieux anticiper et analyser l'environnement afin de prendre les décisions adaptées.
2. Détecter les attaques et les contrer, alerter les victimes potentielles et les accompagner.
3. Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines dans l'objectif de conserver l'autonomie nécessaire.
4. Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales pour une meilleure résilience nationale.
5. Adapter notre droit afin de prendre en compte les évolutions technologiques et les nouveaux usages.
6. Développer nos collaborations internationales en matière de sécurité des systèmes d'information, de lutte contre la cybercriminalité et de cyberdéfense pour mieux protéger les systèmes d'information nationaux.
7. Communiquer, informer et convaincre afin de permettre aux Français de prendre la mesure des enjeux liés à la sécurité des systèmes d'information.

Ce document résume la partie publique des orientations et actions approuvées par le comité stratégique de la sécurité des systèmes d'information institué par le décret n° 2009-834 du 7 juillet 2009 portant création de l'agence nationale de la sécurité des systèmes d'information* (ANSSI).

« La France doit garder un domaine de souveraineté, concentré sur les capacités nécessaires au maintien de l'autonomie stratégique et politique de la nation : la dissuasion nucléaire, le secteur des missiles balistiques, les sous-marins nucléaires d'attaque, la sécurité des systèmes d'information font partie de ce premier cercle. »

« Défense et sécurité nationale, le livre blanc », p.318

Quatre objectifs stratégiques

1. Être une puissance mondiale de cyberdéfense

Le développement de la société de l'information, porté par les réseaux de communications électroniques, parce qu'il crée de la valeur et de nombreux emplois, est un formidable moteur de notre croissance. Il contribue fortement à la compétitivité du tissu économique national et donc au rang de la France dans le monde.

Or, les réseaux de communications électroniques font l'objet d'activités illicites menées directement ou indirectement par des États. Certains se livrent à des opérations massives d'espionnage via ces réseaux et cherchent à obtenir des informations de souveraineté, comme celles relevant du secret de la défense nationale ou encore du patrimoine scientifique, technologique, commercial ou financier des entreprises de nos secteurs stratégiques.

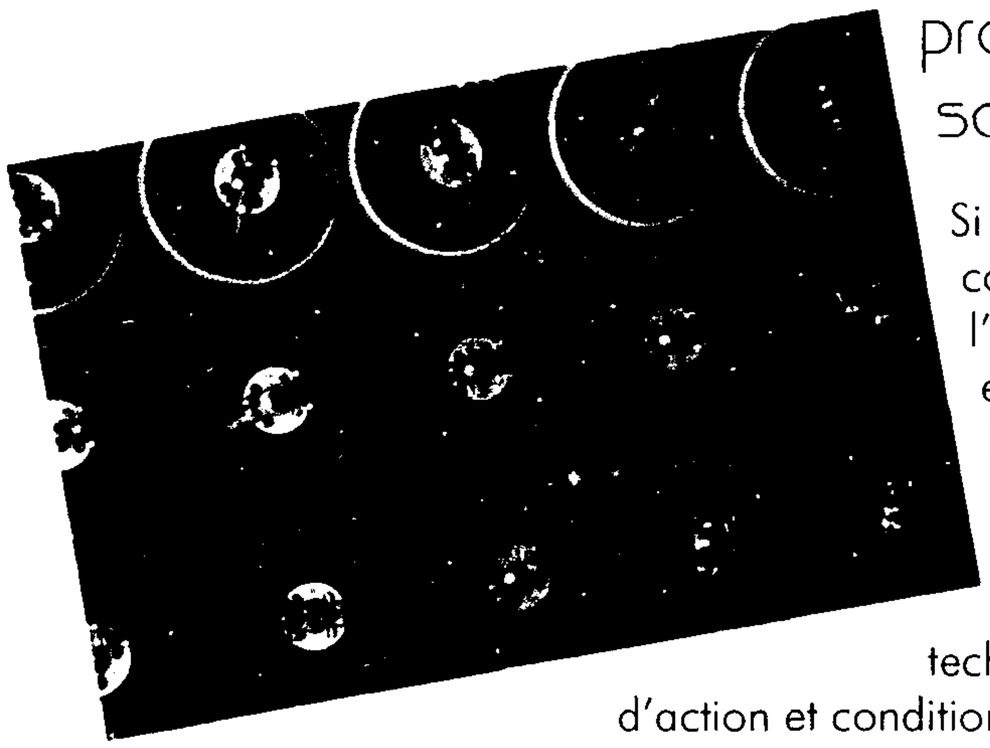
De leur côté, des groupes terroristes utilisent ces mêmes réseaux de communications électroniques pour propager leurs idées, diffuser de l'information opérationnelle à leur organisation et se livrer à des activités de propagande.

Dans un avenir proche, États ou groupes terroristes pourraient attaquer les infrastructures vitales d'États considérés comme idéologiquement hostiles.

Il est donc indispensable que la France se dote d'une capacité de cyberdéfense.

Or, contrairement à ceux du monde matériel, les affrontements dans le cyberespace ne connaissent pas les frontières. Ainsi, une cyberdéfense crédible ne peut être uniquement nationale et doit s'appuyer sur un réseau d'alliés avec lesquels il est possible d'échanger, en temps réel, des informations sur les vulnérabilités, les dispositifs de protection, les attaques et les parades à mettre en œuvre face aux agressions menées dans le cyberespace directement ou indirectement par des États ou des groupes terroristes. La France renforcera ses partenariats opérationnels avec ses alliés les plus proches et mettra à profit son expertise pour contribuer activement à la formulation des politiques de cyberdéfense au sein des organisations internationales, et notamment au sein de l'Union européenne.

2. Garantir la liberté de décision de la France par la protection de l'information de souveraineté



Si l'évolution de la société tend à imposer comme règle l'existence et le partage de l'information et son accès, à la fois instantané et sous de multiples formes, une part de l'équilibre du monde réside toujours dans la capacité à maintenir secrète « l'information de souveraineté », fraction de l'information diplomatique, militaire, scientifique, technique et économique qui permet la liberté d'action et conditionne la prospérité des nations.

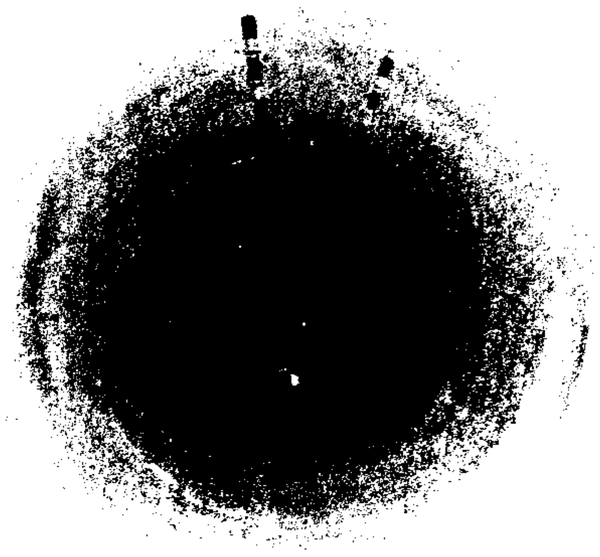
Comme par le passé, les services de renseignement du monde entier, parmi d'autres acteurs, tentent d'obtenir l'information de souveraineté. Les réseaux de télécommunications, notamment Internet, les informations qui y circulent, celles disponibles sur les réseaux ou les terminaux qui s'y connectent, sont devenus à la fois sources d'information et vecteurs de collecte.

Le moyen le plus efficace pour protéger l'information de souveraineté est d'utiliser des techniques de cryptographie* qui rendent impossible, ou du moins retardent, sa compréhension si cette information venait à être altérée, divulguée ou interceptée. Les progrès de la cryptanalyse*, qui suivent notamment ceux de la puissance de calcul des ordinateurs, obligent à concevoir et utiliser des méthodes et techniques plus difficiles à analyser et renouvelées régulièrement.

Le maintien de notre autonomie stratégique repose sur notre capacité à maîtriser les techniques cryptographiques et les technologies clés nécessaires à la conception de produits de sécurité* qui les utilisent, ce qui implique de veiller à ce que le domaine de la sécurité des systèmes d'information reste attractif pour les jeunes diplômés afin d'éviter le tarissement progressif des compétences.

Parallèlement à la nécessité de pouvoir communiquer de manière sûre et confidentielle, les décideurs comme les organismes associés à la gestion des situations de crise doivent avoir à leur disposition des moyens de communication disponibles en toutes circonstances. Ces moyens d'échanges électroniques, de téléphonie et de visioconférence sécurisés ont été conçus et développés. Leur déploiement va se poursuivre dans les années qui viennent, notamment au profit des opérateurs d'importance vitale*.

3. Renforcer la cybersécurité des infrastructures vitales nationales



Par la convergence de multiples technologies, le monde réel et les réseaux s'interpénètrent. De nombreux objets du monde réel — de l'étiquette de supermarché à la raffinerie, de la photocopieuse au drone de combat — embarquent des systèmes d'information et s'y intègrent. À distance, via les réseaux, il est possible de collecter les informations transmises par ces objets, de les maintenir en fonction et de les piloter.

La France a défini dans son code de la défense des secteurs d'activités d'importance vitale dans lesquels agissent des opérateurs qui concourent à la satisfaction des besoins indispensables à la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables.

La plupart des opérateurs d'importance vitale utilisent largement les réseaux de télécommunications, et singulièrement Internet, tant pour leur gestion que pour l'exercice de leur métier. Pourtant, dans la rencontre, ancienne et pourtant inédite parce que bousculée par l'interconnexion des systèmes, entre le monde industriel et le monde de l'informatique, le premier manque de formation et de sensibilisation à la sécurité des systèmes d'information, tandis que le second méconnaît souvent les contraintes et le fonctionnement des systèmes industriels.

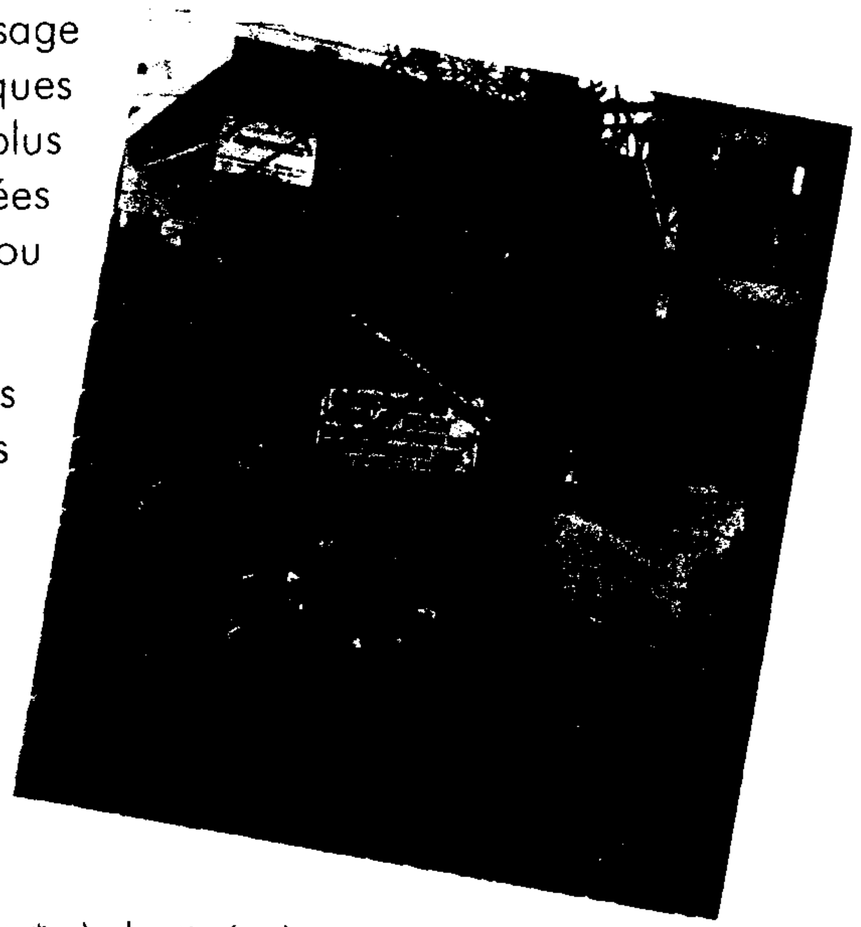
La dépendance de chacun des acteurs vis-à-vis d'Internet est accrue par des tendances lourdes de notre organisation économique et sociale : l'externalisation et l'informatique en nuage, la mutualisation des services supports, la gestion en temps réel et en flux tendus, le nomadisme, le transfert de tâches vers les clients ou les administrés, la création ou la réingénierie de nombreux processus.

En cas d'interruption du fonctionnement des réseaux de télécommunications ou d'Internet, les moyens de substitution peuvent s'avérer très insuffisants, notamment par manque de personnels qualifiés susceptibles de remettre en fonction les processus antérieurs à l'avènement de l'ère numérique. Dans le cas de processus directement issus de nouveaux usages liés aux technologies de l'information, les moyens de substitution n'existent pas.

Comme le démontre régulièrement l'actualité mondiale, les conséquences possibles d'actes de malveillance contre les systèmes automatisés de contrôle des processus industriels déployés par les opérateurs d'importance vitale sont aujourd'hui insuffisamment mesurées. Ainsi, la protection des réseaux de communications électroniques — et notamment d'Internet — comme la sécurisation des systèmes critiques des opérateurs d'importance vitale constituent des priorités nationales.

Quatre objectifs stratégiques

4 Assurer la sécurité dans le cyberespace



Pour une part croissante de nos concitoyens, l'usage des réseaux de communications électroniques comme Internet imprègne les fonctions les plus courantes de la vie quotidienne comme celles liées au commerce, aux démarches administratives ou aux échanges interpersonnels.

Parallèlement, les techniques utilisées dans le cyberespace par des individus ou groupes d'individus malveillants sont de plus en plus performantes et visent à usurper des identités, à se procurer les informations nécessaires à l'accès à des comptes bancaires ou à collecter et revendre des données personnelles. On observe également une multiplication des cas de prises de contrôle malveillantes à distance d'ordinateurs visant à les intégrer dans des réseaux de machines compromises (« *botnets** ») destinés à accomplir des actes illicites tels que des attaques informatiques ou des envois de courriels malveillants.

Dans ce contexte, les administrations doivent montrer l'exemple en protégeant le cyberespace public. Les usagers doivent utiliser en confiance les services électroniques proposés par les autorités publiques, notamment au regard de la protection de leurs données personnelles. Le référentiel général de sécurité* (RGS) publié début 2010 offre un cadre réglementaire susceptible de renforcer cette sécurité. Son respect et sa mise en œuvre par les autorités publiques sont prioritaires.

La sécurisation du cyberespace passe par une démarche systématique d'information des entreprises et des citoyens sur les risques encourus et les moyens de s'en protéger. L'objectif est qu'à terme, chaque citoyen puisse être sensibilisé aux questions de cybersécurité au cours de son éducation. Cette démarche appelle la mise en place d'une politique de communication gouvernementale active.

Enfin, Internet est un espace de droit. La France doit encourager le renforcement ou l'édiction de règles juridiques dans le cyberespace lorsque le droit existant est insuffisant et amplifier l'entraide judiciaire internationale en matière de répression des infractions commises sur ou à travers les réseaux de communications électroniques.

Afin de remplir les quatre objectifs stratégiques,
7 axes d'effort ont été retenus.

Sept axes d'effort

1. Anticiper, analyser

Risques et menaces évoluent rapidement dans le cyberespace. La parution d'un nouveau produit ou d'une nouvelle version d'un logiciel, la publication d'une faille* non corrigée d'un logiciel largement utilisé, l'apparition d'une nouvelle technologie ou d'un nouvel usage, une déclaration politique, peuvent entraîner, dans des délais très courts, une mise en danger de la sécurité des systèmes d'information.

- Dans ce contexte, la défense et la sécurité de nos systèmes d'information passe en premier lieu par un suivi de l'actualité des technologies et par une analyse, une bonne compréhension voire une anticipation du jeu des acteurs publics ou privés.

2. Détecter, alerter, réagir

Compte-tenu de la dépendance croissante à Internet des entreprises, des infrastructures et des services, et en raison des risques systémiques portés par certaines faiblesses, il est nécessaire d'être en mesure de détecter au plus tôt failles et attaques, d'alerter les victimes potentielles ou avérées et de leur proposer dans un délai bref une aide à l'analyse et à l'élaboration de parades.

- Comme l'a prévu le *Livre blanc sur la défense et la sécurité nationale*, la France développe une capacité de détection des attaques sur les systèmes d'information. Notamment déployés dans les réseaux des ministères, des dispositifs permettent d'alerter leurs responsables, d'aider à élucider la nature des attaques et d'élaborer des parades adaptées.
- Pour gérer l'ensemble des informations recueillies par les outils de détection, par les dispositifs de veille ou transmises par nos partenaires, afin de présenter une image en temps réel de la situation des réseaux nationaux et pour être capable de gérer une situation de crise, l'ANSSI se dote d'une « salle d'opération » à la hauteur des enjeux.
- Pour répondre aux crises majeures affectant ou menaçant la sécurité des systèmes d'information des autorités administratives ou des opérateurs d'importance vitale, l'État doit être en mesure de prendre rapidement les mesures nécessaires. Dans cette optique, l'ANSSI assure la fonction d'autorité nationale de défense des systèmes d'information.

3. Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines

La sécurité des systèmes d'information repose sur une maîtrise de technologies et de savoir-faire, également accessibles aux organisations et individus qui veulent y porter atteinte. Si les acteurs étatiques de la sécurité des systèmes d'information doivent connaître « l'état de l'art », ils doivent également être en mesure d'anticiper voire de créer les évolutions technologiques en maintenant leurs capacités de recherche, seules capables de permettre de limiter l'avantage tactique de l'attaquant sur le défenseur.

La France dispose d'équipes de recherche de niveau mondial dans les domaines de la cryptologie et des méthodes formelles. Dans d'autres domaines, comme celui des architectures de sécurité des systèmes d'information, elle rattrape le niveau des nations les plus avancées.

- Pour catalyser ces travaux, la création, avec des partenaires industriels, d'un centre de recherche consacré à la cyberdéfense est à l'étude. Ce centre mènera des activités de recherche scientifique (recherche en cryptologie, étude des groupes d'attaquants et de leurs méthodes, expertise sur les logiciels malveillants et les failles informatiques, développement de logiciels libres sécurisés, élaboration de concepts de défense informatique, etc.), et des actions d'expertise et de formation.

Le développement de la société de l'information crée pour les entreprises un marché d'emblée mondial, aujourd'hui préempté par des acteurs situés hors d'Europe. S'agissant de la sécurité des systèmes d'information, cette situation n'est ni souhaitable ni tenable. La France dispose pourtant d'un tissu industriel de pointe unique en Europe, qui lui permet potentiellement de maîtriser une grande partie des technologies nécessaires à la conception de produits de sécurité, y compris en matière de composants. De nombreuses PME innovantes composent ce tissu. Elles n'ont cependant pas aujourd'hui la taille critique nécessaire et ne sont pas portées par une demande suffisante.

- Les consolidations industrielles seront favorisées par les différents moyens de l'État, notamment par les fonds d'investissement stratégique.

Pour une meilleure efficacité, les concepteurs de produits informatiques et de systèmes d'information doivent prendre en compte les questions de sécurité dès l'origine de leurs développements. L'imprégnation du tissu industriel par des experts en sécurité des systèmes d'information doit donc être renforcée. L'orientation de jeunes vers ces métiers sera encouragée afin d'accroître le vivier national de compétences.

De manière générale, les formations scientifiques et techniques dans les domaines des technologies de l'information devront intégrer un volet relatif à la sécurité des systèmes d'information.

4. Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales

Comme le souligne le *Livre blanc sur la défense et la sécurité nationale*, nous devons disposer « d'une offre de produits de très haute sécurité totalement maîtrisés, pour la protection des secrets de l'État, ainsi que d'une offre de produits et de services de confiance labellisés, à laquelle recourront les administrations et qui seront largement accessibles au secteur économique ». Des réseaux sécurisés résilients* pour « l'ensemble de la chaîne de décision et de commandement sur le territoire métropolitain » doivent être utilisés.

- Relevant de l'information classifiée*, la stratégie française en matière de produits de sécurité et de composants a été redéfinie. Elle prend notamment pleinement en compte le retour de la France dans le commandement intégré de l'OTAN.

- Dans les réseaux ministériels, la mise en place de systèmes d'authentification forte reposant, par exemple, sur l'utilisation de cartes à puce, domaine d'excellence française, va permettre d'en améliorer très significativement la sécurité.

- Les autorités gouvernementales disposent aujourd'hui d'un intranet sécurisé interministériel, d'un réseau de téléphonie à forte disponibilité qui sera totalement équipé de nouveaux terminaux chiffrants d'ici 2012, et d'une solution de visio-conférence protégée, en particulier destinée à équiper les centres de décision ministériels. Le déploiement de ces différents réseaux se poursuivra, notamment dans les administrations territoriales.

- Dans le domaine de la sécurité des systèmes d'information des opérateurs d'importance vitale, un partenariat public-privé sera mis en place afin, d'une part, de faire profiter les opérateurs de l'information dont dispose l'État en matière d'analyse des menaces, et d'autre part, de permettre à l'État de s'assurer que les infrastructures essentielles au bon fonctionnement de la Nation disposent d'un niveau de protection adéquat. Un travail sera également engagé avec les équipementiers.

5. Adapter notre droit

Les nouveaux usages portés par le développement du cyberespace peuvent, si l'on n'est suffisamment vigilant, présenter des dangers pour nos libertés individuelles, le fonctionnement des infrastructures vitales ou l'équilibre de nos entreprises.

Notre cadre législatif et réglementaire doit suivre l'évolution des techniques. Les textes seront adaptés en fonction de l'apparition de nouvelles technologies ou de nouveaux usages, afin de renforcer la sécurité des particuliers et avec le souci du

respect de l'équilibre entre la volonté de peser le moins possible sur la compétitivité des entreprises et la nécessité pour l'État d'être en mesure d'intervenir dans le sens de l'intérêt supérieur de la Nation.

- S'agissant des opérateurs de communications électroniques, la transposition en droit français des directives européennes va permettre d'édicter de nouvelles règles de protection des systèmes d'information et d'alerte des autorités gouvernementales en cas d'incident.
- En ce qui concerne les autorités publiques, la mise en œuvre du « référentiel général de sécurité » (RGS) et son évolution permettront de relever significativement le niveau de protection de leurs systèmes d'information, notamment dans leurs relations avec les usagers.

6. Développer nos collaborations internationales

La sécurité des systèmes d'information repose en partie sur la qualité de l'échange d'informations entre les services compétents des divers États. La France cherchera à établir un large tissu de partenaires étrangers afin de favoriser le partage des données essentielles, comme, par exemple, les informations concernant les vulnérabilités ou les failles des produits et services.

Elle renforcera également ses échanges avec ses partenaires en matière de lutte contre la cybercriminalité.

De la même manière, les relations fortes entre alliés sont la base d'une cyberdéfense efficace. La France construit un cercle très restreint de partenaires de confiance avec lesquels des échanges opérationnels très approfondis seront menés.

7. Communiquer pour informer et convaincre

La sécurité des systèmes d'information repose tant sur la vigilance personnelle que sur l'organisation, les choix et mesures techniques portés par les entreprises et l'action des États.

Devant les conséquences potentielles d'une attaque majeure contre les systèmes d'information sur la vie du pays et de ses citoyens, la sensibilisation et la motivation des personnes et des organisations doivent être assurées.

Or, en France, l'information et le débat public sur les menaces que font peser les atteintes à la sécurité des systèmes d'information sur la défense et la sécurité nationale

ou, plus simplement, sur notre vie quotidienne, restent très largement à développer.

- Un soutien ciblé sera apporté par l'ANSSI aux décideurs afin de les aider à élaborer les mesures et à prendre les décisions nécessaires en matière de sécurité des systèmes d'information essentiels au bon fonctionnement de leurs organisations et à la protection de leur patrimoine technique, scientifique, commercial ou financier.

- Plus largement, une communication appropriée sera développée par l'ANSSI vers le grand public et les entreprises.

Glossaire

Botnet

Un *botnet*, autrement dit un réseau de robots, est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son maître de transmettre des ordres à tout ou partie des machines du *botnet* et de les actionner à sa guise.

Remarques : certains réseaux peuvent atteindre un nombre considérable de machines (plusieurs millions). Celles-ci peuvent faire l'objet de commerce illicite ou d'actions malveillantes contre d'autres machines.

Cryptanalyse

Processus de déchiffrement de données protégées au moyen de cryptographie sans être en possession des clés de chiffrement.

Cryptographie

Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée (ISO 7498-2).

Cryptologie

Science englobant la cryptographie et la cryptanalyse.

Cybercriminalité

Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdéfense

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cyberespace

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cybersécurité

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Faille

Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Information classifiée

L'article 413-9 du code pénal indique que « les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale » font l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Nétiquette

Charte établie en 1995 par l'Internet Engineering Task Force (IETF) présentant les règles de bienséance recommandées pour les échanges ayant lieu dans le cyberespace (voir charte : http://tools.ietf.org/html/rfc1855 ou http://www.sri.ucl.ac.be/rfc1855.fr.html pour une traduction française).

Glossaire

Opérateur d'importance vitale (OIV)

L'article R. 1332-1 du code de la défense précise que les opérateurs d'importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l'article L. 1332-1 du même code, ou parmi les gestionnaires d'établissements mentionnés à l'article L. 1332-2.

Un opérateur d'importance vitale :
- exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ;
- gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

Produit de sécurité

Dispositif matériel ou logiciel conçu pour protéger la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que les systèmes d'information offrent ou qu'ils rendent accessibles.

Résilience

En informatique, capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident.

Référentiel général de sécurité (RGS)

Ensemble des règles établies par l'ANSSI et prévues par l'ordonnance n° 2005-1516 du 8 décembre 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives » que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage. Les règles formulées dans le RGS s'imposent et sont modulées en fonction du niveau de sécurité retenu par l'autorité administrative dans le cadre de la sécurisation des services en ligne dont il est responsable. Ses conditions d'élaboration, d'approbation, de modification et de publication sont fixées par le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance citée relative à la sécurité des informations échangées par voie électronique. (voir http://www.ssi.gouv.fr/rgs).

Sécurité des systèmes d'information

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Système d'information

Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Février 2011

Agence nationale de la sécurité des systèmes d'information

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr

UNCLASSIFIED

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

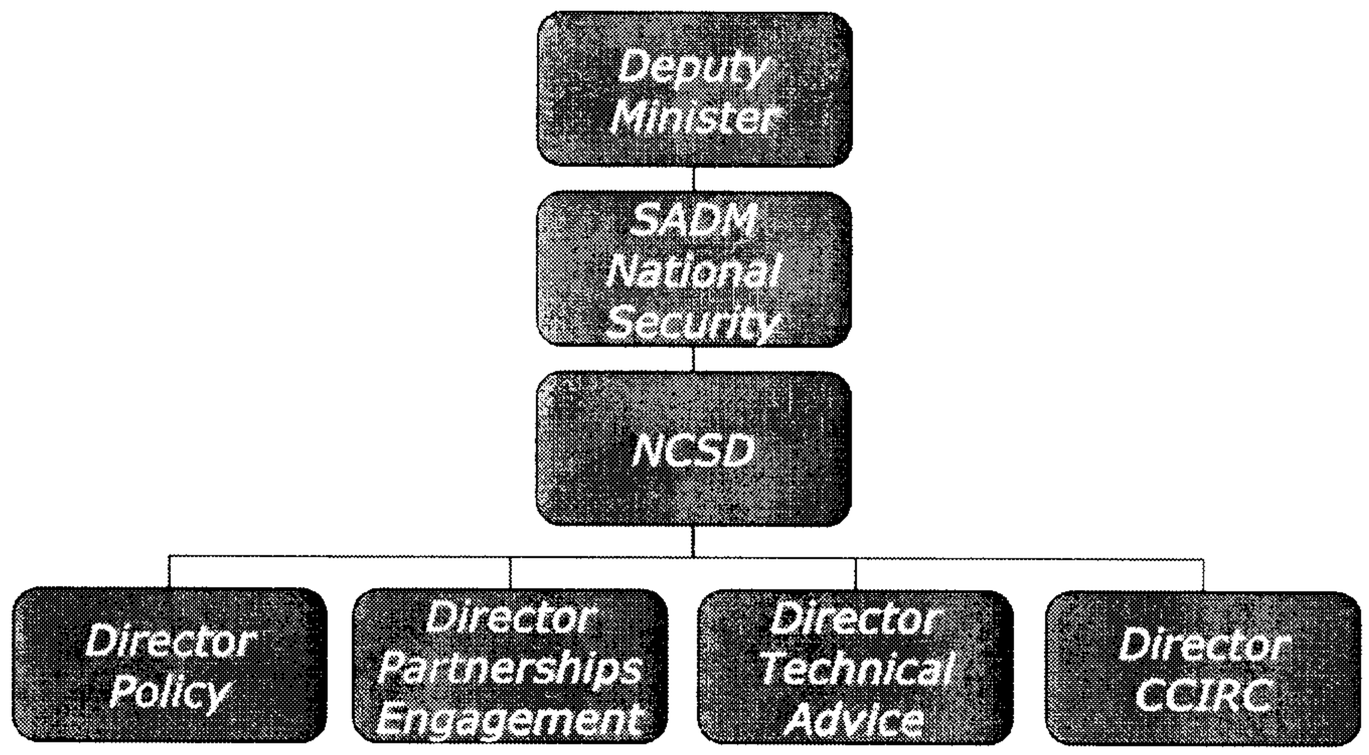
PS NCSD meetings with TrendMicro

Public Safety Canada Overview

Bob Gordon, Special Advisor on Cyber Security

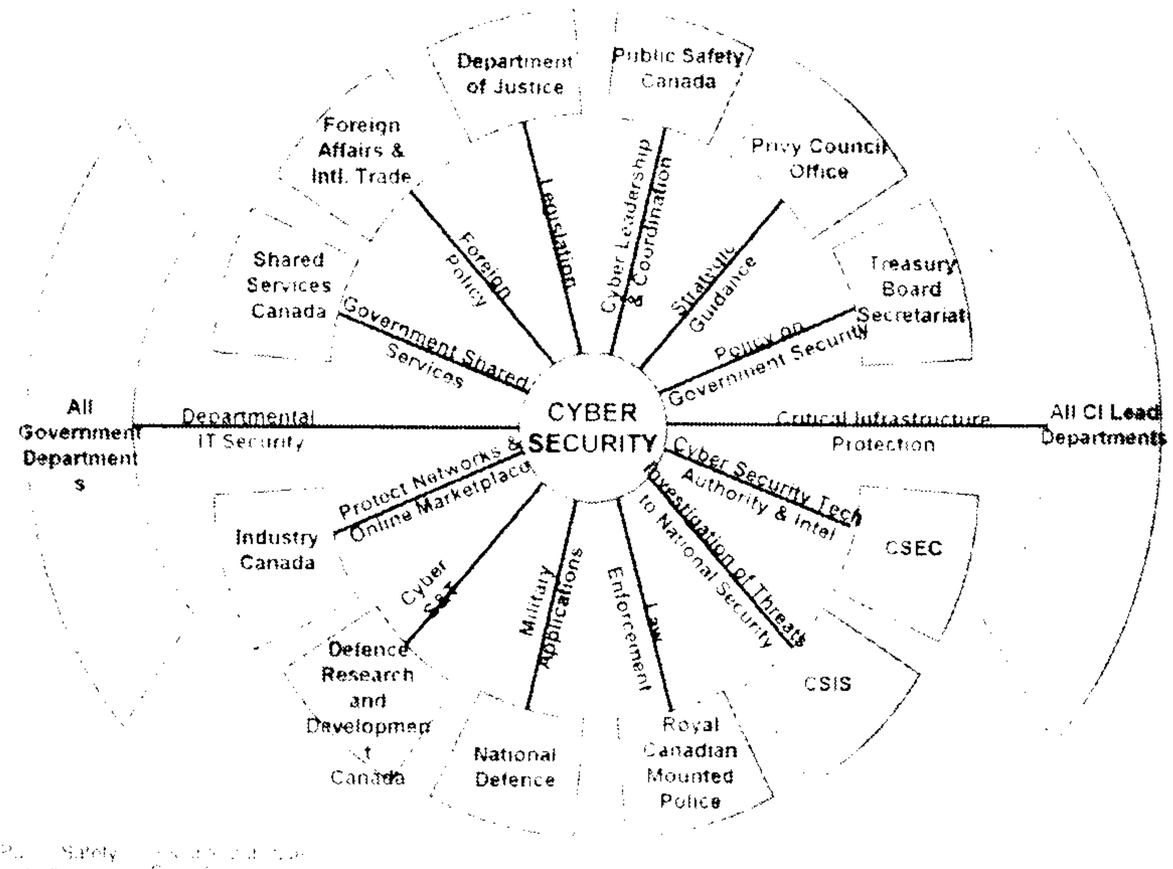
January 26, 2012

Canada

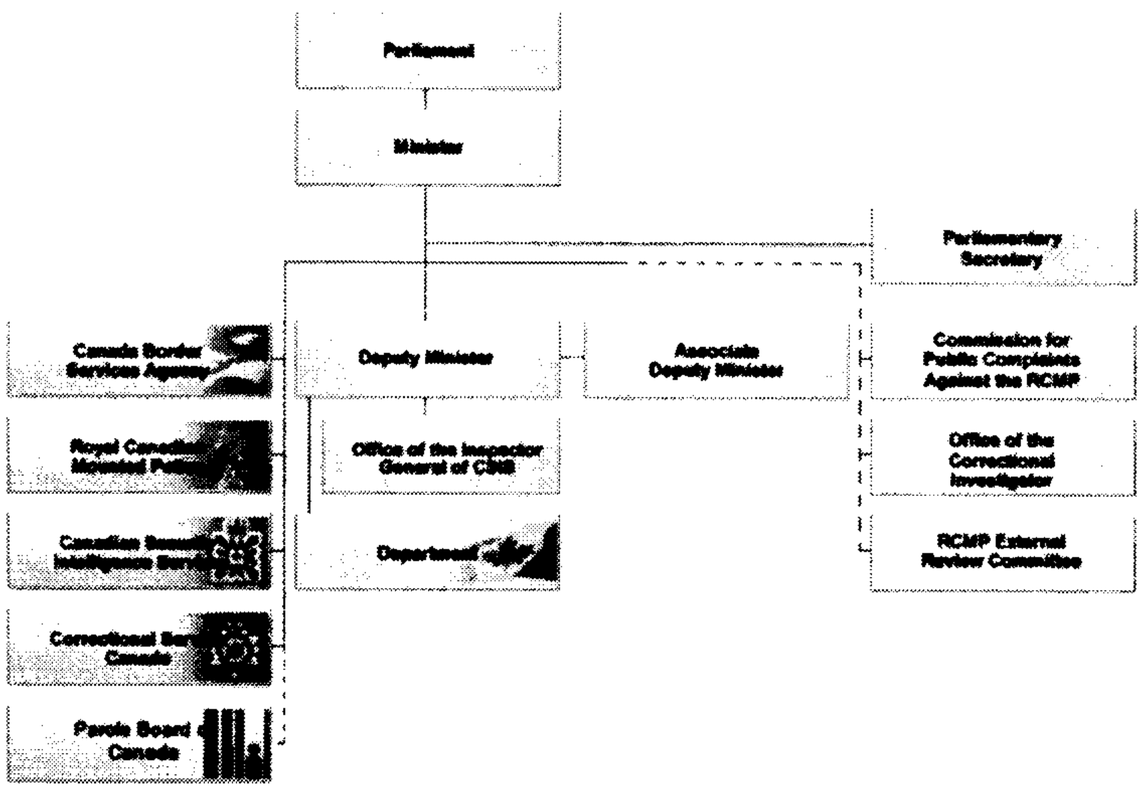


UNCLASSIFIED

Cyber-related roles and responsibilities within the Government of Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**



- On June 20, 2011, the responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the Cyber Threat Evaluation Centre, which is the computer emergency response team for federal departments and agencies.
  - CCIRC is now the national computer emergency response team for provinces, territories and critical infrastructure sectors.

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, mitigation, and response to cyber events.

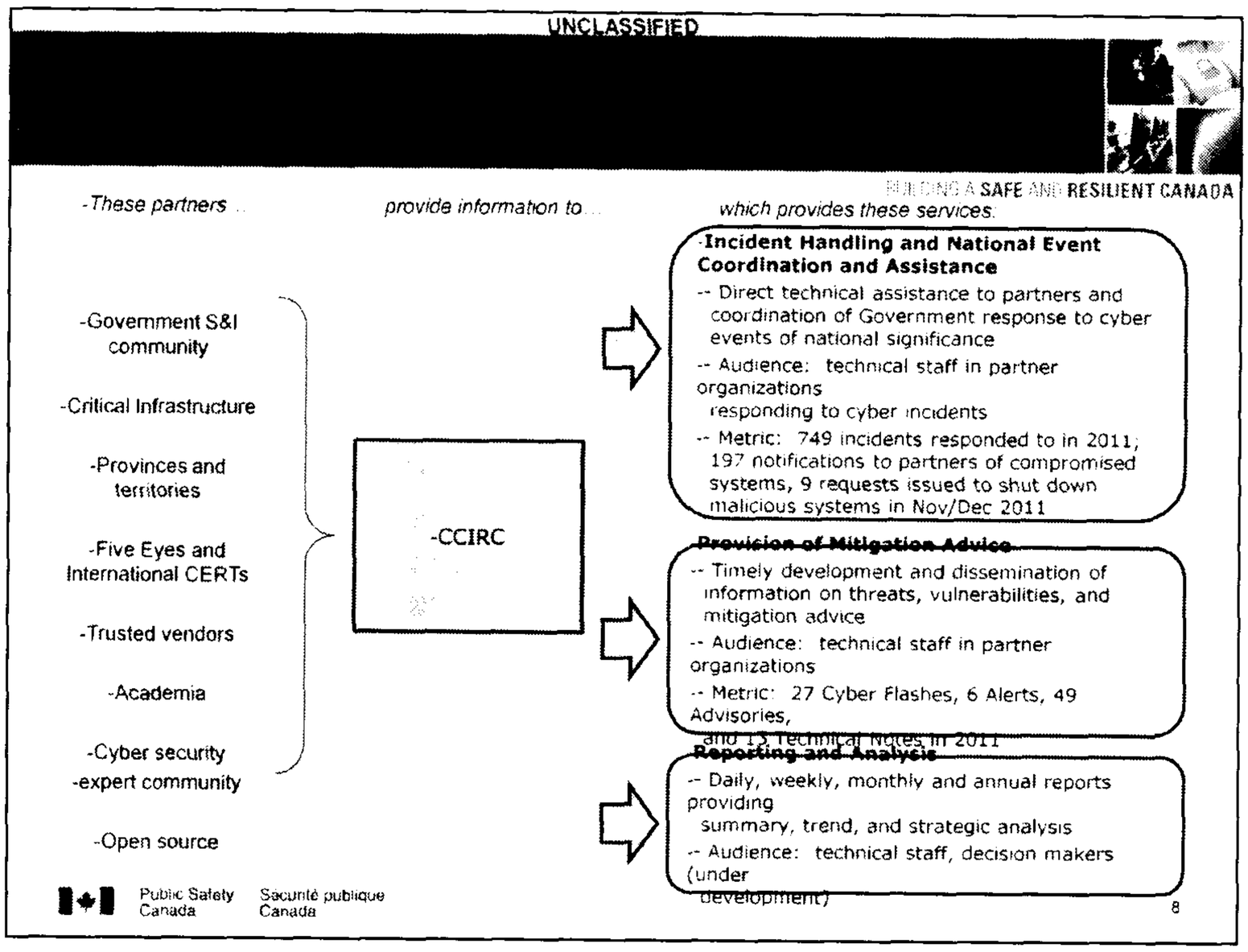
CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

- Incident response centre
  - primary contact point into Government for domestic and international partners
  - CCIRC subject matter experts respond 9-5, 5 days a week
  - after hours coverage by Government Operations Centre

- Computer lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors

- Personnel
  - Mainly highly specialized computer specialists (CS)
  - Augmented by non-computer specialists for analysis of multi-source intelligence and technical data and writing strategic assessments
  - Additional staff planned to support 15/7 operations
- Organized into three functions:
  - Incident Handling – assists partners in identifying, mitigating, and managing incidents
  - Technical Support – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis
  - Strategic Initiatives and Situational Awareness – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers

- Exploring secondments from other departments (CSIS, CSEC, etc.) to staff analytical positions



- !!! Provide benchmark comparison to US, Australia in terms of products released

-Currently Produced

-In Development

Product	Cyberflash	Daily Report	Weekly Technical Report	Information Notes	Technical Report	Advisory	Monthly Statistical Report	Weekly SA Report	Monthly SA Rollup	Issue of the Month	Annual Report	Ad hoc
Description	Time sensitive reports for immediate security issues - Security fix unavailable	Daily situation report	Summary of daily reports, CCIRC products / events / activities / indicators / and cyber reporting	Report on significant cyber events - for general awareness	Detailed report WRT a cyber security issue - Ad hoc	Cyber security advisory on threat and vulnerability - Security fix available	All CCAP products + (1) incidents handled ; (2) take down requests; and (3) victim notifications	Notable cyber events / CCIRC products / open source reports	Summary of weekly SA reports for ADM	Single strategic cyber issue analysis	Yearly status report WRT Canadian cyber security	Strategic cyber issue 1 pagers
Clients	P/T/CI operational contacts	CCIRC / trusted GoC partners	P/T/CI/GoC operational contacts	P/T/CI/GoC - Posted on website	P/T/CI operational contacts	P/T/CI operational contacts - Posted on website	Public Safety /other Federal departments	GoC managers / executives P/T/CI partners	Public Safety / Senior GoC executives	P/T/CI partners	Public	Public Safety

-Operational / Technical

-Strategic

- Signals cyber security as a priority investment for the Government of Canada.
- Coordinates and unifies domestic and international action.
- Built on three pillars:
  1. Secure Government systems.
  2. Partner to secure systems outside the Government of Canada.
  3. Help Canadians to be secure online.

Legislation

- Passed two pieces of legislation to enhance cyber security.

  Anti-Spam Bill:

  - Seeks to deter the most damaging and deceptive forms of spam from occurring in Canada.
  - Authorizes the creation of a spam reporting centre.

  - Bill S-4:

    - Amends the *Criminal Code* to create three new offences related to identity theft, with five-year maximum sentences.
    - Authorizes courts to order offenders to pay restitution to a victim of identity theft as part of their sentence.

- Examining ways to provide law enforcement with modernized investigative tools to address cyber crimes.

Engagement Activities

- The objective is to implement the Strategy in collaboration with partners
- Using the Critical Infrastructure framework:
  - 10 CI sectors
  - National Cross Sector Forum process
- Currently targeting the cyber engagement with the:
  - Provinces and Territories;
  - Financial sector;
  - Energy; and
  - Telecommunications
- International Partners

Canadian Security Telecommunications Advisory Council

- CSTAC is comprised of senior executives from the public and private sectors. It provides a forum to:
  - exchange information;
  - collaborate strategically on current and evolving issues that may affect the confidentiality, integrity or availability of the telecommunications infrastructure; and
  - provide advice on measures to address these issues.
- The Committee is focusing on several areas:
  - risks to the critical telecommunications infrastructure, including proactive and mitigating measures to address threats and vulnerabilities;
  - network monitoring;
  - interdependencies; and
  - emergency management and disaster recovery.

Some Points for Discussion

- Is there value in a more formal partnership between Public Safety and security vendors? Are there good international examples?
- Would there be value in establishing a collaborative group between trusted security vendors and Public Safety?
- What would the key objectives of the relationship be?
- Could we take a sector-specific approach to disseminating threat information / mitigation advice in a targeted way?

UNCLASSIFIED

Progress on Implementation and Upcoming Initiatives

- Updating laws to reflect the realities of the digital world.
- Developed cyber security public awareness campaign.
- Redefined the responsibilities for cyber security incidents affecting Canadian networks.
- Streamlined and consolidated Government IT infrastructure, and created Shared Services Canada.

s.14(a)

- Created the National Cross-Sector Forum to build partnerships, improve information sharing, and address the physical and cyber vulnerabilities that span all critical infrastructure sectors.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

Canada – United States

Cyber Security Action Plan
DHS & PS Discussion Strawman

January 26, 2012

Canada

Proposed Action Plan Elements

BUILDING A **SAFE** AND **RESILIENT CANADA**

For discussion:

1. Enhanced collaboration between national cyber operations centers
2. Joint engagement and information sharing with private sector
3. Coordination of cyber incident response communications
4. Cooperation on cyber security public awareness & education
5. Expansion of joint leadership on international cyber security issues

Does this correctly scope PS-DHS cyber activity?

Enhanced Collaboration

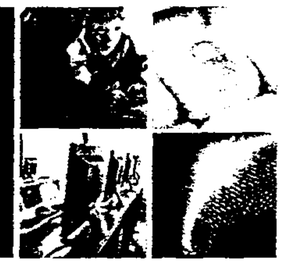
BUILDING A **SAFE** AND **RESILIENT CANADA**

For discussion:

- Align services and information products provided to external clients
- Joint analysis and technical work
- Improve shared cyber security situational awareness by coordinating internal trend and summary reports
- Better coordinate and align cyber incident management processes and protocols, especially those dealing with threats to shared critical infrastructure
- Jointly participate in exercises to test and improve processes and mechanisms
- Exchange of tools, practices, and resources
- Highlight industrial control systems work

What are quick hits? What is already in progress?

Joint Engagement with Private Sector



BUILDING A **SAFE** AND **RESILIENT CANADA**

For discussion:

- Binational calendar of private sector engagements and briefings
- Joint threat and sector-specific briefing material
- Compare protocols for sharing information with, and assisting, critical infrastructure and private sector stakeholders

What is in NCSD/NCSD control? What would require other government stakeholders?

Coordination of Incident Communications

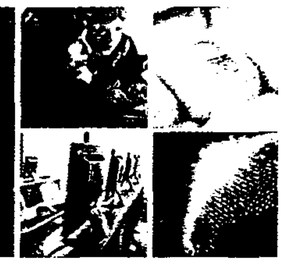
BUILDING A **SAFE** AND **RESILIENT CANADA**

For discussion:

- Joint cyber incident communications protocol for ongoing cyber security operations
- Production of aligned and, when appropriate, joint communications products

Is this ambitious enough?

Cooperation on Public Awareness & Education



BUILDING A **SAFE** AND **RESILIENT CANADA**

For discussion:

- Collaboration on public awareness campaigns, including websites, social media activities, education material, etc.
- Collaboration on Cyber Security Awareness Month (October)

How do / should we involve the private sector? International partners?

Expand Joint Leadership Internationally

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

For discussion:

[redacted]

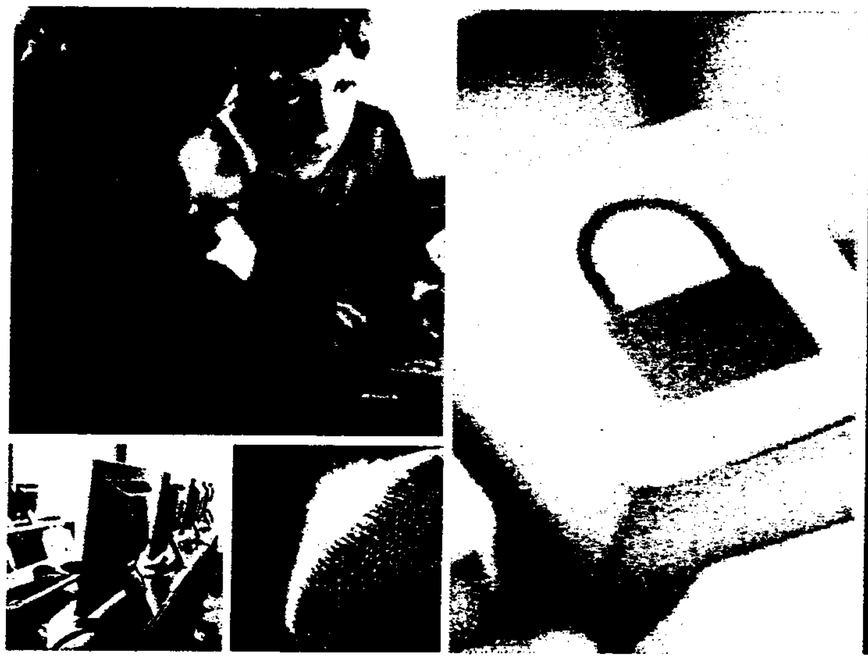
- Promulgate cyber security best practices, particularly in the service of third countries seeking to build capacity

[redacted]

What can PS-DHS do? What other stakeholders needs to be involved?

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

Canada

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

DHS NCSD visit to PS NCSD

Canada's Cyber Security Strategy – 15 months in

January 26, 2012

Canada

Public Safety Canada Portfolio

BUILDING A **SAFE** AND **RESILIENT CANADA**

Parliament

Minister

Deputy Minister — **Associate Deputy Minister**

Parliamentary Secretary

- Canada Border Services Agency
- Royal Canadian Mounted Police
- Canadian Security Intelligence Service
- Correctional Service Canada
- Parole Board of Canada

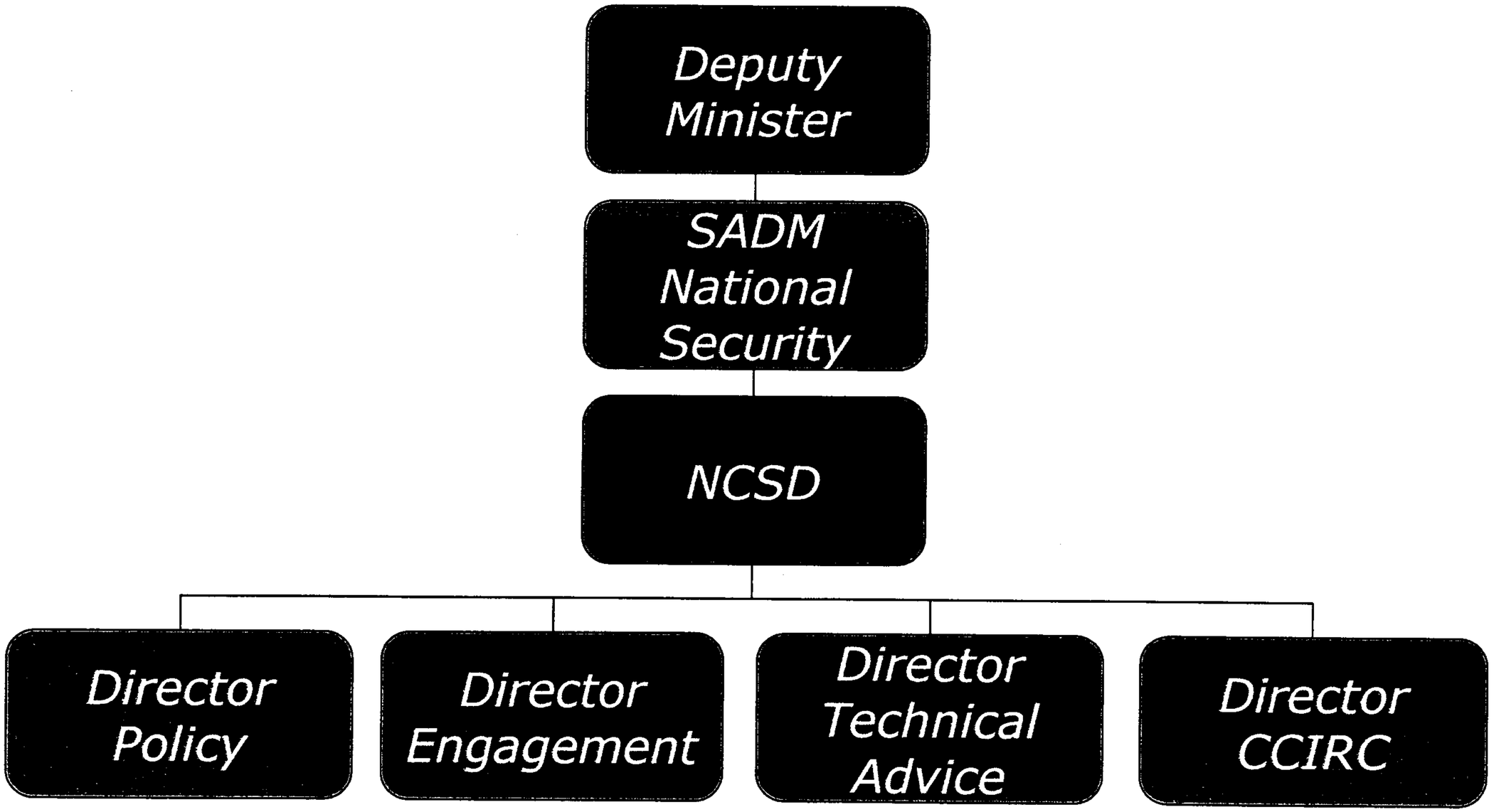
Office of the Inspector General of CSIS

Department

- Commission for Public Complaints Against the RCMP
- Office of the Correctional Investigator
- RCMP External Review Committee

National Cyber Security Directorate

BUILDING A **SAFE** AND **RESILIENT CANADA**



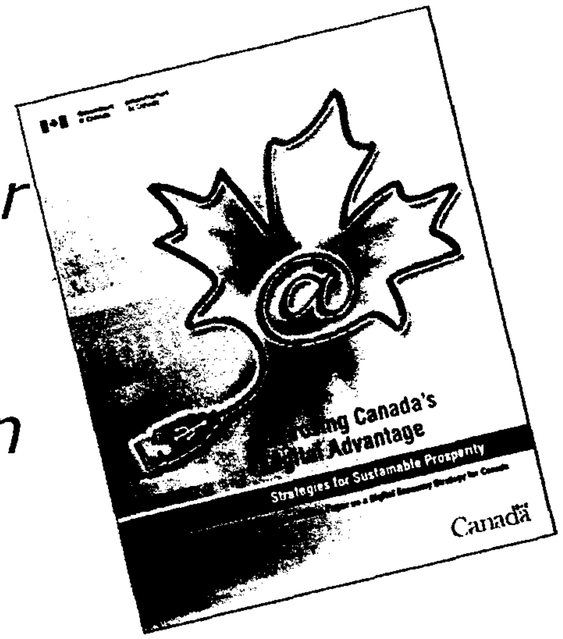
Government of Canada Initiatives

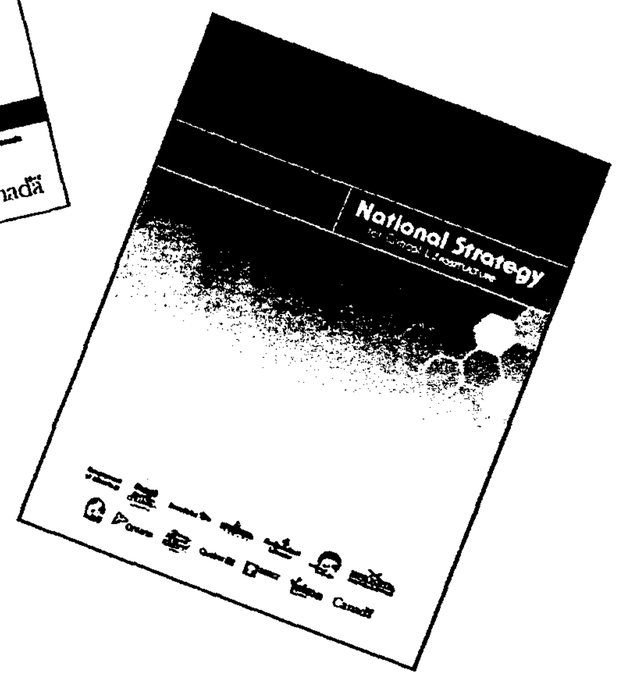
BUILDING A **SAFE** AND **RESILIENT CANADA**

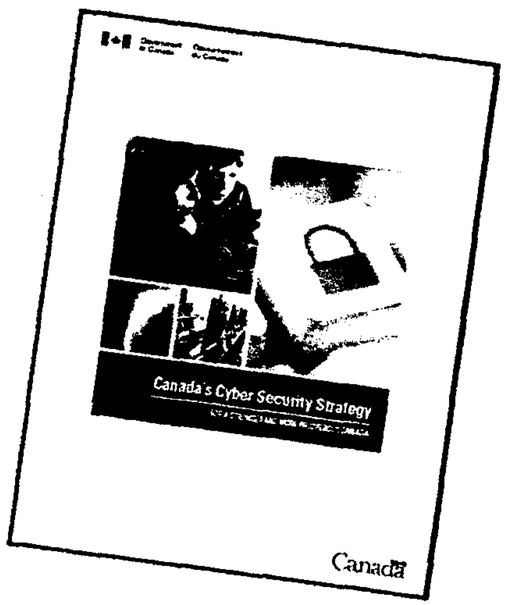
- *Consultation Paper on a Digital Economy Strategy for Canada* (May 2010).

- *National Strategy and Action Plan for Critical Infrastructure* (May 2010).

- *Canada's Cyber Security Strategy* (October 2010).







Canada's Cyber Security Strategy

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Signals cyber security as a priority investment for the Government of Canada.

- Coordinates and unifies domestic and international action.

- Built on three pillars:

  1. Secure Government systems.

  2. Partner to secure systems outside the Government of Canada.

  3. Help Canadians to be secure online.

Canada's Cyber Security Strategy

BUILDING A CANADA

Leverage existing activities and investments

Canada's Cyber Security Strategy

Meet our goals

Support national priorities

Key legislation and policies

Structural changes

Cyber Security Awareness Month

National Strategy & Action Plan for Critical Infrastructure

Secure Government systems

Partner to secure systems outside the Government of Canada

Help Canadians to be secure online

Strengthen capability

Build credibility

Promote awareness

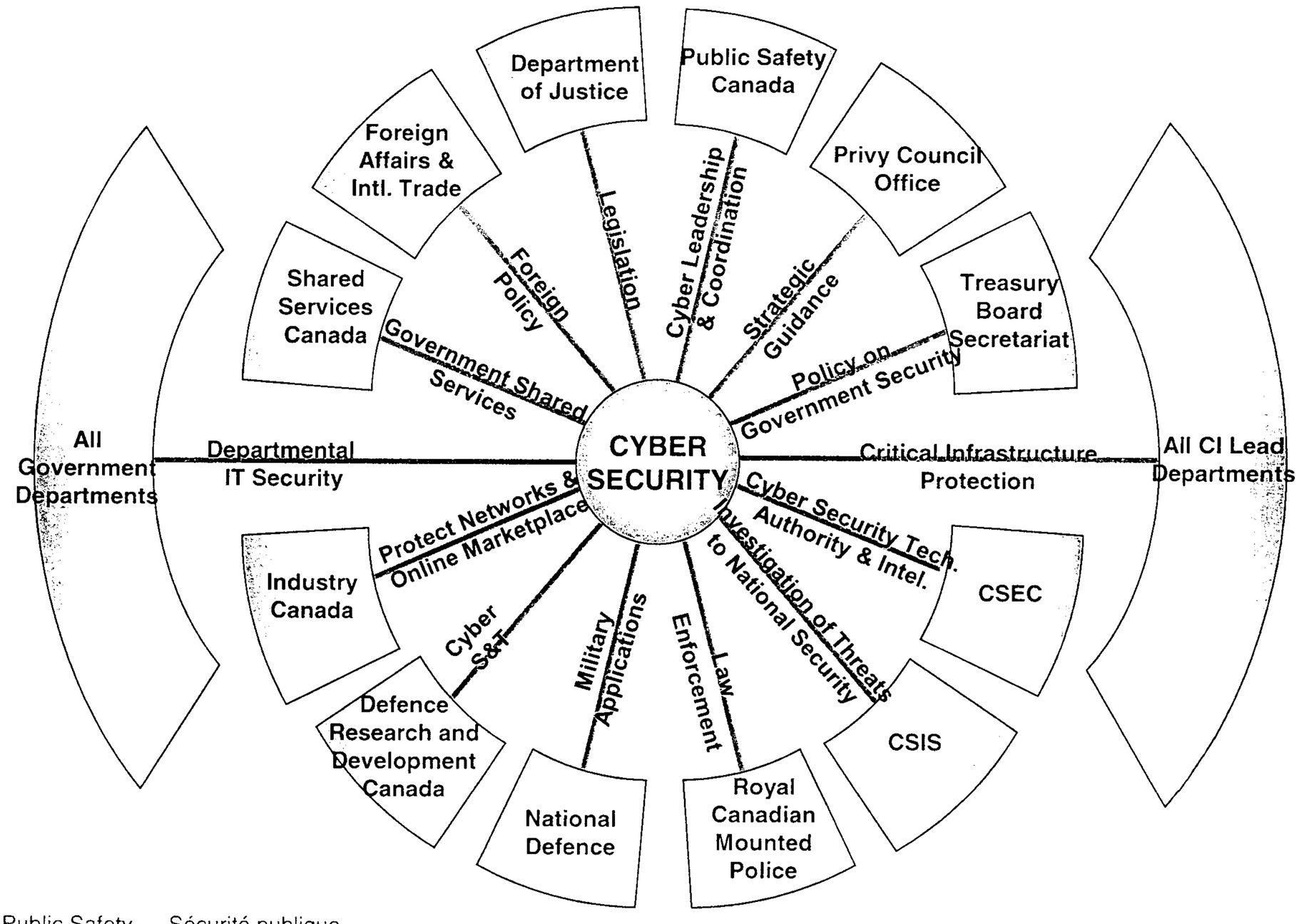
National security

Economic prosperity

Quality of life

Cyber Security Roles and Responsibilities within the Government of Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

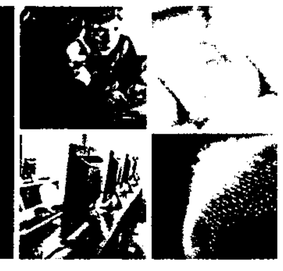


Progress on Implementation and Upcoming Initiatives

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Updating laws to reflect the realities of the digital world.
- Developed cyber security public awareness campaign.
- Redefined the responsibilities for cyber security incidents affecting Canadian networks.
- Streamlined and consolidated Government IT infrastructure, and created Shared Services Canada.
- Engaged provincial and territorial governments to shape a joint action plan to guide collaboration on cyber security matters.
- Created the National Cross-Sector Forum to build partnerships, improve information sharing, and address the physical and cyber vulnerabilities that span all critical infrastructure sectors.

Legislation



- Passed two pieces of legislation to enhance cyber security.
  - Anti-Spam Bill (passed December 2010):
    - Seeks to deter the most damaging and deceptive forms of spam from occurring in Canada.
    - Authorizes the creation of a spam reporting centre.
  - Bill S-4 (passed October 2009):
    - Amends the *Criminal Code* to create three new offences related to identity theft, with five-year maximum sentences.
    - Authorizes courts to order offenders to pay restitution to a victim of identity theft as part of their sentence.
- Examining ways to provide law enforcement with modernized investigative tools to address cyber crimes.

Get Cyber Safe.ca Campaign

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Public Safety Canada's Communications Directorate has launched a national public awareness advertising campaign to deliver on the third pillar of *Canada's Cyber Security Strategy.*
- Provides Canadians with information on cyber threats in order for them to take action to protect themselves and their personal information.
- Includes advertising, a cyber-specific website, marketing partnerships and international coordination of messaging, as well as issues management in response to cyber incidents.
- Was launched in October to coincide with Cyber Security Awareness Month and the one-year anniversary of the Strategy.

Public Awareness Campaign

BUILDING A **SAFE** AND **RESILIENT CANADA**

Government of Canada / Gouvernement du Canada

Canada

Get Cyber Safe

GetCyberSafe.ca

Français | Home | Contact Us | Help | Search | canada.gc.ca

Home

Know the Risks

- Online Activities
- Common Threats
- Scams and Fraud

Protect Yourself

- Protect Your Identity
- Protect Your Money
- Protect Your Family

Protect Your Devices

- Computers, Laptops and Tablets
- Mobile Devices
- Home Networks
- Storage

Resources

GETCYBERSAFE

Make cyber safety a personal priority with tips and resources to help protect everything that's important to you.

Find out where the risks are

The first step to keeping yourself safe from online risks is knowing where they are.

Email | Banking & Finance | Social Networks | Mobile

Online Shopping | Entertainment Games & | Downloading & File Sharing | Voice Over Internet

Share | Email

Search

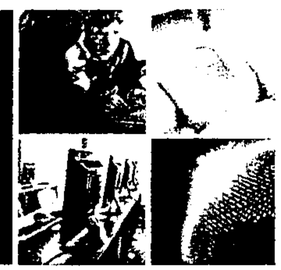
GetCyberSafe Video

See the Ad

It Happened to Me

Here's your chance to share your story and read about others' experiences. By passing along any helpful information you've

Division of Cyber Security Roles in Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**

- On June 20, 2011, the responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the Cyber Threat Evaluation Centre, which is the computer emergency response team for federal departments and agencies.
  - CCIRC is now the national computer emergency response team for provinces, territories and critical infrastructure sectors.

Shared Services Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

- Effective August 4, 2011, the Government streamlined and consolidated its IT architecture in the areas of email, data centres and networks.
- This will produce savings and reduce the Government's footprint; strengthen security and the safety of Government data to ensure Canadians are protected; and realize economies of scale and make it more cost-effective to modernize these IT services.
- All resources associated with the delivery of email, data centre and network services are being transferred from 44 of the more IT-intensive departments to a new entity called Shared Services Canada.

Meetings with Provincial and Territorial Governments

- Initiated dialogue with provincial and territorial interlocutors to strengthen intergovernmental engagement on cyber security.
- Key objectives from a federal perspective:
  - clarify national operational roles and responsibilities;
  - improve information sharing;
  - engage critical infrastructure and private sectors;
  - ensure a better informed population by maximizing resources and leveraging provincial and territorial access to the public;
  - establish a forum for consultation on legislative and policy undertakings;
  - explore interest in the development of a national cyber incident response framework; and
  - ensure a cohesive front in regards to international efforts and pressures.

National Cross-Sector Forum

- Four priorities were identified at the inaugural meeting:
  - Develop a common understanding of critical infrastructure within and across sectors.
  - Establish an information sharing framework for sensitive information shared between public-private and private-private entities.
  - Identify key assets and critical systems.
  - Identify key interdependencies and vulnerabilities.
- Engaged with provincial and territorial departments of telecommunications, energy and natural resources.

Canadian Security Telecommunications Advisory Council

BUILDING A **SAFE** AND **RESILIENT CANADA**

- CSTAC is comprised of senior executives from the public and private sectors. It provides a forum to:
  - exchange information;
  - collaborate strategically on current and evolving issues that may affect the confidentiality, integrity or availability of the telecommunications infrastructure; and
  - provide advice on measures to address these issues.
- The Committee is focusing on several areas:
  - risks to the critical telecommunications infrastructure, including proactive and mitigating measures to address threats and vulnerabilities;
  - network monitoring;
  - interdependencies; and
  - emergency management and disaster recovery.

Canada-U.S. Cooperation

- Long history of bilateral cooperation on cyber security:
  - critical infrastructure protection;
  - operational cyber incident coordination (CERT to CERT);
  - bilateral and multi-national collaboration in exercises; and
  - intelligence and information sharing.

- Recent years have seen this accelerate and broaden through the Emergency Management Consultative Group and other mechanisms:
  - policy and program development;
  - Beyond the Border Perimeter Vision
    - collaboration through multinational fora
    - enhanced operations and private sector outreach;

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

[redacted]

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

Canada

Public Safety Canada | Sécurité publique Canada

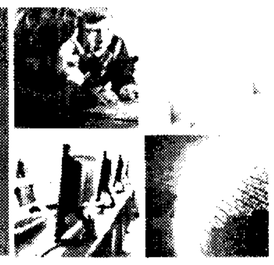
SAFE AND RESILIENT CANADA

Cyber Security in Canada

Ernst & Young CEO Breakfast Sessions
February 2012

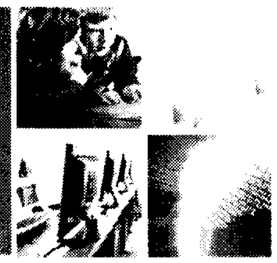
Canada

The Cyber Environment: Where we live, work and play



- **2 Billion Internet users and growing...**
  - 340+ Billion web sites
  - 294 Billion emails sent every day, 2.8M /sec. (Est. Radicati Group. 2010)
  - 700 Million users on Facebook...
- **Heavy reliance on IT by citizens, business and government**
  - >130 GC services on-line
  - 79% Canadians on-line (2010 Canadian Internet Use Survey. Statistics Canada)
  - $16 Billion on-line sales in Canada in 2010; doubled by 2015; $412 Billion global sales (Statistics Canada. 2010)
- **As technology evolves, the way you do business will continue to change**

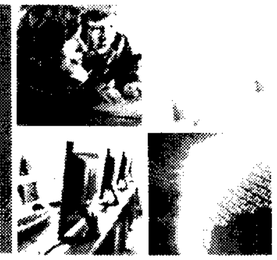
The Cyber Environment: Where we store what we value



"Information about the package is as important as the package itself."
– Frederick W. Smith, founder of FedEx

- Information a critical underpinning of competitive advantage
  - intellectual property
  - plans and strategies
  - customer profiles
  - reputation
- Our ever-increasing need for analysis, information and insight has driven systems integration to deliver better information to leaders
- Integrating information has huge upsides for decision-making, but creates greater risk

The Cyber Environment: Who's Out There?



State Sponsored Cyber Espionage and Military Activities

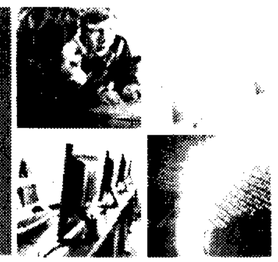
Many nations with cyber exploitation capabilities

- Organized Crime
  - Identity theft
  - Electronic bank heists
  - Illicit trade
- Terrorist Networks
  - Recruitment / propaganda
  - Financing
  - Planning
- Low level Actors
  - Thrill seekers
  - Hacktivists

Cyber Threat Attributes

- Inexpensive
- Basic skills can cause much damage
- Attack detection and attribution difficulty increases as attack sophistication increases

The Cyber Environment: Where information and wealth is exploited

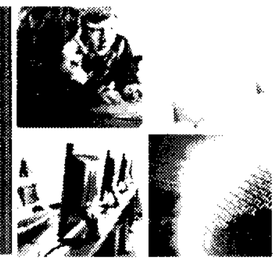


- IT systems and networks are lucrative targets
  - 86% of large commercial organizations self-reported attacks (CA Canada . "Security and Privacy Survey" 2008)
  - Cybercrime losses, globally $114 B est. (Norton Cybercrime Report, 2011)
  - In Canada $4.7 B est. was lost in productivity and remediation costs due to malware remediation and reactive measures (Norton Cybercrime Report)
  - Identity theft is estimated to cost the Canadian economy $2.5 B per year (Canadian Council of Better Business Bureaus)

A new piece of malware is created every 1.5 seconds*

(Trend Micro, 2009)

The Cyber Environment: Where information and wealth is exploited



- 1 in every 284 emails contains malware
- 1 in every 445 emails contains a phishing attempt
- 95 Billion phishing emails in 2010

Phishing Defined...

- An email sent to broad audience to allow for the delivery of malware
- Messages contain socially engineered text designed to appear legitimate and trustworthy

Symantec Reports:

- 2008: 1.6M new threat signatures
- 2010: 6M new threat signatures

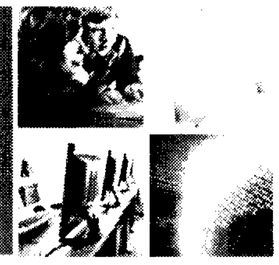
McAfee Reports:

- >60 million pieces of malware

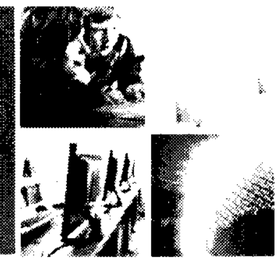
- Legitimate web sites hosting malware: 3200 identified daily
- Canada hosted 5-10% of the world's phishing sites in 2010
- Botnets can deliver 3-4 million new infections per month

SOURCE: (Norton Cybercrime Canada Report, 2011)

Cyberspace changes approach to risk



- Interconnectedness facilitates targeting and stealing business information assets
- It's about the weakest link: vulnerabilities of those to whom you're connected become yours
- Bigger walls won't work – you can't protect everything perfectly
- Even with the best technology in place, the human factor still needs to be taken into account

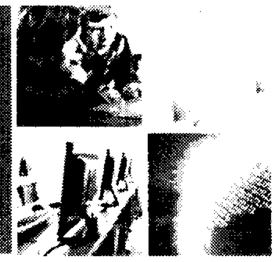


The majority of cyber incidents relate to known vulnerabilities for which there are known solutions

Consider key measures to reduce the effectiveness of current cyber intrusion attempts

Cyber Security Best Practices

1. Consolidate Internet traffic
2. Patch IT systems to combat vulnerabilities
3. Whitelist safe Internet browsing
4. Limit local administration privileges
5. Increase user awareness of current cyber threats



Cyber Realities

- IT best practices only get us part of the way there
- Rate of threat change causes unsustainable response treadmill
- We will never eliminate threat risks but we can make it as hard and as expensive as possible for attackers

There is no Silver Bullet

- Advanced persistent threats, such as state-sponsored cyber espionage, will continue
- Need persistent vigilance and monitoring
- Invest in continuous collaboration with key stakeholders across all levels of government

How do you manage your risk?

- Take the time to protect what is critical:
  - How do you secure your competitive advantage?
  - How secure are your partners and suppliers?
  - What legal obligations do you have to your customers?

- Securing your information means breaking down barriers between information technology, personnel, and physical security silos

- The security perimeter must encompass not only your physical assets but also your personnel and business relationships

The Government takes this seriously

- Launched *Canada's Cyber Security Strategy* in October 2010 to coordinate response across a range of policy and operational areas

- Bolstered Canadian Cyber Incident Response Centre's (CCIRC) ability to provide national cyber incident response

- Engaging with international partners to share best practices and address legislative gaps

- Engaging domestically with provinces, territories, and critical infrastructure owners and operators

Public Safety Canada | Sécurité publique Canada

GC Response to Threat Environment

Canada's Cyber Security Strategy

Achieve cyber integrity of government

Protect critical assets and information

Combat cyber facilitated crime and promote public awareness

Strengthen Canada's national security and contribute to global security

Sustain Canada's economic prosperity

Protect Canadian citizens on line

October 2010

Canada

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT** CANADA

Critical Information Infrastructure Protection and Cyber Security

Canada's Cyber Security Strategy – One Year Later

January 31 - February 1, 2012

Montreal Control Systems Security Workshop

Canada

Government of Canada Initiatives

- *Consultation Paper on a Digital Economy Strategy for Canada* (May 2010).

- *National Strategy and Action Plan for Critical Infrastructure* (May 2010).

- *Canada's Cyber Security Strategy* (October 2010).

Canada's Cyber Security Strategy

- Signals cyber security as a priority investment for the Government of Canada.

- Coordinates and unifies domestic and international action.

- Built on three pillars:

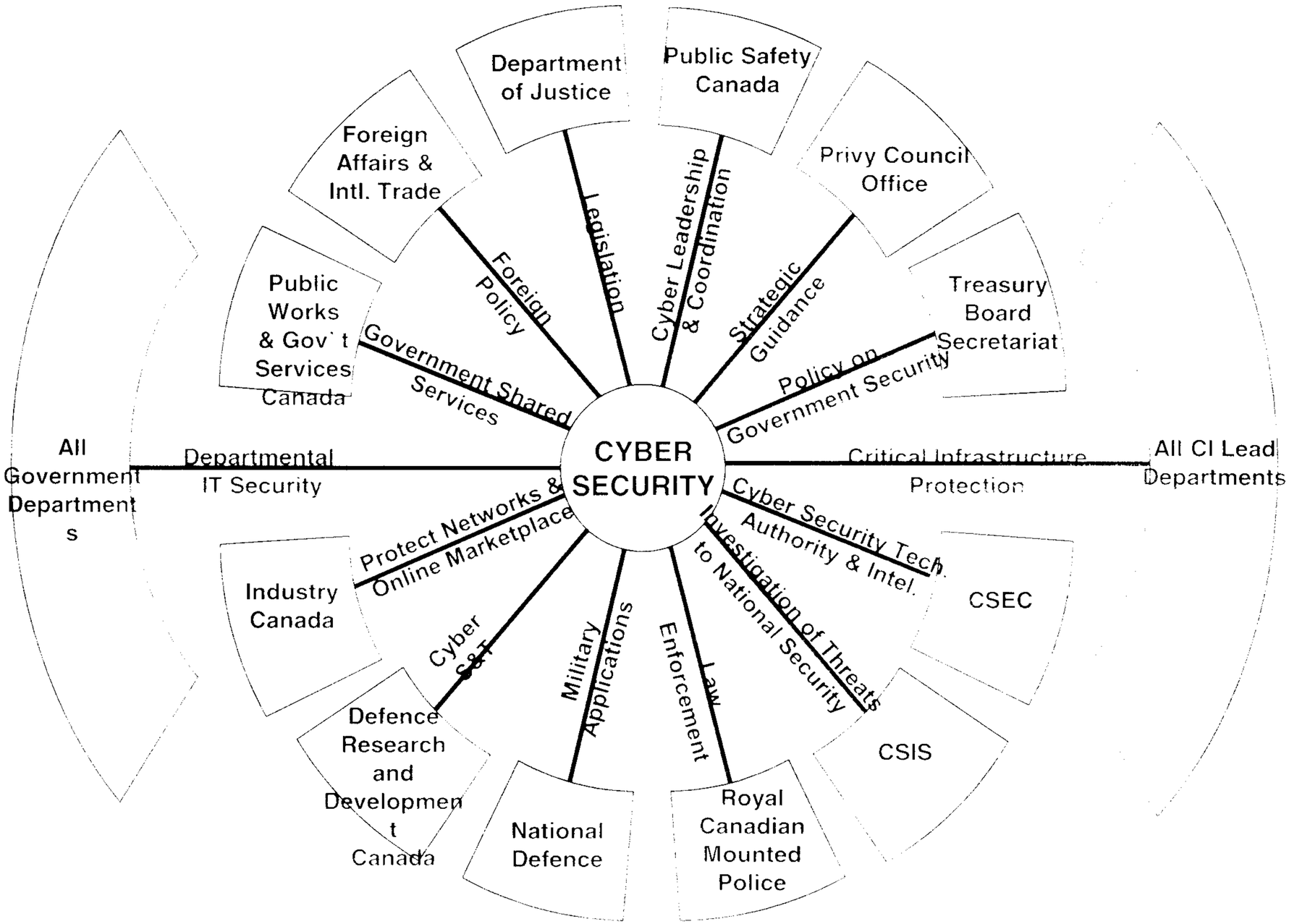
1. Secure Government systems.

2. Partner to secure systems outside the Government of Canada.

3. Help Canadians to be secure online.

UNCLASSIFIED

Cyber Security Roles and Responsibilities within the Government of Canada



000807

Progress on Implementation and Upcoming Initiatives

- Updating laws to reflect the realities of the digital world.
- Developed cyber security public awareness campaign.
- Redefined the responsibilities for cyber security incidents affecting Canadian networks.
- Streamlined and consolidated Government IT infrastructure, and created Shared Services Canada.

s.14(a)

- [redacted]
- Created the National Cross-Sector Forum to build partnerships, improve information sharing, and address the physical and cyber vulnerabilities that span all critical infrastructure sectors.

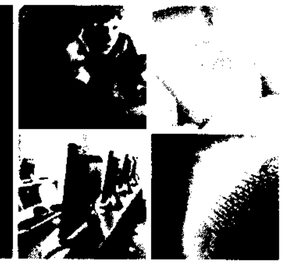
Legislation

- Passed two pieces of legislation to enhance cyber security.
  - Anti-Spam Bill:
    - Seeks to deter the most damaging and deceptive forms of spam from occurring in Canada.
    - Authorizes the creation of a spam reporting centre.
  - Bill S-4:
    - Amends the *Criminal Code* to create three new offences related to identity theft. with five-year maximum sentences.
    - Authorizes courts to order offenders to pay restitution to a victim of identity theft as part of their sentence.
- Examining ways to provide law enforcement with modernized investigative tools to address cyber crimes.

Get Cyber Safe.ca Campaign

- Public Safety Canada's Communications Directorate has launched a national public awareness advertising campaign to deliver on the third pillar of *Canada's Cyber Security Strategy*.
- Provides Canadians with information on cyber threats in order for them to take action to protect themselves and their personal information.
- Includes advertising, a cyber-specific website, marketing partnerships and international coordination of messaging, as well as issues management in response to cyber incidents.
- Was launched in October to coincide with Cyber Security Awareness Month and the one-year anniversary of the Strategy.

[redacted]



Know the Risks

- Online Activities
- Common Threats
- Scams and Fraud

Protect Yourself

- Protect Your Identity
- Protect Your Money
- Protect Your Family

Protect Your Devices

- Computers, Laptops and Tablets
- Mobile Devices
- Home Networks
- Storage

Resources

GETCYBERSAFE

Make cyber safety a personal priority with tips and resources to help protect everything that's important to you.

GetCyberSafe Video

It Happened to Me

Here's your chance to share your story and read about others' experiences. By passing along any helpful information you've

Division of Cyber Security Roles in Canada

- On June 20, 2011, the responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the Cyber Threat Evaluation Centre, which is the computer emergency response team for federal departments and agencies.
  - CCIRC is now the national computer emergency response team for provinces, territories and critical infrastructure sectors.

Shared Services Canada

- Effective August 4, 2011, the Government streamlined and consolidated its IT architecture in the areas of email, data centres and networks.
- This will produce savings and reduce the Government's footprint; strengthen security and the safety of Government data to ensure Canadians are protected; and realize economies of scale and make it more cost-effective to modernize these IT services.
- All resources associated with the delivery of email, data centre and network services are being transferred from 44 of the more IT-intensive departments to a new entity called Shared Services Canada.

Meetings with Provincial and Territorial Governments

- Initiated dialogue with provincial and territorial interlocutors to strengthen intergovernmental engagement on cyber security.
- Key objectives from a federal perspective:
  - clarify national operational roles and responsibilities;
  - improve information sharing;
  - engage critical infrastructure and private sectors;
  - ensure a better informed population by maximizing resources and leveraging provincial and territorial access to the public;
  - establish a forum for consultation on legislative and policy undertakings;
  - explore interest in the development of a national cyber incident response framework; and
  - ensure a cohesive front in regards to international efforts and pressures.

National Cross-Sector Forum

- Four priorities were identified at the inaugural meeting:
  - Develop a common understanding of critical infrastructure within and across sectors.
  - Establish an information sharing framework for sensitive information shared between public-private and private-private entities.
    - Identify key assets and critical systems.
    - Identify key interdependencies and vulnerabilities.
- Engaged with provincial and territorial departments of telecommunications, energy and natural resources.

Canadian Security Telecommunications Advisory Council

- CSTAC is comprised of senior executives from the public and private sectors. It provides a forum to:
  - exchange information;
  - collaborate strategically on current and evolving issues that may affect the confidentiality. integrity or availability of the telecommunications infrastructure: and
  - provide advice on measures to address these issues.
- The Committee is focusing on several areas:
  - risks to the critical telecommunications infrastructure. including proactive and mitigating measures to address threats and vulnerabilities;
  - network monitoring;
  - interdependencies; and
  - emergency management and disaster recovery.

www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

Canada

UNCLASSIFIED

MEETING WITH PETER MACAULAY
HEAD CORPORATE SECURITY
OFFICE OF THE CORPORATE CHIEF INFORMATION OFFICER
ONTARIO GOVERMENT

OBJECTIVE(S)

- Introduce NCSD, its mission and objectives
- Gain knowledge of ON's cyber security maturity
- Identify areas for cooperation/partnership

ISSUES TO RAISE

- Status of Strategy
- Re-focused mandate of CCIRC, products and services available
- Establishment of a National Cyber Incident Response Framework and the roles of the PTs
- We will be requesting their assistance in gaining knowledge of their incident handling procedures and their information sharing protocols

s.14(a)

BACKGROUND

[redacted]

CONSIDERATIONS

- Peter Macaulay is a former RCMP Superintendent who was the Officer in Charge of the High Tech Crime Unit several years ago (Position now held by Tony Pickett)

s.14(a)

- [redacted]

Prepared by: Kent Schramm
Approved by: Kent Schramm for Adam Hatfield

Feb 6, 2012

Public Safety Canada / Sécurité publique Canada

Senior Assistant Deputy Minister / Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

Seen by the DM
Vu par le SM

For your meeting with: John Forster, CSEC
On: February 14, 2012 at 3:30 p.m. – 4:30 p.m.
Where: 19th floor boardroom, 269 Laurier Ave. W.

SECRET (with attachments)

DATE: Feb 13, 2012

File No.: 385743 / RDIMS No.: 562554

MEMORANDUM FOR THE DEPUTY MINISTER

MEETING WITH JOHN FORSTER, CHIEF, COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

(Information only)

ISSUE

You are scheduled to meet with Mr. John Forster, Chief of the Communications Security Establishment Canada (CSEC), on February 14, 2012.

CONSIDERATIONS

This meeting with Mr. Forster is expected to be a high level, introductory discussion. While the meeting is intended as a courtesy call, it will also provide an opportunity to discuss Public Safety Canada's (PS) and CSEC's roles and responsibilities as they relate to cyber security, It will also be important to note that progress has been made in recent months in the implementation of Canada's Cyber Security Strategy, and that cooperation with CSEC, particularly in the area of information sharing, is improving.

In preparation for your meeting, attached are:

- a briefing note outlining the above noted issues (**TAB A**);
- suggested speaking points (**TAB B**); and
- a briefing note that outlines PS' role in cyber governance (**TAB C**).

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

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosures: (3)

Canada

Feb 13 2012

SECRET // CC

Courtesy Call on February 14, 2012, with Mr. John Forster, Chief, Communications Security Establishment of Canada

Objectives:
1. discuss further implementation of Canada's Cyber Security Strategy by bolstering Public Safety Canada's (PS) relationship with the Communications Security Establishment (CSEC);
2. offer PS' views on cyber security; and
3. [redacted]

BACKGROUND:

- CSEC is Canada's national cryptology agency, providing two main services: foreign signals intelligence in support of defence and foreign policy; and the protection of electronic information and communications. CSEC's advanced technical abilities are also used to aid federal law enforcement and security agencies [redacted]

- On November 16, 2011, CSEC became a standalone agency whose Chief is a deputy head and accounting officer, reporting directly to the Minister of National Defence. Prior to this change, CSEC was considered part of the Department of National Defence (DND) and reported through two separate Deputy Ministers: the National Security Advisor on policy and operational issues, and the Deputy Minister of National Defence on administrative and financial matters.

- Mr. John Forster was appointed Deputy Head and Chief of CSEC effective January 30, 2012. Prior to this appointment, Mr. Forster served as Associate Deputy Minister of Infrastructure from 2009 to 2012, and served at Transport Canada in various capacities from 1998 to 2009. He holds a Bachelor of Science (University of Toronto), a Master's of Business Administration (York University), and has pursued studies in environmental economics at Harvard.

CONSIDERATIONS

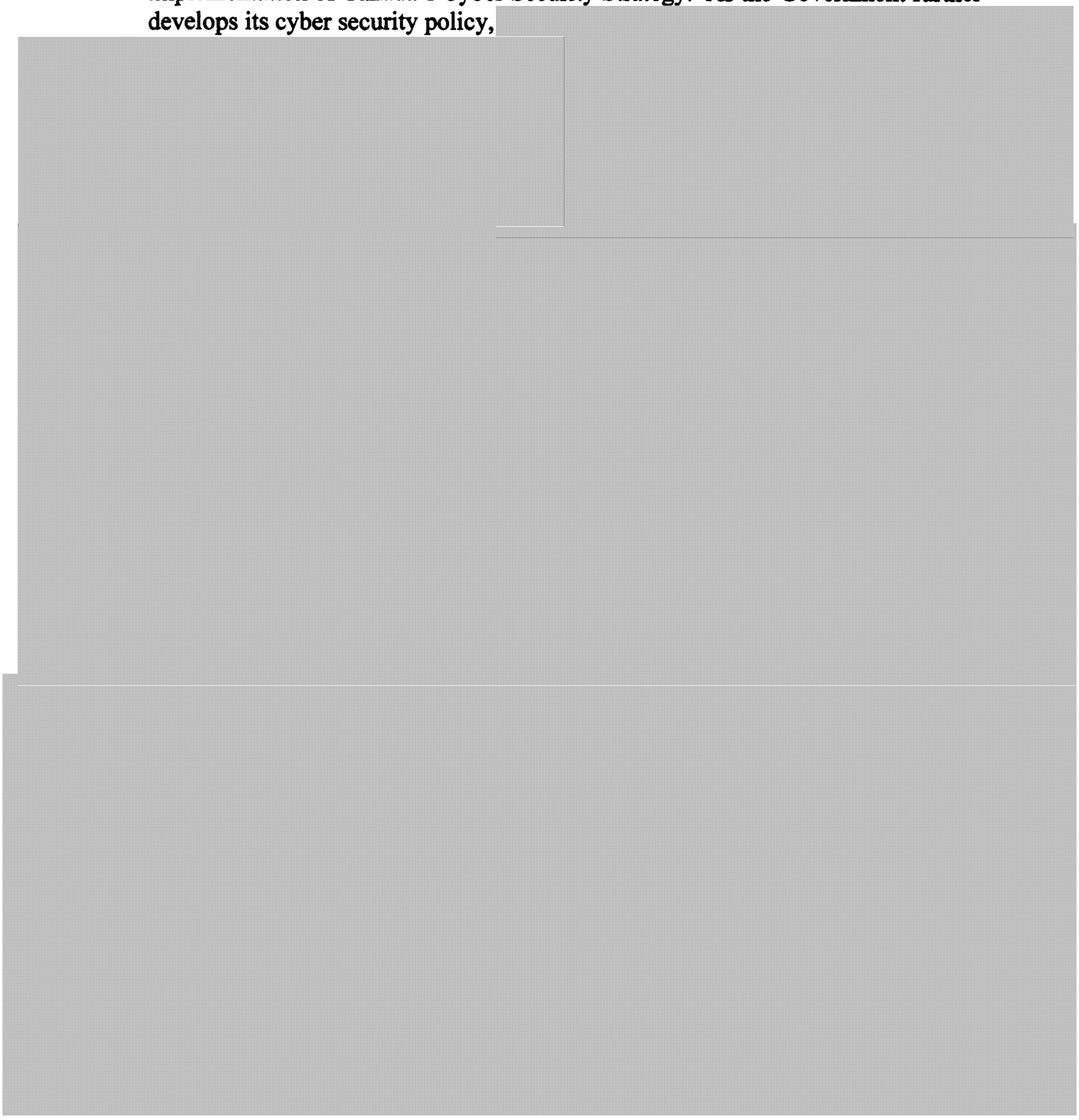
Roles and Responsibilities

- You may wish to touch on cyber security roles and responsibilities with Mr. Forster, emphasizing the important role CSEC played (and continues to play) in the implementation of Canada's Cyber Security Strategy, and offering your views on PS' role within the cyber community, particularly as it relates to the governance function exercised through the Deputy Ministers' Committee on

s.15(1) - Int'l
s.15(1) - Subv
s.16(1)(b)
s.21(1)(a)
s.21(1)(b)

Cyber Security (DM Cyber). This issue is summarized in detail at **TAB C**. You may also wish to offer your thoughts on the DM Cyber process so far, including the inaugural meeting which took place on January 12, 2012, and provide an indication as to where you see that process leading.

- CSEC's intelligence gathering and technical abilities are critical to the implementation of Canada's Cyber Security Strategy. As the Government further develops its cyber security policy,



Feb 13, 2012

UNCLASSIFIED

PUBLIC SAFETY CANADA'S ROLE IN CYBER GOVERNANCE

Objective:

- overview of Public Safety Canada's (PS) role in the governance of cyber security related issues

BACKGROUND

PS is the lead for the Government in the implementation of Canada's Cyber Security Strategy (the Strategy) and has overall responsibility for Government policy and coordination related to cyber security activities.

PS also runs the Canadian Cyber Incident Response Centre (CCIRC), which is Canada's national computer emergency response team, or CERT, which is responsible for coordinating the national response to any cyber security incident and is responsible for monitoring and providing advice on cyber threats for critical networks outside of Government.

[redacted]

Given the size and complexity of the cyber domain, a coherent governance structure is critical to ensuring that policies and activities are well coordinated. The Deputy Ministers' Committee on Cyber Security (DM Cyber) is now the key governance mechanism for the cyber security community. DM Cyber meets quarterly to establish policy direction, set priorities, consider emerging issues and monitor progress on the implementation of the Strategy.

DM Cyber's core members are:

- Director, Canadian Security Intelligence Service;
- Commissioner, Royal Canadian Mounted Police;
- Deputy Minister, National Defence;
- Chief of Defence Staff, Canadian Forces;
- Chief, Communications Security Establishment Canada;
- Deputy Minister, Foreign Affairs;
- Deputy Minister, Industry Canada;
- Deputy Minister and Deputy Attorney General of Canada, Department of Justice Canada;
- National Security Advisor to the Prime Minister, Privy Council Office;
- President, Shared Services Canada; and
- Secretary of the Treasury Board, Treasury Board of Canada Secretariat

The inaugural meeting of DM Cyber was held on January 12, 2012, at which time DMs agreed on the terms of reference and membership for the committee, as well as planned work going forward. DM Cyber will be supported by its sub-committees, the Assistant Deputy Ministers' and Director Generals' Committees on Cyber Security, which will foster collaboration at the working level among Government organizations.

CONSIDERATIONS

Governance and coordination are key challenges that many countries are facing in the implementation of their respective cyber security strategies.

Varied mandates and the evolution of cyber security: The relative newness of the cyber domain has meant that varied national security and law enforcement organizations, in pursuit of their separate mandates, have developed their own cyber security capacity over a number of years prior to coordinated Government strategies being put in place. In addition, the activities and intelligence used by these organizations are often governed by different legal regimes which can make coordination difficult. The challenge for Government lies in bringing together a wide range of players, joining up resources and focusing activities. PS' National Cyber Security Directorate is conducting exercises to help improve coordination between these players. DM Cyber is also paying close attention to this issue.

The scope of potential activities and prioritization: Cyber vulnerabilities have proliferated as both the private sector and Governments have become increasingly networked, often with little regard for the security implications of this interconnectedness. As a result, there is a nearly endless array of potential issues that could be addressed under the rubric of cyber security. A key challenge is to identify and focus attention on priorities within the policy landscape. We have made progress with the Strategy and subsequent action to prioritize, but new pressures emerge constantly in this space.

s.15(1) - Int'l

s.15(1) - Subv

s.21(1)(a)

s.21(1)(b)

The role of Government: The role of Government in protecting cyber systems outside Government continues to be debated. [redacted]

International dimensions: Cyber security issues are transnational, as the actors, intermediaries and targets are often scattered across the globe, requiring cooperation with allies and allied organizations to address cyber threats. [redacted]

Feb 8, 2012

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

Meeting on February 14, 2012, with Mr. John Forster, Deputy Head and Chief, Communications Security Establishment of Canada

ISSUE

- On Tuesday, February 14, 2012, you will be meeting with the Communication Security Establishment's (CSEC) new Chief, John Forster.

- Two unclassified briefing notes are included in this binder as background information: Public Safety's Role in Cyber Governance (**TAB A**); and Public Safety's Memorandum of Understanding (MoU) with CSEC (**TAB B**). A classified briefing is included in **TAB C**.

OBJECTIVES

1. To prepare for further implementation of Canada's Cyber Security Strategy by building Public Safety's relationship with CSEC.
2. To offer Public Safety's views on cyber security.
3. [redacted]

BACKGROUND:

- Mr. Forster was appointed Deputy Head and Chief of the Communications Security Establishment Canada (CSEC) effective January 30, 2012.

- Prior to his appointment, Mr. Forster served as Associate Deputy Minister of Infrastructure from 2009 – 2012. He has served in Transport Canada in various capacities since 1998.

- Mr. Forster's education includes a Bachelor of Science (University of Toronto), a Master's of Business Administration (York University), and studies in environmental economics at Harvard. Mr. Forster does not have previous experience within CSEC.

- Mr. Forster's background indicates that he may bring a fresh perspective to his role at CSEC.

CONSIDERATIONS:

- As Mr. Forster is new to the security community, he might benefit from your views on Public Safety's various roles and responsibilities. Your views on cyber security may be particularly relevant, given the important role played by CSEC in this regard.

s.21(1)(a)

s.21(1)(b)

- Mr. Forster may also benefit from your views on Public Safety's leadership role within the Government of Canada's cyber community, in particular the governance function exercised by the Deputy Minister's Committee on Cyber Security (DM Cyber). This issue is summarized in **TAB A**. You may wish to offer your thoughts on the DM Cyber process so far, including its inaugural meeting which took place on January 12, 2012, and give an indication on where you see that process leading.

[redacted]

TALKING POINTS:

- **Partnership with CSEC**. CSEC provides vital cyber capabilities to the Government of Canada which are essential to implementing Canada's Cyber Security Strategy. The activities and programs CSEC is responsible for directly support the Strategy's first pillar, securing government systems.

- **Information sharing.** In order to manage common cyber challenges across government, operating from a common information base is critical. [redacted] We recognize and respect CSEC's mandate and believe efforts to improve information sharing between our organizations should continue.

- **Public Safety's cyber governance role**. Public Safety plays an important role leading the twelve departments and agencies contributing to cyber security through the National Cyber Security Directorate and DM Cyber.

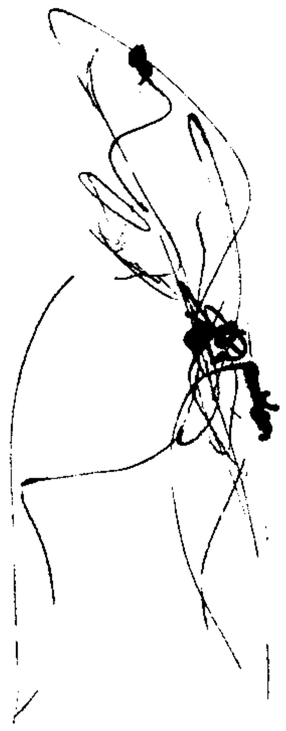
- **DM Cyber**. I am looking forward to your partnership on cyber issues, such as your participation on the DM Cyber.

Responsive only:

[redacted]

Prepared by: Ian Anderson

UNCLASSIFIED



ADM Cyber

February 14, 2012
10:00 to 11:00

17B-2000
269 Laurier Avenue West

Public Safety Canada / Sécurité publique Canada

Ottawa, Canada
K1A 0P8

For your meeting with:
ADM Cyber
On:
February 14, 2012, 10:00 to 11:00

UNCLASSIFIED

DATE: FEB 0 9 2012

COPY

This is the copy I used during the meeting

File No.: 395660
RDIMS No.: Dragon 1255

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

FEBRUARY 14, 2012 MEETING OF THE ASSISTANT DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

(Information only)

ISSUE

You will chair a meeting of the Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber) on February 14, 2012, from 10:00 to 11:00 in boardroom 17B-2000 at 269 Laurier Avenue West.

Ian Anderson, Policy Analyst, National Cyber Security Directorate (NCSD), will be present to take notes.

BACKGROUND

ADM Cyber last met on December 5, 2011, at which you spoke to the creation of the Deputy Ministers Committee on Cyber Security (DM Cyber), which held its inaugural meeting on January 12, 2012.

CURRENT STATUS

There are six items on the February 14, 2012 agenda, including your opening remarks and the closing roundtable.

Item	1. Opening Remarks
Purpose	Information
Your role	Lead
Desired outcome	– Welcome members to the meeting.
Additional documents	– Proposed talking points (TAB 1)

Canada

.../2

Item	2. Debrief of DM Cyber
Purpose	Information
Your role	Lead Bob
Desired outcome	Debrief your colleagues on the outcome of the DM Cyber meeting. – Key points that you could raise include: • Deputies' agreement with the proposed terms of reference for DM Cyber; • Deputies' improved understanding of cyber security roles and responsibilities within Government, including the anticipated role of Shared Services Canada; and • the role of network hygiene and consolidation within Government.
Additional documents	– Proposed talking points and briefing note **(TAB 2)**

Item	3. Debrief on Federal-Provincial-Territorial (FPT) Clerks meeting
Purpose	Information
Your role	Introduce Rennie Marcoux, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office, as the lead.
Desired outcome	– Debrief ADM Cyber members on the outcome of the FPT Clerks meeting, which took place on January 23, 2012. [redacted]
Additional documents	– Proposed talking points and briefing note **(TAB 3)**

Item	4. Cyber Security Forward Agenda
Purpose	Discussion
Your role	Lead
Desired outcome	– Set the future direction for DM Cyber. – At the DM Cyber meeting, Deputies mentioned several items that could be considered at future meetings, including: [redacted]
Additional documents	– Proposed talking points and briefing note **(TAB 4)** • Draft forward agenda **(annex to TAB 4)**

Role of Govt.

.../3

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

Item	
Purpose	
Your role	
Desired outcome	
Additional documents	– Proposed talking points and briefing note (TAB 5) – annex to TAB 5)

Item	6. Roundtable
Purpose	Information
Your role	Lead
Desired outcome	–
Additional documents	– N/A

CONCLUSION

Should you require additional information, please do not hesitate to contact me or Mark Matz, Director, Policy and Issues Management, NCSD, at 613-993-9635.

Robert Dick
Director General
National Cyber Security

Enclosure: (1)

Prepared by: Melanie Mohammed

Sécurité publique Canada | Public Safety Canada

UNCLASSIFIED

Assistant Deputy Ministers Committee on Cyber Security

February 14, 2012 – 10:00 to 11:00
17B-2000, 269 Laurier Avenue West

AGENDA

	Time	Item	Associated Documentation
1.	10:00 *5 min*	**Opening Remarks** Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada	N/A
2.	10:05 *10 min*	**Debrief on the Deputy Ministers Committee on Cyber Security** Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada *For information: Debrief on the inaugural Deputy Ministers Committee on Cyber Security, which took place on January 12, 2012.*	N/A
3.	10:15 *10 min*	**Debrief on FPT Clerks Meeting** Rennie Marcoux, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office *For information: Debrief on the FPT Clerks meeting that took place on January 23, 2012.*	N/A
4.	10:25 *10 min*	**Cyber Security Forward Agenda** Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada *For discussion: Seek input on the DM Cyber forward agenda.*	Forward agenda
5.	10:35 *15 min*	[redacted]	
6.	10:50 *10 min*	**Roundtable**	N/A

s.15(1) - Int'l

s.15(1) - Subv

Sécurité publique Canada | Public Safety Canada

NON CLASSIFIÉ

Comité des sous-ministres adjoints sur la cybersécurité

Le 14 février 2012 – 10h00 à 11h00
17B-2000 au 269, avenue Laurier ouest

ORDRE DU JOUR

	Heure	Item	Documentation connexe
1.	10h00 *5 min*	**Mot de bienvenue** Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, Sécurité publique Canada	S/O
2.	10h05 *10 min*	**Compte rendu sur la réunion des sous-ministres sur la cybersécurité** Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, Sécurité publique Canada *Pour information : Faire un compte rendu sur la première réunion du comité des sous-ministres sur la cybersécurité, ce qui a eu lieu le 12 janvier 2012.*	S/O
3.	10h15 *10 min*	**Compte rendu sur la réunion des greffiers FPT** Rennie Marcoux, secrétaire adjointe du Cabinet, sécurité et renseignement, bureau du Conseil privé *Pour information : Faire un compte rendu sur la réunion des greffiers FPT, ce qui a eu lieu le 23 janvier 2012.*	S/O
4.	10h25 *10 min*	**Programme d'activités à long terme sur la cybersécurité** Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, Sécurité publique Canada *Pour discussion : Chercher des contributions au programme proposé d'activités à long terme pour le comité des SM sur la cybersécurité.*	Programme d'activités à long terme
5.	10h35 *15 min*	[redacted]	
6.	10h50 *10 min*	**Tour de table**	S/O

s.15(1) - Int'l

s.15(1) - Subv

s.15(1) - Subv

Public Safety Canada / Sécurité publique Canada

MEETING PARTICIPANTS - PS

PARTICIPANTS À LA RÉUNION - SP

DATE :	CONTACT PERSON - PERSONNE RESSOURCE :
➲ February 14, 2012	➲ CARMEN VOGHEL OR RUBA PIASKO
TIME - HEURE :	TELEPHONE No - N° DE TÉLÉPHONE :
➲ 10:00	➲ 991-7025 OR 991-2901
ROOM - SALLE :	DIVISION & SECTION :
➲ 17th floor, 17B2000	➲ NS

PASS NUMBER / NUMÉRO DU LAISSEZ-PASSER	NAMES OF GUESTS / LISTE DE NOMS DES INVITÉS	DEPARTMENT/COMPANY / MINISTÈRE/ENTREPRISE
✓	[redacted]	CSE
✓		CSIS
✓	KEITH CHRISTIE for K. BUCK	DFAIT
	STEVE NOONAN for J. TURNER	DND
TENTATIVE	JILL SINCLAIR	DND
Rod Ansem	ANTHONY ASHLEY for M. FORTIN	DRDC
✓	GUY MITCHELL for H. McDONALD	IC
✓	MARK SCRIVENS for D. THERRIEN	JUSTICE
~~bof~~ ✓?	DONALD PIRAGOFF	JUSTICE
✓	RENNIE MARCOUX	PCO
	NO REP AVAILABLE	RCMP
	BENOIT LONG	SSC
	BARBARA GLOVER	PWGSC
	JOHN OSSOWSKI SCOTT MILLAR	TBS
	PIERRE BOUCHER	TBS
	BOB GORDON	PS
	ROBERT DICK	PS
TBC	STEPHANIE DURAND	PS

Rod Ansem

1. OPENING REMARKS

- Bonjour tout le monde, et bienvenue à la réunion.
  - *Good afternoon everyone, and welcome to the meeting.*

- For the first item on today's agenda, I will be debriefing you on the outcome of the January 12, 2012 inaugural DM Cyber meeting.

- Next, Rennie (Marcoux) will debrief us on the outcome of the FPT Clerks meeting that took place a couple weeks ago on January 23, 2012.

- At the DM Cyber meeting, Deputies mentioned several items that could be considered at future meetings. I will share those items with you, and would invite each of you to identify future topics that you feel could be raised at future DM Cyber meetings.

s.15(1) - Int'l

s.15(1) - Subv

TAB 1

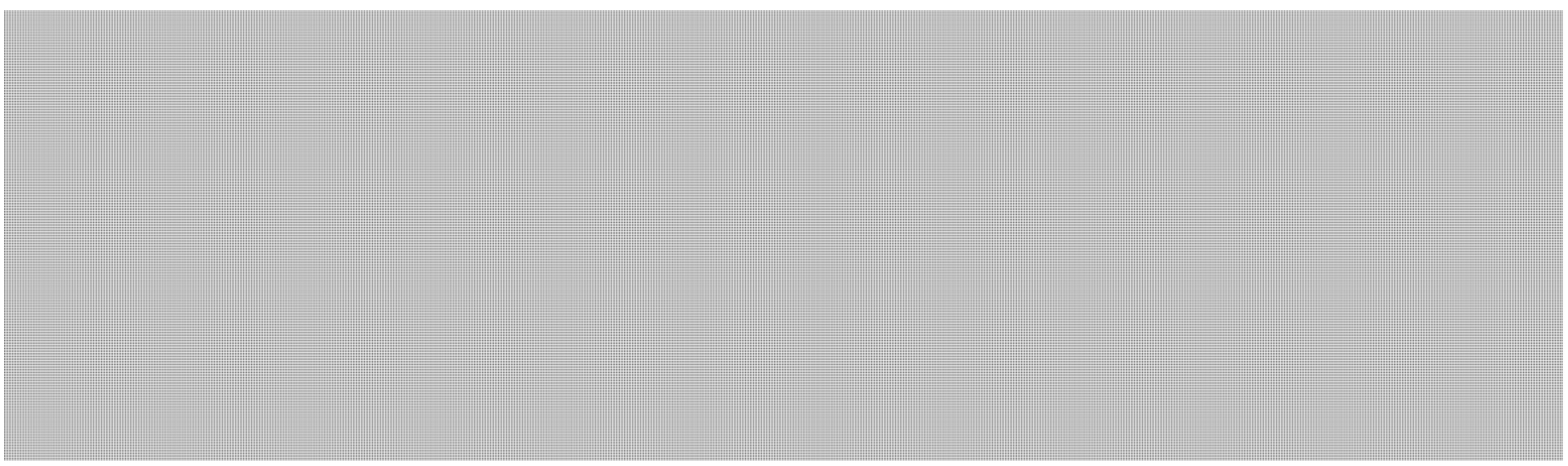
TAB 2

2. DEBRIEF ON THE DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

PROPOSED TALKING POINTS

- At the inaugural DM Cyber meeting, the Deputy Minister of Public Safety explained that DM Cyber was created to serve as a forum to explore emerging policy issues in the realm of cyber security. Deputies agreed to the proposed terms of reference and membership for the Committee.
    - Deputies were open to having other Deputy Heads join meetings when necessary.

- TBS's presentation on network hygiene was well-received by Deputies.



    - Those at the table were in agreement that the Management Accountability Framework may be the most appropriate and effective manner by which to deliver the message that network consolidation and hygiene are essential to cyber security. It was also mentioned that it may be useful to brief other Deputy Heads on the threat environment to provide them with a better understanding of the necessity of proper network hygiene.

s.15(1) - Int'l

s.15(1) - Subv

- Deputies also placed emphasis on branding SSC as an economic benefit, as well as an important component to ensuring security.

- Deputies appreciated the high-level overview of roles and responsibilities, and asked about work underway regarding information sharing within and outside Government. The National Cyber Security Directorate is currently working with Defence Research and Development Canada to analyze the results of the recent information sharing questionnaire that was sent to certain departments and agencies. This analysis will help us respond to Deputies' concern.

ISSUE

You will debrief members on the outcome of the Deputy Ministers Committee on Cyber Security (DM Cyber), which took place on January 12, 2012.

No documents are required for this item.

BACKGROUND

Terms of Reference and Membership

At the inaugural DM Cyber meeting, it was explained that the Committee was created to provide a forum to explore emerging cyber policy issues. Deputies were in agreement that such a fora was required, especially given the high priority allocated to cyber security by the current government, and the pace at which the threat environment is evolving. It was agreed that the proposed terms of reference and membership for the Committee were suitable, and that the Committee would be supported by the Assistant Deputy Ministers Committee on Cyber Security, which would be supported by the Directors General Committee on Cyber Security. Deputies agreed that non-member Deputy Heads could also be invited to attend meetings when necessary.

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

Network Hygiene

[redacted]

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

[redacted]

TBS and SSC stressed the fact that consolidation would go a long way to helping secure Government networks. Deputies were in agreement that the Management Accountability Framework may be the most appropriate and effective manner by which to deliver the message that network consolidation and hygiene are essential to cyber security. It was also mentioned that it may be useful to brief other Deputy Heads on the threat environment to provide them with a better understanding of the necessity of proper network hygiene.

Roles and responsibilities

Deputies appreciated the high-level overview of roles and responsibilities, and asked about work underway regarding information sharing within and outside Government. The National Cyber Security Directorate is currently working with Defence Research and Development Canada to analyze the results of the recent information sharing questionnaire that was sent to certain departments and agencies. This analysis will help to respond to Deputies' concern.

Prepared by: Melanie Mohammed
Approved by: Mark Matz

TAB 3

Pages 843 to / à 844

are withheld pursuant to section

sont retenues en vertu de l'article

14(a)

of the Access to Information

de la Loi sur l'accès à l'information

TAB 4

4. CYBER SECURITY FORWARD AGENDA

[redacted]

ISSUE

You will lead a discussion on the forward agenda for the Deputy Ministers Committee on Cyber Security (DM Cyber).

A draft forward agenda was distributed to participants at the beginning of the meeting, and is enclosed for your ease of reference.

BACKGROUND

At the inaugural DM Cyber meeting, Deputies mentioned several items that could be considered at future meetings, including:

[redacted]

While input to the DM Cyber forward agenda was requested at the Assistant Deputy Minister and Director General levels before the 2011-12 holiday break, responses were only received from the Department of National Defence / Canadian Forces, the Department of Foreign Affairs and International Trade, and the National Cyber Security Directorate. Industry Canada indicated that they would be better placed to provide input in the second to fourth quarters of 2012-13.

CONSIDERATIONS

Additional input is required on the DM Cyber forward agenda in order to ensure that Deputy Heads are focusing on current priorities and gaining a clear perspective of cyber security issues.

Prepared by: Melanie Mohammed
Approved by: Mark Matz

s.15(1) - Int'l

s.15(1) - Subv

UNCLASSIFIED

s.21(1)(a)

CYBER SECURITY FORWARD AGENDA

[redacted] RADAR

FOR INFORMATION

CYBER SECURITY ROLES AND RESPONSIBILITIES
Issue: Clarify and streamline roles and responsibilities of cyber security lead departments.
Description: TBC
Lead: PS
Required documents: TBC

[redacted]

FOR DECISION

FOR DISCUSSION

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

Date, time and location	Proposed items
DG Cyber February 8, 2012 9:30 to 10:30 Teleconference	**FOR INFORMATION** **DEBRIEF ON DM CYBER** **Issue**: Debrief on inaugural DM Cyber meeting. **Description**: The inaugural DM Cyber meeting was held on January 12, 2012. Deputies agreed on the terms of reference and membership for the Committee, which will be supported by ADM and DG Cyber. They also discussed the challenge in protecting Government systems, work undertaken to date, and planned work going forward. **Lead**: PS **Required documents**: N/A **DEBRIEF ON FPT CLERKS MEETING** **Issue**: Debrief on the FPT Clerks meeting that took place on January 23, 2012. **Description**: TBC **Lead**: PCO **Required documents**: N/A **FOR DECISION** **FOR DISCUSSION** [redacted] **CYBER SECURITY FORWARD AGENDA** **Issue**: Seek input on the cyber security forward agenda. **Description**: Deputy Ministers discussed the concept of a cyber security forward agenda at their inaugural meeting. Input received has been limited, but will be required going forward to ensure that the forward agenda reflects current priorities. **Lead**: PS **Required documents**: Forward agenda
ADM Cyber February 14, 2012 (TBC) 10:00 to 11:00 17B-2000 269 Laurier Ave. W.	**FOR INFORMATION** **DEBRIEF ON DM CYBER** **Issue**: Debrief on inaugural DM Cyber meeting. **Description**: The inaugural DM Cyber meeting was held on January 12, 2012. Deputies agreed on the terms of reference and membership for the Committee, which will be supported by ADM and DG Cyber. They also discussed the challenge in protecting Government systems, work undertaken to date, and planned work going forward. **Lead**: PS **Required documents**: N/A **DEBRIEF ON FPT CLERKS MEETING** **Issue**: Debrief on the FPT Clerks meeting that took place on January 23, 2012.

Date, time and location	Proposed items
	Description: TBC **Lead**: PCO **Required documents**: N/A **FOR DECISION** **FOR DISCUSSION** [redacted] **CYBER SECURITY FORWARD AGENDA** **Issue**: Seek input on the cyber security forward agenda. **Description**: Deputy Ministers discussed the concept of a cyber security forward agenda at their inaugural meeting. Input received has been limited, but will be required going forward to ensure that the forward agenda reflects current priorities. **Lead**: PS **Required documents**: Forward agenda
DG Cyber Date TBC Time TBC Location TBC	**FOR INFORMATION** **TREND MICRO BRIEFING** **Issue**: Provide a briefing regarding a recent meeting with Trend Micro and provide an overview of the current situation. **Description**: TBC **Lead**: PS – Hatfield **Required documents**: TBC **ENGAGING KEY VENDORS (THIS ITEM MUST BE PRESENTED AT THE SAME MEETING AS THE "MICROSOFT SECURITY COOPERATION PROGRAM" ITEM)** **Issue**: TBC. **Description**: TBC **Lead**: PS – Labelle **Required documents**: TBC [redacted] **FOR DECISION** **CYBER SECURITY WORKING GROUPS** **Issue**: Consolidate working groups and, where possible, dissolve those that are no longer required.

Date, time and location	Proposed items
	Description: At the November 30, 2011 DG Cyber meeting, and at the December 5, 2011 ADM Cyber meeting, it was agreed that too many cyber security working groups currently exist within the community. It was decided that DG Cyber members should look to consolidate working groups, and, where possible, dissolve those that are no longer required with a view to freeing up resources (people and time) to focus on new and emerging issues. **Lead**: PS **Required documents**: Inventory of cyber security working groups **MICROSOFT SECURITY COOPERATION PROGRAM (THIS ITEM MUST BE PRESENTED AT THE SAME MEETING AS THE "ENGAGING KEY VENDORS" ITEM)** **Issue**: Seek decision on whether Government's agreement with Microsoft's Security Cooperation Program is relevant and meeting our needs. **Description**: Government is a signatory to Microsoft's Security Cooperation Program. Given changes in departmental roles and responsibilities, it is timely to revisit this agreement and ensure it is meeting Government needs and all relevant players are engaged. **Lead**: PS – Hatfield **Required documents**: TBC **FOR DISCUSSION** **DEBRIEF ON TABLETOP EXERCISE "FROZEN POND"** **Issue**: Provide a debrief on results and suggested next steps. **Description**: As directed by ADMs and DGs, a tabletop exercise to clarify roles and responsibilities of Government departments and agencies in supporting a whole-of-government response to a national cyber incident has been completed. **Lead**: PS – Hatfield **Partner departments**: All DG Cyber members **Required documents**: TBC
ADM Cyber Date TBC Time TBC Location TBC	**FOR INFORMATION** **FOR DECISION** **FOR DISCUSSION**
DG Cyber Date TBC Time TBC Location TBC	**FOR INFORMATION** [redacted] **FOR DECISION**

s.14(a)

Page 852

is under consultation

est sous consultation

s.15(1) - Int'l

s.15(1) - Subv

UNCLASSIFIED

Date, time and location	Proposed items
Time TBC Location TBC	
DM Cyber April 19, 2012 (TBC) TBC 19th floor boardroom 269 Laurier Ave. West	**FOR INFORMATION** [redacted] **FOR DECISION** **FOR DISCUSSION**

ARCHIVE

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

FOR INFORMATION

NETWORK HYGIENE
Issue: Provide an aperçu of the challenge in protecting Government IT systems, the actions taken to date, and forward work.
Description: N/A
Lead: TBS
Required documents: Deck: Cyber Security – The Challenge in Protecting Government Systems

CYBER SECURITY ROLES AND RESPONSIBILITIES
Issue: Provide an overview of the roles and responsibilities of cyber security lead departments.
Description: N/A
Lead: PS
Required documents: Roles and responsibilities map

Inaugural DM Cyber

January 12, 2012
14:00 to 15:00

19th floor boardroom
269 Laurier Ave. West

[redacted]

FOR DECISION

DM CYBER
Issue: Agree upon the proposed role and scope of the Committee, and discuss Committee forward agenda.
Description: N/A
Lead: PS
Required documents: Draft terms of reference, and draft forward agenda

FOR DISCUSSION

FPT CLERKS MEETING, JANUARY 23, 2012
Issue: Seek views on the strategic objectives for the meeting.
Description: N/A
Lead: PS
Required documents: TBC

TAB 5

Pages 856 to / à 862

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

TAB 6

6. ROUNDTABLE

During the roundtable, it is not expected that you will have any items to add.

Page 865

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 15(1) - Subv, 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

TAB A-1

THE BUDAPEST CONVENTION AND OTHER CYBER CRIME EFFORTS

[redacted]

ISSUE

[redacted]

BACKGROUND

The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the only widely-recognised attempt to deal with cybercrime issues and contains the most accepted typology for cybercrime. The treaty describes which actions are prohibited in cyberspace, the extent of personal and corporate liability, and search and seizure of computer data. It also provides specific mechanisms to facilitate law enforcement cooperation in cyberspace through a 24/7 assistance network. Only 31 countries are parties to the Convention.

Canada signed the *Convention* in 2001 but has not yet adopted certain provisions in national legislation to permit ratification. The Government has committed to introducing these provisions in the current Parliament.

While the *Convention* is trumpeted as the gold standard to combat cybercrime among Western countries, a number of states have been reluctant to join largely on the grounds that some of its core elements, such as the 24/7 information sharing network, violate national sovereignty. It is also on sovereignty grounds that certain countries reject provisions in the Convention that allows Parties to access stored computer data with consent of the data's host or where it is publicly available.

Some countries also view it as politically unacceptable to accede to a largely European-centric treaty, having been negotiated between members and observers of the Council of Europe. These countries, largely in the developing world, believe that a global cybercrime instrument, negotiated through a United Nations process, would be more representative of a global consensus. [redacted]

CONSIDERATIONS

Given the unease with the Budapest Convention in some countries [redacted]

[redacted]

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

[redacted]

U.N. Study on Cybercrime

A U.N. study group, of which a Justice Canada official is the Rapporteur, is examining the issue of cybercrime and the viability of a global treaty. The U.N. report is not expected until 2013, at the earliest. A questionnaire that will be distributed to countries in the Spring is currently being translated. [redacted]

Accelerating the process would potentially not give countries enough time to comprehensively answer the questionnaire. [redacted]

[redacted]

Public Safety Canada / Sécurité publique Canada

SECRET REL

TAB A-2

ISSUE

The Internet has been built on an open, and multistakeholder model of governance, embodied in the International Corporation for Assigned Names and Numbers (ICANN).

ARGUMENTS FOR THE STATUS QUO

Pages 869 to / à 870

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

SECRET REL [redacted]

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

TAB A-3

[redacted]

ISSUE

[redacted]. In 2008, the ITU Secretary General signed a Memorandum of Understanding with IMPACT and he sees the organization as the ITU's "operational arm." Over 130 countries are members of the organization, including India and Brazil. None of the countries with advanced cyber capabilities, such as Australia, China, France, Russia, Sweden, the United Kingdom, and the United States have joined the group.

[redacted]

BACKGROUND

[redacted]

CONSIDERATIONS

[redacted]

[redacted]

Pages 872 to / à 873

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Pages 874 to / à 879

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Subv, 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 880 to / à 882

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

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

TAB C-2

WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS

Upcoming WCIT-preparatory events:
27-29 February in Geneva (Attending will be four Industry Canada reps and Paul Charlton)
23-25 April in Geneva
Second week of May in Buenos Aires (ITU-sponsored regional meeting for the WCIT)
20-22 June in Geneva

Page 884

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 15(1) - Subv, 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 885 to / à 886

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Page 887

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 15(1) - Subv, 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 888 to / à 894

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

F.L. 22.2012

UNCLASSIFIED

DATE:

File No.: 385988
RDIMS No.: 557418

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

ACADEMIC ENGAGEMENT PLAN FOR CYBER SECURITY

(For information)

ISSUE

To outline the proposed Academic Engagement Strategy on cyber security.

BACKGROUND

Canada's Cyber Security Strategy (the Strategy) signaled the Government's commitment to working with the academic community and other partners to help protect Canada's digital infrastructure. The academic community offers unique technological and analytical expertise, and their collaboration is essential to our shared success in securing Canada's digital infrastructure.

Research in cyber security tends to reflect the interconnected and multifaceted nature of the field, and covers a range of subject areas including computer science, information security, criminology, privacy, law and international relations. Given the multidisciplinary nature of cyber security, academics are currently not particularly cohesive or united in their approach to research.

Over the **long term**, the objectives of academic engagement are to:

- increase Canadian cyber security expertise;
- promote the creation of a trusted and knowledgeable community of academics to provide Government with advice and support on policy and legislative proposals; and
- facilitate the establishment of productive partnerships between academics, the private sector, and critical infrastructure sectors.

.../2

To reach these objectives, a key **short term** priority will be to develop a much more comprehensive diagnostique of the existing academic activity on cyber security in Canada. The National Cyber Security Directorate (NCSD) has taken some important initial steps to better understand the research landscape, and to bring together academics working across a range of fields and specializations. Last fall, NCSD commissioned seven research projects from a variety of faculties across Canada. See the complete list (**TAB A**).

These papers have now been completed and will provide a base for future policy relevant research. The papers will also help to generate a richer discourse on emerging cyber security policy issues and tensions, and to encourage the creation of a more comprehensive body of knowledge. To build on that momentum, NCSD, in collaboration with the Critical Infrastructure and Strategic Coordination Directorate, are planning to hold a 2-day workshop in June, 2012. The purpose of the workshop will be to promote the development of a cohesive community of academics in order to facilitate a constructive policy dialogue while looking at areas of common interest, such as industrial control systems. The scale of the workshop is proposed to be deliberately small in order to maximize the benefits of the policy discussion.

In the short term, NCSD has been reaching out to some of the established leaders in the field:

- In February, NCSD visited with the University of Toronto's Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, and identified some areas of mutual interest. As a result, NCSD will be participating in the Munk School's Cyber Dialogue scheduled for March, 2012.

- NCSD has engaged the National Cyber Forensic Training Alliance (NCFTA) based at Concordia University. The NCFTA brings a great deal of technical and analytical expertise and has established productive partnerships with the private sector, particularly telecommunications providers and information technology companies. NCFTA also has very productive relationships with law enforcement agencies in Quebec. We are currently working with the Royal Canadian Mounted Police (RCMP), the Canadian Radio-television Telecommunications Commission (CRTC) and Defence and Research Development Canada (DRDC) to explore partnership opportunities.

- NCSD will strategically identify and attend key events that allow academics, the private sector and critical infrastructure sectors to engage on cyber security research. The calendar of cyber events is kept up-to-date and shared with key partners to allow us to complement efforts and avoid duplication.

In the **medium term**, NCSD will be looking to develop an inventory of the existing research activity on cyber security. Over the next two to three years, we will work with the federal research agencies such as the Natural Science and Engineering Research

.../3

Council (NSERC), the Social Science and Humanities Research Council (SSHRC), the National Research Council (NRC) and DRDC to take stock of existing research, identify gaps and collaborate to develop a national research agenda on cyber security.

We will also explore the opportunities to leverage some of the existing research in the United States (US). Stephen Flynn will be invited to the June workshop and we will explore other opportunities to benefit from US academic engagement expertise.

CURRENT STATUS

NCSD and CIPD are collaborating in the organisation of the June workshop, and will explore future events, based on the outcome of the June workshop.

Engagement with other Government partners is proceeding, and we are looking into the requirement for an interdepartmental governance instrument, for example a working group under DG Cyber.

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Mr. Sébastien Labelle, Director, Engagements and Partnerships, at 613-990-2655.

Robert Dick
Director General
National Cyber Security Directorate

Prepared by: Sébastien Labelle

Research Projects Comissioned by NCSD

"Economic Impact of Cyber Threats and Attacks"
Dr. Sara M. Smyth, Assistant Professor, School of Criminology at Simon Fraser University

"Examination of the current normative discourse on the balance between privacy and security in cyberspace"
Laura Huey, Department of Sociology, University of Western Ontario

"The legal and policy framework anchoring the Canadian approach to securing cyberspace"
Dr. Avner Levin, Director, Privacy and Cyber Crime Institute, Ryerson University

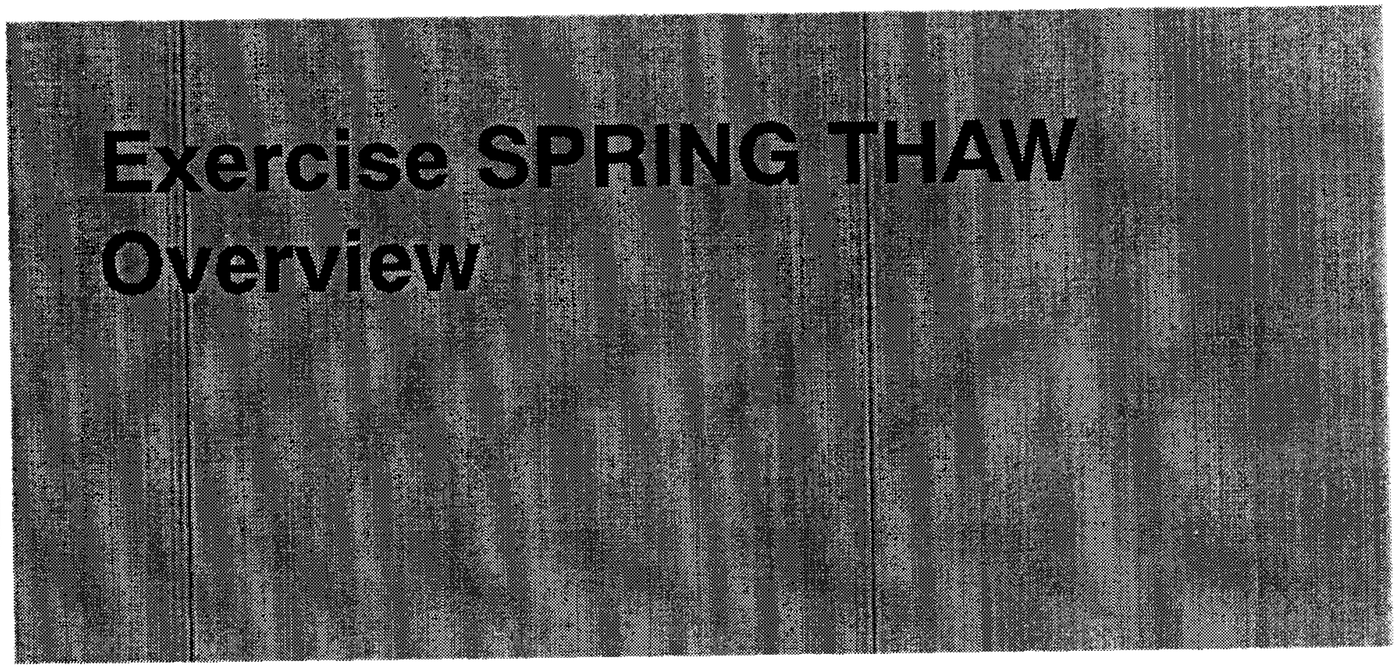
"Key socioeconomic trends in the next decade and implications for cyber security policy"
Rafal Rohozinski, The Citizen's Lab, Munk Centre, University of Toronto

"Crime, Culture and Technology in the next decade and implications for cyber security policy"
Benoit Dupont, Directeur du Centre international de criminologie comparée, Université de Montréal

"Key ethical and legal trends in the next decade and implications for cyber security policy"
David Fewer, Director, Canadian Internet Policy and Public Interest Clinic, Faculty of Common Law, University of Ottawa

"Ethical Hacking: An Analysis"
Dr. Alana Maurushat, Academic Director, Cyberspace Law and Policy Centre Lecturer, Faculty of Law, The University of New South Wales

Public Safety Canada | Sécurité publique Canada



Exercise SPRING THAW
Overview

DATE TBD
RDIMS # 572593

Canada

Concept of Operations

- Half day exercise
- Two scenarios plus immediate after action report/ discussion
- Scenario #1
  - Attack against a province
  - Criminal actors
- Scenario #2
  - Attack against CI with request for assistance from Premier of province
  - State sponsored

Exercise Participants

- PS – CCIRC
- RCMP – High Tech Crime
- CSIS – Information Operations
- CSEC – GC CTEC

Objectives

- Define what constitutes a significant cyber event that would require Government of Canada intervention/coordination
  - Identify trigger criteria/thresholds
- An entity (PT, CI, industry) has requested GC assistance:
  - Who should entertain this request?
  - Who should be the "spokesperson" or "lead" for the GC?
  - Identify what assistance the GC could provide
    - Legal mandate or duty of care?
  - Identify what information the GC could provide
  - Do we have criteria to share information?
  - Does the status of the entity matter?
    - i.e. Provincial government, CI, small or large industry

Objectives

- What about an academic institution, small business?
  - What are the criteria?
- Does the importance of the network at risk matter?
  - How do we define a system of importance to the GC?
  - Who is responsible for making this call?
  - Who would be the lead for the GC?
- A foreign state has been identified as being responsible for an attack against a PT or CI network
  - How does the GC respond to this?
  - Who is lead?
  - How would we provide response options?
    - Political, economic, military or other?
    - Policy issues (existing or lacking)

Objectives

- What is the criteria to brief up?
  - Again what are the thresholds?
- What is the escalation approach?
- What information should be provided?
- Who is lead?
- How does an equity decision unfold? (RCMP, CSIS and CSEC)

Ex SPRING THAW Concept of Operations

- A significant cyber event has occurred and a Director level meeting was held with the decision that DGs should meet
- A consolidated brief would be provided to each DG
  - Need to confirm with each Director what it would entail
- Scenario #1 plays out (45-60 minutes)
- Scenario #2 plays out (45-60 minutes)
- Post exercise (60 minutes)
  - Discussion
  - Identification of lessons learned
  - Action items
  - Next steps

Public Safety Canada | Sécurité publique Canada

SAFE RESILIENT CANADA

A New Vision for the Canadian Cyber Incident Response Centre - Presentation to ADM

RDIMS: 415224

Canada

Challenge/Consequences

- Canada must have a national cyber presence

- Challenge: CCIRC is over mandated and under resourced

- Consequences
  - Poor credibility with some stakeholders
  - Capacity and capability to deliver on core CERT functions is limited
  - Role ambiguity confuses operations and negatively impacts your effectiveness and outcomes

Strategy

- Fix CCIRC in its current role
  - Clarify roles, mandate and mission space
  - Focus on operations; leverage NCSD
  - Quick hits for improving credibility
  - Communications plan

- Define multi-year roadmap

Clarify Role

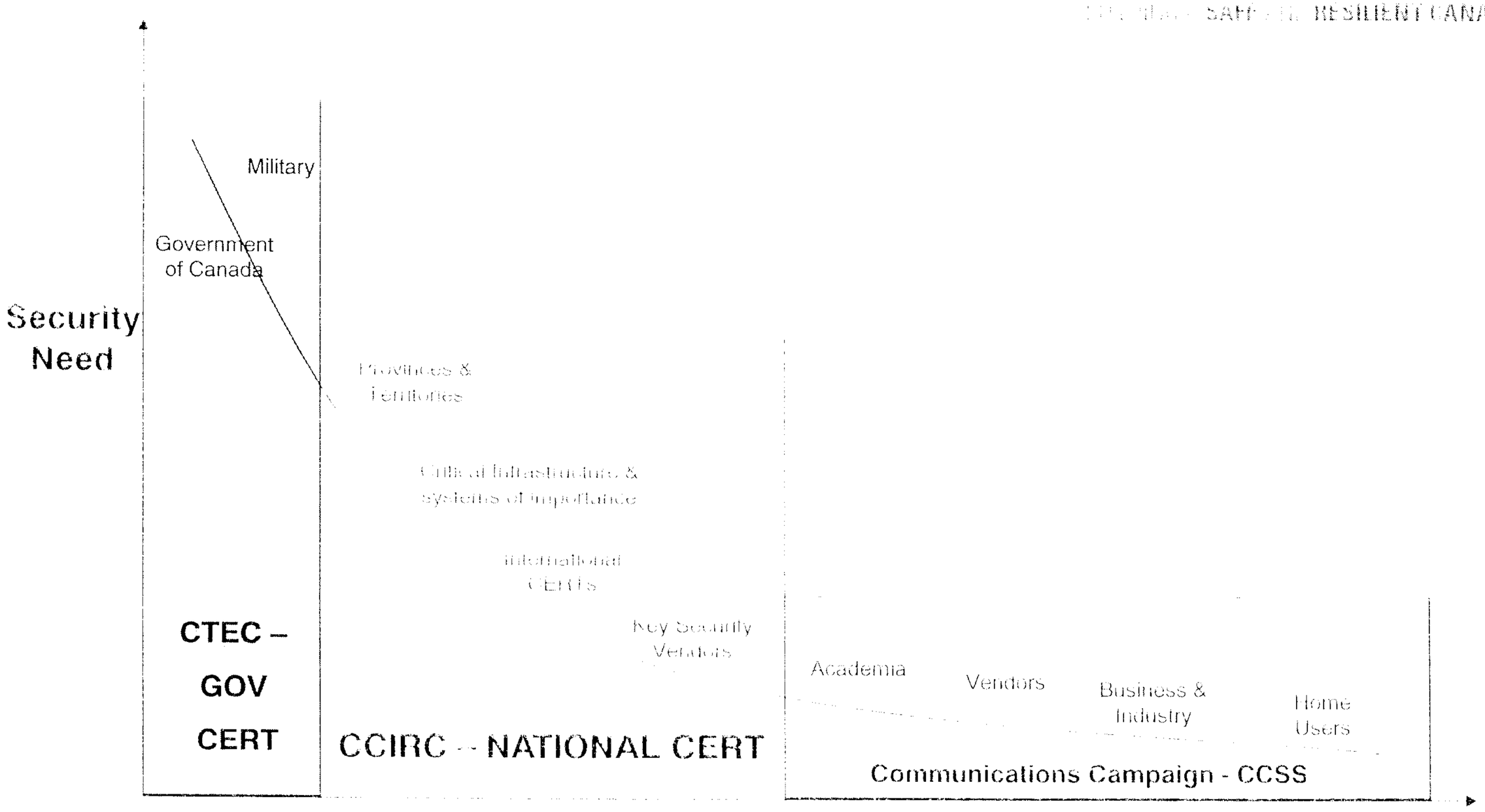
- Cyber Threat Evaluation Centre – Government CERT
- CCIRC – National CERT

- Revised GC IT Incident Management Plan
  - Limited coordination role as per the FERP
- Formalize CCIRC mandate in public-friendly format
- Provide strategic cyber situational awareness by bringing together government and non-government information

Mandate and Mission Space

Core CERT Function	Proposed CCIRC Role
Safe Point of Contact	Viable with comms strategy
Coordination of Nat'l Response	Opportunity for leadership
Provision of information	Value added and aggregation
Mitigation operations	Needs to be fully resourced
Tailored technical support	Beyond current resources
Capacity Building	N/A; best efforts by NCSD

Client Base



Focus on Operations

- Operational impediments that need to be resolved
  - Production of Situational Awareness products
  - Strictly defined client base
  - Protocol for incident prioritization
  - Regular reporting of incident statistics
  - Technical infrastructure
- Leverage NCSD for engagement and strategic initiatives

Quick Hits

- Re-branding of products
  - Weekly technical report
  - Weekly strategic report
  - Existing flashes and alerts to be more clearly prioritized per client feedback
- More structured engagement with PTs, CEA, CBA via NCSD
- Staffing
  - 3 x CS for tech expertise
  - 3 x EC positions for SA

Communications Plan

- Engage Comms branch
- Re-brand CCIRC as a national CERT with a focussed outreach and communications strategy
- Re-branding of existing products
- New web presence

Define Multi-Year Roadmap

- Pressures
  - National IT incident management framework
  - CAN/US Borders Accord
  - Cyber Storm IV – May 2012
  - Staffing, training, retention
- [redacted]

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

Public Safety Canada | Sécurité publique Canada

Exercise SPRING THAW

Proposal For Discussion

DATE TBD

RDIMS # 575067

Canada

Overview

- Half day exercise (3 hours)
- Two scenarios plus immediate after action report/discussion

- PS – CCIRC
- RCMP – High Tech Crime
- CSIS – Information Operations Centre
- CSEC – GC CTEC

Objectives

- Explore what constitutes a significant cyber event that would require Government of Canada (GC) intervention/coordination
  - Identify trigger criteria/thresholds
- Explore GC role in responding to a request for assistance
  - Who should entertain this request?
  - Who should be the "spokesperson" or "lead" for the GC?
  - Identify what assistance the GC could provide
    - Incident coordination, public affairs, mitigation advice, forensics, cyber defence, prosecution, other?
  - Legal mandate or duty of care?
  - Identify what information the GC could provide
    - Do we have criteria to share information?
  - Does the status of the entity matter?
    - i.e. Provincial government, CI, small or large industry

Additional Questions For Discussion

- What about an academic institution, small business?
  - What are the criteria?
- Should all requests go through PT EMOs, CIOs?
- Does the importance of the network at risk matter?
  - How do we define a system of importance to the GC?
  - Who is responsible for making this call?
  - Who would be the lead for the GC?
- A foreign state has been identified as being responsible for an attack against a PT or CI network
  - How does the GC respond to this?
  - Who is lead?
  - How would we provide response options?
    - Political, economic, military or other?
    - Policy issues (existing or lacking)

Additional Questions for Discussion (Cont'd)

- What are the criteria to brief up?
  - Again what are the thresholds?
- What is the escalation approach?
- What information should be provided?
- Who is lead?
- How does an equity decision unfold? (RCMP, CSIS and CSEC)

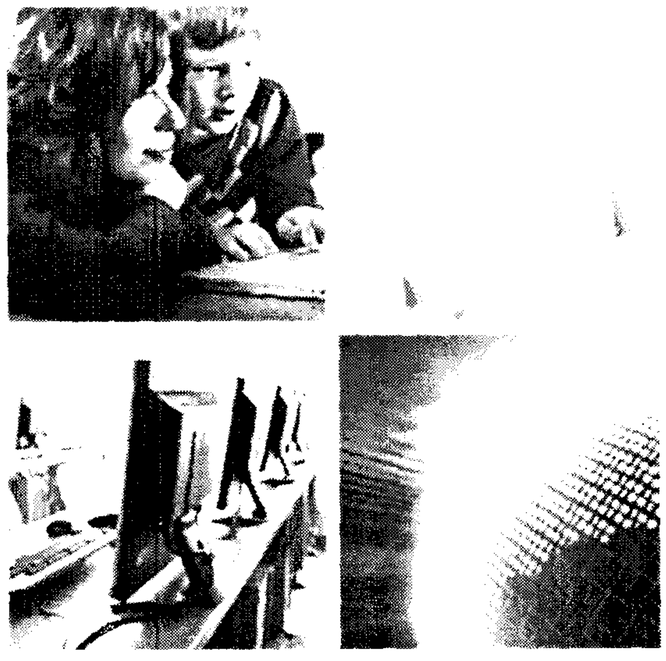
Ex SPRING THAW Concept of Operations

- A significant cyber event has occurred and a Director level meeting was held with the decision that DGs should meet
- A consolidated brief would be provided to each DG
  - Need to confirm with each Director what it would entail
- Scenario #1 plays out (45-60 minutes)
- Scenario #2 plays out (45-60 minutes)
- Post exercise (60 minutes)
  - Discussion
  - Identification of lessons learned
  - Action items
  - Next steps

Potential Dates

- Thursday, 22 March, 9:00-12:00
- Monday, 2 April, 9:00-12:00
- Monday, 9 April, 9:00-12:00

Public Safety Canada | Sécurité publique Canada



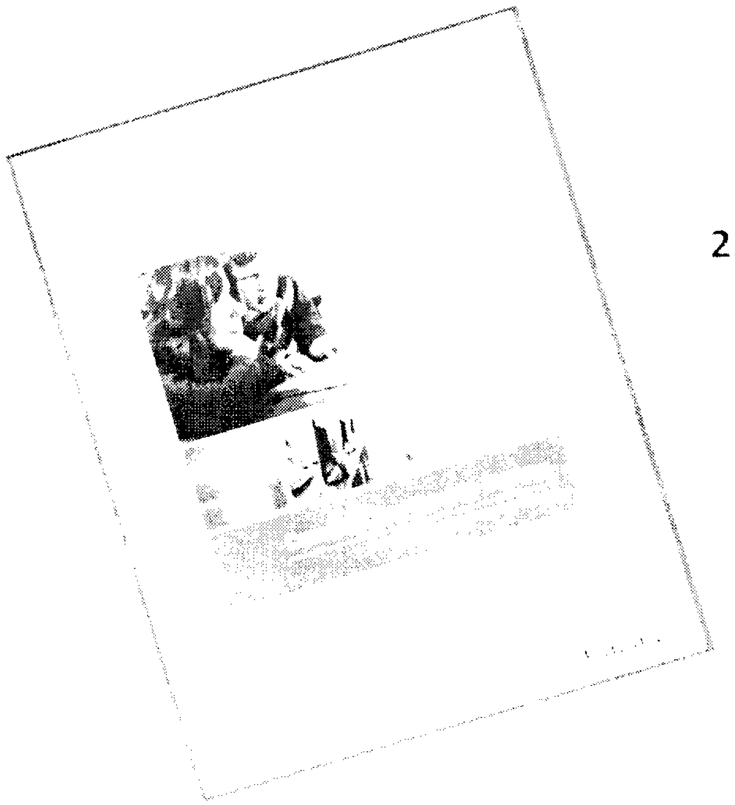
Update on Canada's Cyber Security Strategy

Information Technology Association of Canada
Cyber Security Forum
6 March 2012

Canada

Progress in Implementation

Since the release of the Government of Canada's Cyber Security Strategy in 2010, Public Safety Canada has been working to implement the **three** pillars:



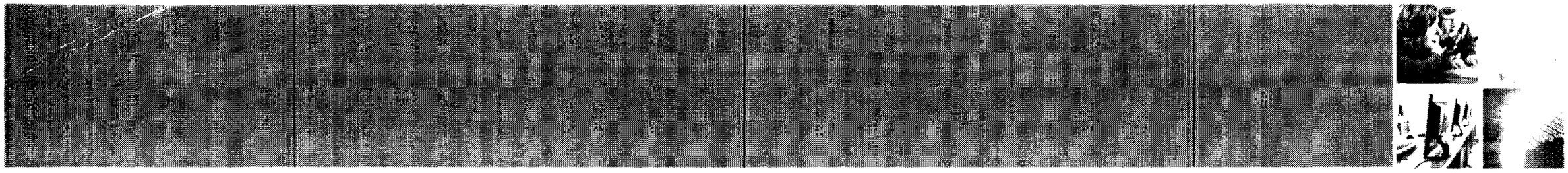
1. **Secure Government systems**
   - **Network consolidation:** established *Shared Services Canada*
   - **Improved cyber incident response capabilities:** realigned roles for the Communications Security Establishment Canada (CSEC) and the Canadian Cyber Incident Response Centre (CCIRC)

2. **Partner to secure systems outside the Government of Canada**
   - **Engaging critical infrastructure:** established collaborative mechanisms for information sharing and joint action plans
   - **Equipping the private sector:** strengthened CCIRC's relationships and service offerings
   - **Defining Roles and Responsibilities:** creating a *National Incident Response Framework* to coordinate response in the event of a major cyber incident
   - **Working with international partners:** developing policy and operational partnerships with key allies

3. **Help Canadians to be secure online**
   - **Improved public awareness:** launched a nationwide communications campaign *"Get Cyber Safe"* in October 2011

Aligning resources with priorities

Goals of resource allocation	*Canada's Cyber Security Strategy*	Support national priorities
Achieve integrity and strengthen capability	**Pillar 1**: Secure Government systems	Strengthen Canada's national security
Protect critical assets and information	**Pillar 2**: Partner to secure vital cyber systems outside the Government of Canada	Sustain Canada's economic prosperity
Combat cyber crime and promote public awareness	**Pillar 3**: Help Canadians to be secure online	Protect Canadian citizens online



Engaging critical infrastructure sectors is vitally important in order to sustain Canada's economic prosperity:

Information Sharing and National Reporting

- Improving threat, vulnerability, incident and mitigation information sharing between government and industry
- Launched the "CI Gateway" – a multi-sector information sharing portal and continue to develop a *National Cyber Incident Response Framework*
- Developed operational arrangements with private sector partners, including memorandums of understanding

Cross Sector Collaboration

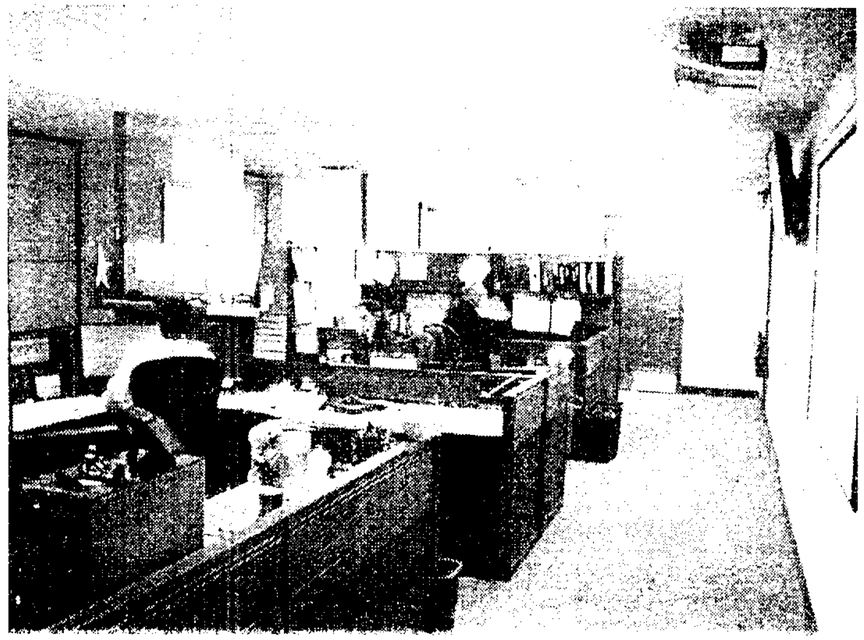
- Help to build a culture of security and position cyber a key component on the organizational security agenda
- Host an annual *National Cross Sector Forum* and biannual intercessional events to strengthen operational relationships between various critical infrastructure sectors
- Creating cyber-focused Action Plans for specific sectors to align priorities and promote collaboration

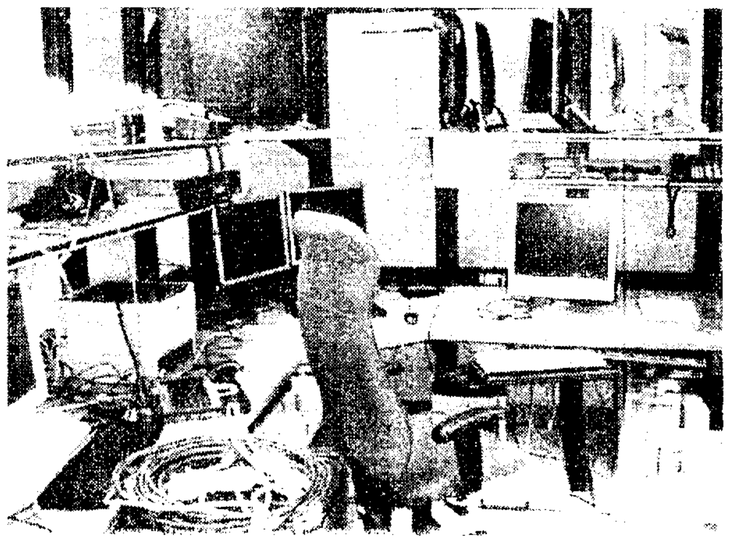
Repositioning CCIRC

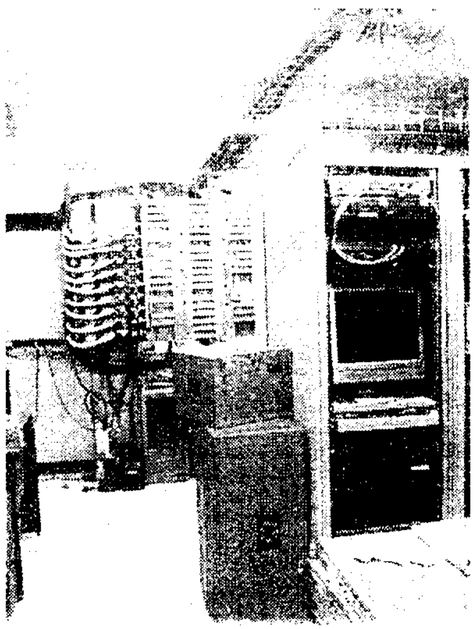
- CCIRC is now the national computer emergency response team (CERT) for provinces, territories and critical infrastructure sectors
- Entrusted with coordinating the response to cyber security incidents of national interest and protecting critical infrastructure
- Provides a range of products and services to public and private partners

The Canadian Cyber Incident Response Centre

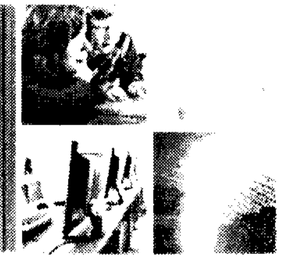
- CCIRC is Canada's cyber response team:
  - primary contact point into Government for domestic and international partners, including the private sector and critical infrastructure partners
  - CCIRC subject matter experts respond 07:00 – 23:00, 16 hour support function, with after hours coverage by the *Government Operations Centre*
- CCIRC also functions as a Computer Research and Test Lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors







CCIRC functions



These partners..

Government S&I community

Critical Infrastructure

Provinces and territories

Five Eyes and International CERTs

Trusted vendors

Academia

Cyber security expert community

Open source

provide information to..

CCIRC

which results in these services:

Incident Handling and National Event Coordination and Assistance
- Direct technical assistance to partners and coordination of Government response to cyber events of national significance
- Audience: technical staff in partner organizations responding to cyber incidents
- Metric: 749 incidents responded to in 2011. 197 notifications to partners of compromised systems. 9 requests issued to shut down malicious systems in Nov-Dec 2011

Provision of Mitigation Advice
- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice
- Audience: technical staff in partner organizations
- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

Reporting and Analysis
- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis
- Audience: technical staff and decision makers

Questions?

Sébastien Labelle
National Cyber Security Directorate, Public Safety Canada
Sebastien.labelle@ps.gc.ca

For more information on **CCIRC** or the CI Gateway Information Sharing Portal, please contact:
cyber-incident@ps-sp.gc.ca

05/13/2012

CYBER SECURITY

Issue

- Information is a strategic asset, and Canada and a growing number of countries are putting in place national cyber security strategies to address this type of threat.

CANADIAN POSITION

- Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential to maintaining an innovative, prosperous economy and a secure society

- *Canada's Cyber Security Strategy* was announced by the Government in 2010. The Strategy unifies efforts across Government and reflects our view that cyber security is both an economic and a national security issue.

BACKGROUND

- Cyber systems – computers and the Internet – are fundamental for the effective operation of Government and national security, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians. A secure cyberspace is key to Canada's competitive advantage in the global marketplace, where industry relies on secure, stable and resilient digital infrastructure to transact business and protect personal and commercially sensitive information such as intellectual property.

- In recent years, there has been an alarming increase in the number of cyber incidents directed against all levels of society. The threats are often global in nature, and involve foreign states' military and intelligence agencies, transnational cyber criminals, industrial cyber espionage, and cyber terrorists looking to further military, economic and political objectives.

CYBER SECURITY – CANADA

- *Canada's Cyber Security Strategy* is now in its second year of implementation. It is designed to engage our international allies, as well as create partnerships with the private sector in promoting the cyber security of Canada's critical infrastructure sectors. Canada's Strategy is built on three pillars:

    - Securing Government systems to protect the information that Canadians and Canadian businesses entrust to us and to secure national security activities.

    - Partnering to secure vital cyber systems outside the federal government, including the systems that control our critical infrastructure and those that hold the valuable intellectual property of Canadian business. Early priorities include the governments of the provinces/territories and the

energy, financial, and telecommunications sectors.

- Helping Canadians to be secure online, We have started a national public awareness campaign to get Canadians the information they need to protect themselves online.

- The Strategy is a whole-of-Government effort being led by Public Safety Canada, with roles being played by 11 other departments and agencies. It allocates $90 million in funding over five years (2010-2015), with $18 million in annual funding thereafter.

CYBER SECURITY ACTIVITY IN THE AMERICAS

- Outside of bilateral work with the United States, Canada has had little engagement on cyber security issues within the hemisphere. Regionally, only a few countries (Canada, the United States and Colombia) have released formal cyber security strategies, although the issue is gaining in visibility following high profile cyber incidents in Brazil, Mexico, Venezuela and Chile over the last year.

- There has been no uniform response to cyber security within the hemisphere or more generally. Some nations have dealt with it as an issue for telecommunications regulation, while some have taken a law-enforcement/anti-terrorism approach. A smaller group have pursued an intelligence or military response. By way of example, in August 2010, the Brazilian army created a cyber-defense wing known as the Centro de Defesa Cibernética do Exército (Army's Center for Cybernetic Security). Canada's Strategy has elements of all of those approaches, although is only minimally focussed on the military dimension.

- Experts have noted that a lack of dedicated resources and technical expertise present significant obstacles to cyber security programs in Latin America. The Organization of American States has been trying to provide the means to pool expertise and provide a regional focus for cyber security programs. In 2003, the OAS General Assembly passed Resolution 1939 calling for the "Development of an Inter-American Strategy to Combat Threats to Cybersecurity."

- Since that time, hemispheric cyber security work has continued under the leadership of the OAS' Inter-American Committee against Terrorism (CICTE). There are four main streams to the proposed OAS Strategy:

  - information sharing with telecommunication operators;
  - fostering public-private partnerships to increase awareness and education;
  - setting technical standards to ensure information stays secure; and
  - adopting similar standards in cyber-crime legislation and policies.

- These four goals align well with Canada's own efforts, with the first two points being explicit parts of our national Strategy, while the last two points have guided our international partnerships more generally.

Drafted by: Corey Dvorkin, Public Safety/ Cyber Policy, 990-9608
Date of Draft: 5 March 2012

CYBER SECURITY IN THE AMERICAS

KEY MESSAGES TO CONVEY

- Cyber security is recognized internationally as a national security issue demanding government attention. We all rely on information systems and technology, and there is no going back to paper based systems.

- But those networks and connections need to be safe if they are to continue to help fuel innovation and prosperity. In a networked world, our cyber security is only as strong as the weakest link.

- Canada has recognized this and released its own Cyber Security Strategy in 2010, an element of which commits us to working with partners, both abroad and domestically, to pursue our shared security.

- Our Strategy reflects our outlook that cyber security has elements of national security, of economic security as well as personal security and privacy. We see the best way to achieve those goals as being through partnerships, both in Canada and internationally.

- Finally, I would like to note that dealing with cyber security in a counter terrorism/anti-crime context, as has been the case in the OAS context, does not always capture all aspects of the issue. In moving ahead with this issue we should continue to ensure that critical infrastructure protection and public engagement and awareness remain focal points of our efforts.

s.15(1) - Int'l

s.15(1) - Subv

- ***RESPONSIVE ONLY –*** [redacted]

  - While we are not in a position to make firm commitments at this time, we anticipate that we may be able to share our experiences in an experts visit or a regional workshop.

7 March 2012

Update on the Audit of Protecting Critical Infrastructure from Cyber Threats

Scope

The Office of the Auditor General (OAG) has requested documents and conducted interviews with key personnel concerning all aspects of Public Safety Canada's role in the development and implementation of *Canada's Cyber Security Strategy* (CCSS).

Based on the documents requested from the National Cyber Security Directorate, and communication with CCSS partners, it can be concluded that the scope of the audit is focused on the first two Pillars of the strategy.

Interest in the issues surrounding securing Government of Canada systems is implied by virtue of government being one of the ten critical infrastructure sectors. Moreover, the bulk of the new resources provided to implement the CCSS were dedicated to this task.

Interest in the activities under the second Pillar is implicit in the title of the audit, and is expected given the national scope of setting out to "secure systems of importance outside of the federal government."

Recommendations

The OAG has signalled that the draft recommendations will not be available until middle to late June, 2012.

However, the main themes being pursued by the OAG appear to be:

s.21(1)(a)

- Breadth and scope of the consultative process prior to the unveiling of the CCSS

s.21(1)(b)

- Governance of CCSS's implementation
- Horizontal coordination (resolving issues that affect multiple CCSS partners)
- Information sharing

[redacted]

Key Takeaways

- Leadership
- Clarity of roles and responsibilities
- Level of effort and progress on Pillar 2

Prepared by: Sergey Vershinin

Pages 936 to / à 939

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 940 to / à 956

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Subv, 21(1)(a), 21(1)(b), 15(1) - Int'l, 16(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 957 to / à 964

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - Subv, 15(1) - Int'l, 16(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Proposed Cyber Incident Management Framework – Outline For Discussion

DATE: April 2012
RDIMS # 574066

March 19th, 2012

-0

Outline – Major Headings

"Common look and feel with other similar documents of national scope"

- Purpose
- Background/Threat environment
- Scope
- Concept of operations
- Roles and responsibilities
- Control and communications
- Annexes

Purpose

- Provide a consolidated approach to the management and coordination of a significant cyber event
- Brings to bear the resources required to coordinate the response or mitigation actions to help secure Canadian cyberspace
- Voluntary compliance
- Partnership between FPT governments, CI and industry

Points to Consider:

- *Any other points to include?*

Background/Threat Environment

- Identifies the overall approach to cyber security in Canada (Canada's Cyber Security Strategy)
- Comments on the cyber landscape
- General points on cyber threats and how to manage and respond

Points to Consider:

- *Any other points to include?*

Scope

- Framework is an operational document dealing with a *significant* cyber threat or event
- Framework recognizes and complements legislative responsibilities of federal, provincial/territorial/municipal and other stakeholders
- Framework aligns with existing emergency management frameworks and structures

Points to Consider:

- *Significant could be defined as "something affecting Canada's national security, economic prosperity and quality of life."*
- *Do any other points need to be identified?*

Concept of Operations

- Phase I
  - Prevention/mitigation
  - Normal daily operations
- Phase II
  - Preparation/preparedness
- Phase III
  - Response
- Phase IV
  - Recovery

Points to Consider:

- *Should we identify who does what in each phase?*
- *Any other points to include?*

Roles and Responsibilities

- Role(s) of federal stakeholders
- Role(s) of other levels of government
- Role(s) of other stakeholders

Points to Consider:

- *It is recognized that the roles and responsibilities in cyber space are different than for traditional emergencies...*
- *What level of detail do we need?*
- *Any other points to include?*

Control and Communications

- Link to FERP
- Identify governance bodies at each level
- Escalation process

Points to Consider:

- *Do we list in the annex points of contact, 24/7 operation centres?*
- *Any other points to include?*

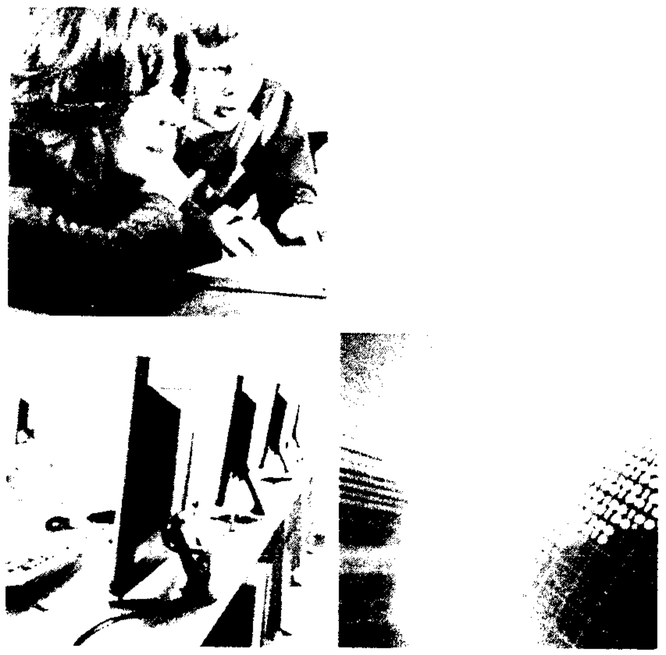
Annexes

- CCIRC's Information Sharing MOU
- Other information sharing agreements (i.e. Sector to sector?)
- Incident reporting template
- Trigger/escalation criteria
- 24/7 contact list?

Points to Consider:

- *What else should be included?*

Public Safety Canada | Sécurité publique Canada



Update on Canada's Cyber Security Strategy

Control Systems Security Workshop
Calgary, Alberta
March 27-28, 2012

Canada

Government of Canada Initiatives

- *Consultation Paper on a Digital Economy Strategy for Canada* (May 2010).

- *National Strategy and Action Plan for Critical Infrastructure* (May 2010).

- *Canada's Cyber Security Strategy* (October 2010).

- Beyond the Border: a shared vision for perimeter security and economic competitiveness

Canada's Cyber Security Strategy

- Signals cyber security as a priority investment for the Government of Canada.
- Coordinates and unifies domestic and international action.
- Built on three pillars:

1. Secure Government systems.
2. Partner to secure systems outside the Government of Canada.
3. Help Canadians to be secure online.

Aligning resources with priorities

Achieve integrity and strengthen capability	**Pillar 1**: Secure Government systems	Strengthen Canada's national security
Protect critical assets and information	**Pillar 2**: Partner to secure vital cyber systems outside the Government of Canada	Sustain Canada's economic prosperity
Combat cyber crime and promote public awareness	**Pillar 3**: Help Canadians to be secure online	Protect Canadian citizens online

Progress in Implementation

Since the release of the Government of Canada's Cyber Security Strategy in 2010, Public Safety Canada has been working to implement the **three** pillars:

1. **Secure Government systems**
   - **Network consolidation:** established *Shared Services Canada*
   - **Improved cyber incident response capabilities:** realigned roles for the Communications Security Establishment Canada (CSEC) and the Canadian Cyber Incident Response Centre (CCIRC)

2. **Partner to secure systems outside the Government of Canada**
   - **Engaging critical infrastructure:** established collaborative mechanisms for information sharing and joint action plans
   - **Equipping the private sector:** strengthened CCIRC's relationships and service offerings
   - **Defining Roles and Responsibilities:** creating a cyber incident management framework to coordinate response in the event of a major cyber incident
   - **Working with international partners:** developing policy and operational partnerships with key allies

3. **Help Canadians to be secure online**
   - **Improved public awareness:** launched a nationwide communications campaign "*Get Cyber Safe*" in October 2011

Engagement with Critical Infrastructure

Engaging critical infrastructure sectors is vitally important in order to sustain Canada's economic prosperity:

Information Sharing and National Reporting

- Improving threat, vulnerability, incident and mitigation information sharing between government and industry
- Launched the "CI Gateway" – a multi-sector information sharing portal and continue to develop a framework for cyber incident management
- Developed operational arrangements with private sector partners, including memorandums of understanding

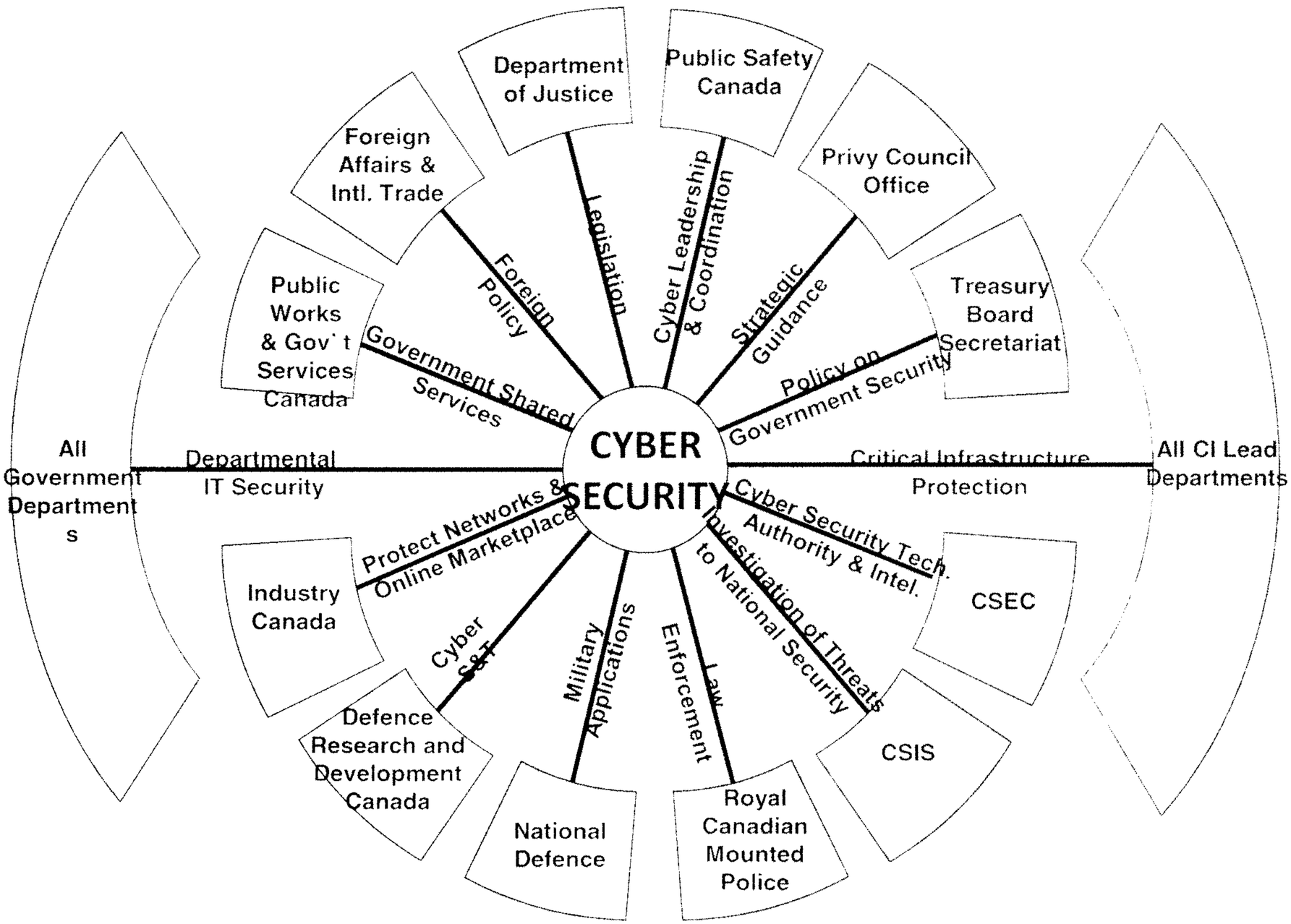
Cross Sector Collaboration

- Help to build a culture of security and position cyber a key component on the organizational security agenda
- Host an annual *National Cross Sector Forum* and biannual intercessional events to strengthen operational relationships between various critical infrastructure sectors
- Creating cyber-focused Action Plans for specific sectors to align priorities and promote collaboration

Repositioning CCIRC

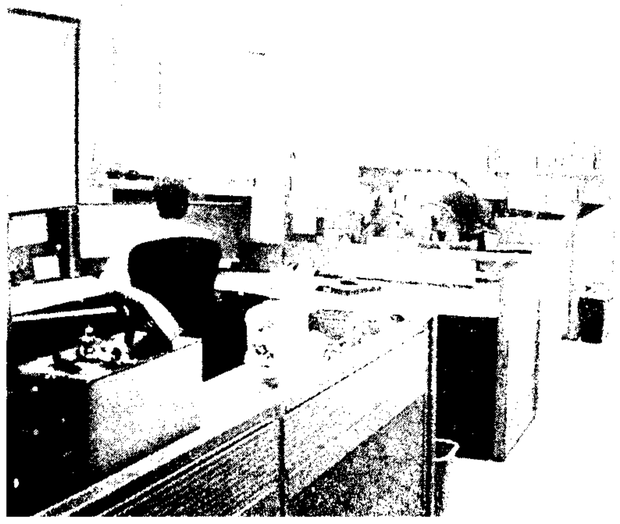
- CCIRC is now the national computer emergency response team (CERT) for provinces, territories and critical infrastructure sectors
- Entrusted with coordinating the response to cyber security incidents of national interest and protecting critical infrastructure
- Provides a range of products and services to public and private partners

Cyber Security Roles and Responsibilities within the Government of Canada



The Canadian Cyber Incident Response Centre

- CCIRC is Canada's cyber response team:
  - primary contact point into Government for domestic and international partners, including the private sector and critical infrastructure partners
  - CCIRC subject matter experts respond 07:00 – 23:00, 16-hour support function, with after hours coverage by the *Government Operations Centre*



- CCIRC also functions as a Computer Research and Test Lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors

CCIRC functions

These partners...

Government S&I community

Critical Infrastructure

Provinces and territories

Five Eyes and International CERTs

Trusted vendors

Academia

Cyber security expert community

Open source

provide information to...

CCIRC

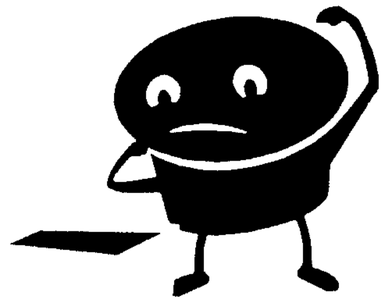
which results in these services:

Incident Handling and National Event Coordination and Assistance
- Direct technical assistance to partners and coordination of Government response to cyber events of national significance
- Audience: technical staff in partner organizations responding to cyber incidents
- Metric: 749 incidents responded to in 2011: 197 notifications to partners of compromised systems. 9 requests issued to shut down malicious systems in Nov/Dec 2011

Provision of Mitigation Advice
- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice
- Audience: technical staff in partner organizations
- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

Reporting and Analysis
- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis
- Audience: technical staff and decision makers

Questions?



Robert Dick
National Cyber Security Directorate, Public Safety Canada
robert.dick@ps-sp.gc.ca

For more information on **CCIRC** or the CI Gateway Information Sharing Portal, please contact:
cyber-incident@ps-sp.gc.ca

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

UPDATE ON NATIONAL DEVELOPMENTS

Growing awareness of the importance of cyber issues within Government
(Government of Canada lead: Public Safety Canada)
Cyber security issues are becoming a more frequent agenda item at senior levels within the federal and provincial governments of Canada. Within the federal government, senior management has requested more frequent cyber-related briefings, with Deputy Ministers meeting quarterly and Assistant Deputy Ministers meeting monthly.

The increased visibility of cyber security issues at senior levels of government will facilitate a whole-of-government response to strengthening Canada's cyber security.

Shared Services Canada
(Government of Canada lead: Public Works and Government Services Canada)
On August 4, 2011, the Government of Canada created Shared Services Canada to streamline the Government of Canada's information technology (IT) infrastructure. All resources associated with the delivery of email, data centre and network services are being transferred from 44 of the more IT-intensive departments and agencies to Shared Services Canada. These departments and agencies will no longer provide these services internally.

In addition to saving money, this consolidation will make Government of Canada IT systems and networks more secure. Reducing the number of data centres, Internet access points, and e-mail systems will create choke points, allowing Communications and Security Establishment Canada to better monitor network traffic throughout the Government of Canada. It will also facilitate the deployment of sensors capable of detecting threat signatures. Finally, having a centralized IT authority will facilitate the uniform deployment of patches and systems with built-in security across the federal government.

Spam Reporting Centre
(Government of Canada lead: Industry Canada)
As part of the Anti-Spam bill that was passed into law in December 2010, the Government will establish the Spam Reporting Centre. The Centre will be responsible for identifying and analysing trends in spam and other threats to electronic commerce.

The Spam Reporting Centre will accept various types of electronic messages from individuals and organizations in Canada. Reporting spam and related electronic threats will not stop such dangers completely; however, the data sent to the Spam Reporting Centre will help identify trends and find out from whom and from where spam is being sent. This will aid in the future prosecution and civil proceedings against those responsible for electronic threats in Canada and internationally.

The Government of Canada solicited bids via an open Request for Proposals to develop and operate the Spam Reporting Centre. The bid solicitation period closed on January 3, 2012,

and the Government of Canada is now reviewing submissions. The Centre is expected to become operational in the summer of 2012.

In addition to the Spam Reporting Centre, the Anti-Spam bill will prohibit, among other things:

- the sending of commercial messages without the recipient's consent;
- the installation of computer programs without the expressed consent of the owner of the system; and
- the collection of electronic addresses by the use of computer programs or the use of such addresses, without permission.

Critical Infrastructure Protection
(Government of Canada lead: Public Safety Canada)
Throughout 2011, Public Safety officials have taken a number of steps to engage domestic and international partners to protect Canada's critical infrastructure. They have:

- Provided cyber security briefings to critical infrastructure stakeholders through the National Cross Sector Forum and critical infrastructure sector networks, including energy and utilities, safety, government, and information and communications technology. As cyber security gains traction with the National Cross Sector Forum, it will facilitate future government engagement with private sector entities to strengthen Canada's cyber security.

- Held a cyber security awareness symposium with executives and critical infrastructure owner and operators, and hosted an international event on critical infrastructure dependencies, including cyber systems, with experts from Australia, the United Kingdom, Germany, Sweden, Netherlands and the United States (U.S.).

- Initiated and chaired and Interdepartmental Working Group on Process Control Systems Security to improve the resilience and security of process control (SCADA) systems. Public Safety Canada has hosted a series of SCADA workshops in various regions in Canada in cooperation with the Royal Canadian Mounted Police and our U.S. partners.

Throughout 2012, we will continue to expand the delivery of cyber security briefings to the critical infrastructure community to include additional sectors and classified briefings. Our officials will also work with sectors to identify and address cyber risks to critical infrastructure and finalize a cyber security information sharing framework to guide the dissemination and protection of cyber information shared between provincial and territorial governments and the critical infrastructure community.

Lawful Access Legislation and Implementation of the Budapest Convention
(Government of Canada lead: Public Safety Canada)
In February 2012, the Minister of Public Safety introduced Bill C-30, the *Protecting Children from Internet Predators Act*. Among other things, the Bill will allow Canada to implement provisions of the Budapest Convention that are not already part of Canadian law.

Parliament is now considering the legislation.

Copyright Modernization Act
(Government of Canada lead: Industry Canada)
On September 29, 2011, the Government introduced Bill C-11, *Copyright Modernization Act*, which aims to modernize Canada's copyright laws in a manner that would balance the interests of users and rights holders in the digital age. For example, the Bill includes provisions to expand the exemptions to use protected works for non-commercial purposes while increasing penalties for those who illegally use of distribute them.

The Bill is currently at Second Reading and is expected to be reviewed by Parliamentary Committee in the coming months.

SUGGESTED TALKING POINTS

- There have been a number of domestic cyber security developments in Canada.

- First, as part of our cyber security outreach efforts, we are raising the profile of cyber security in both the public and private sectors.

  - Within the federal government, Public Safety Canada has established a Deputy Ministers-level committee on cyber security which will meet quarterly.

  - With the critical infrastructure sector, we are stressing the importance of cyber security to keep our networks, electricity grid, and financial sector strong and resilient.

  - All of this awareness raising is putting cyber security on the minds of key decision makers. Over time, this will facilitate the implementation of *Canada's Cyber Security Strategy* as we will have buy-in from key stakeholders.

- Second, we are strengthening Canada's cyber security by consolidating government networks and developing tools to limit the delivery of spam.

  - In August 2011, the Government of Canada created Shared Services Canada which will take control and consolidate all resources associated with the delivery of email, data centre and network services from 44 departments.

  - This consolidation will make Government of Canada IT systems and networks more secure, by creating choke points that will allow Communications and Security Establishment Canada to better monitor network traffic throughout the Government of Canada.

  - Having a centralized IT authority will also facilitate the uniform deployment of patches and systems with built-in security across the federal government.

  - Canada is also establishing a Spam Reporting Centre, which will be responsible for identifying and analysing trends in spam and other threats to electronic commerce. The establishment of the Centre is a result of the omnibus Anti-Spam legislation that Canada passed in December 2010.

  - The Centre will aid in the future prosecution and civil proceedings against those responsible for electronic threats in Canada and internationally. It is expected to become operational early this summer.

- Third, the Government of Canada has introduced legislation that would modernize Canada's lawful intercept laws and implement provisions of the Budapest Convention that are not already part of Canadian law. Further, we are modernizing our copyright laws to deal with the demands of the digital world.

Pages 989 to / à 995

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

April 2012

CYBER SECURITY

Issue

- The Government of Canada has instituted *Canada's Cyber Security Strategy* and enjoys significant Canada-US cooperation in this area. Canada-Mexico cooperation on cyber security is limited by significantly differing justice regimes.

Canadian Position

- Canada is actively working to implement *Canada's Cyber Security Strategy* by enhancing the security of federal systems, partnering to secure systems outside of the federal government, and helping Canadians to be secure online.

- Canada and the US cooperate extensively on cyber security policy, operations, threat mitigation, and international engagement due to shared priorities. Mexican cyber priorities are very different and engagement is therefore limited.

Background

Information is a strategic asset. In Canada, all levels of government, the economy and society writ large are critically dependant on electronic and physical infrastructure which are vulnerable to exploitation by malicious actors.

Federal departments and agencies are making strides in the implementation of all three pillars of *Canada's Cyber Security Strategy*. First, the Government is enhancing the security of federal networks and systems, and establishing national leadership for cyber security programs. In August 2011, Shared Services Canada was created, which will improve federal cyber security. Second, the Government is pursuing partnerships to protect systems outside its control. Among early priorities is cooperation with the provinces, territories and critical infrastructure partners in the energy, financial, and telecommunications sectors.

Finally, a public awareness and education campaign aimed at giving Canadians the information they need to protect themselves has begun. It is being coordinated with similar American efforts.

Canadian and US officials are in regular contact within the intelligence, cyber security operations, and policy groups. Last fall, the Deputy Ministers of Public Safety and National Defence met with their US counterparts to discuss cyber security operations, international engagement and further underscore our mutual commitment to cyber security collaboration. Furthermore, under the *Shared Vision for Perimeter Security and Economic Competitiveness,* Canada and the US have outlined two specific cyber security focused initiatives. We are working together to strengthen bilateral coordination between Canadian and American national cyber security operations centres to ensure that North American critical infrastructure owners and operators receive the same information, advice, and guidance at the same time.

In future, and if resources permit, Canada will enhance its operational capability in the Canadian Cyber Incident Response Centre, and improve bilateral collaboration on cyber security information sharing and incident management between levels of government, our national critical infrastructure sectors, and with the US.

The second initiative is for the Government of Canada introduce legislation to enable the ratification of the Council of Europe *Convention on Cybercrime* and take steps to enhance joint leadership on international cyber security efforts. This will include the improved articulation of Canadian cyber security policy internationally and ensuring that Canadian delegations are well prepared to manage the strategic international positioning on cyber security issues at international fora.

The Budapest Convention

s.15(1) - Int'l

s.15(1) - Subv

The United States has made the promulgation of the Budapest Convention a central feature of its May 2011 *International Strategy for Cyberspace*, and is undertaking significant diplomatic effort to have the Convention become the international standard for cybercrime cooperation. The United States has requested Canada accelerate its efforts to ratify the Budapest Convention as part of the Beyond the Borders process.

The Budapest Convention is one of the only binding pieces of international legislation dealing with cybercrime. It commits partner states to establishing domestic laws to prosecute various aspects of cyber-crime, alongside a formal commitment to operational cooperation by law enforcement agencies in collecting evidence and honouring foreign warrants. The Government of Canada signed the Convention in 2001. However, a number of technical changes to allow sharing of police information internationally and for regulating the operations of domestic Canadian telecommunications companies are required before Canada would be in a position to ratify that signature. While such Bills have been brought forwarded several times in the past, none have passed. On February 14, 2002 the Government tabled a new piece of legislation, Bill C-30 the *Protecting Children from Internet Predators* Act which would, among other things, put in place the regulatory changes needed to ratify the Budapest Convention.

CYBER SECURITY
TALKING POINTS

- Especially in cyberspace, a threat to any of us is a threat to all. Coordinating our efforts and engaging our shared critical infrastructure owners and operators is essential to strengthening our collective cyber security.

- My Government launched *Canada's Cyber Security Strategy* last year. It focuses on enhancing the security of federal systems, partnering to secure systems outside of the federal government, and helping Canadians to be secure online. We are making progress in its implementation.

- We need to encourage our officials to broaden and deepen our engagement efforts to strengthen North American cyber security.

- ***RESPONSIVE*** **– Budapest Convention**: Canada fully supports the Budapest Convention, and is an active participant in its rapid response network. The Government of Canada signed the Convention in 2001.

- A number of technical changes are required before Canada would be in a position to ratify that signature.. We have recently introduced legislation which will allow us to proceed with domestic ratification. That Bill is now before committee.

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

s.15(1) - Int'l

s.15(1) - Subv

BRIEF ON CYBER ISSUES

[redacted]

Cyber security: Canada is concerned about the rising threats emanating from cyberspace and recognizes that partnerships with our allies and engagement at multilateral fora are critical in this respect.

Cybercrime: Canada fully supports the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*) as the best tool to fight cybercrime at the international level.

[redacted]

BACKGROUND

Cyber norms: A number of states, most prominently Russia and China, are seeking to reassert the role of the state in cyberspace, largely by arguing that concepts of national sovereignty be extended to this domain. [redacted]

Using this approach, they have sought to garner international support for this vision of cyberspace. For example, Russia has actively been pushing for the global adoption of an international information security treaty for the last decade.[1] Given cyberspace's destabilizing potential, Russia argues that a new international treaty is required to create an arms control regime to limit the proliferation of cyber weapons (however these are defined), and to prohibit cyber attacks and cyber terrorism under international law. [redacted]

[redacted]

Similarly, Russia and China, supported by Tajikistan and Uzbekistan, introduced a non-binding "International Code of Conduct for Information Security" at the United Nations General Assembly in September 2011.

The U.K., has launched an international discussion on non-binding cyber norms, which would set out the broad "rules of the road" for interactions in cyberspace. This approach seeks to reemphasize the importance existing cyber norms, such as the support for the multistakeholder model for Internet governance, and garner support for the idea that existing principles of international law (e.g. human rights law, the law of armed conflict) apply equally in cyberspace. Underpinning this normative approach to cyberspace is the idea that no major structural modifications to the cyberspace governance model or the international system are required to address new cyber issues. The London Conference on Cyberspace (November 1-2, 2011) brought together representatives from over 60 countries, the private sector and civil society to discuss a vision of cyberspace based on these high-level principles. Hungary will host the next iteration of the conference in Budapest in October 2012 and South Korea will host in 2013.

Cyber Security: The Government of Canada released Canada's Cyber Security Strategy in October 2010. Over the first five-year timeframe, the Strategy will secure Government of Canada systems, enhance partnerships to secure vital cyber systems outside the federal Government, and help protect Canadians as they connect to each other and to the world.

As part of its efforts to implement the Strategy, the Government of Canada has:

- Updated its laws to reflect the realities of the digital world by passing the *Anti-Spam Act* and creating new *Criminal Code* provisions related to identity theft.
- Introduced Bill C-30, the *Protecting Children from Internet Predators Act*, which will bring Canada in line with its international partners on lawful interception capabilities and mutual legal assistance;
- Strengthened the Canadian Cyber Incident Response Centre (CCIRC) by making it the national computer emergency response team for provinces, territories and critical infrastructure sectors;
- Engaged provincial and territorial governments to shape a joint action plan to guide collaboration on cyber security matters; and
- Developed a cyber security awareness campaign.

Cybercrime: The only international instrument that deals with cybercrime is the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*). Canada signed the Convention in 2001. In order to permit ratification of the Convention, Canada needs to make amendments to its domestic legislation. These changes are included in Bill C-30.

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

While the Convention is trumpeted as the gold standard to combat cybercrime among Western countries, a number of states have been reluctant join on the grounds that some of its core elements, such as the 24/7 information sharing network, are deemed to violate national sovereignty. It is also on sovereignty grounds that certain countries reject provisions in the Convention that allows Parties to access stored computer data with consent of the data's host or where it is publicly available.

Some countries also view it as politically unacceptable to accede to a largely European-centric treaty, having been negotiated between members and observers of the Council of Europe. These countries believe that a global cybercrime instrument, negotiated through a United Nations process, would be more representative of a global consensus. Currently, a U.N. study group, of which a Justice Canada official is the Rapporteur, is examining the issue of cybercrime and the viability of a global treaty. The U.N. report is not expected until 2013, at the earliest.

KEY MESSAGES

Approach to cyber issues

- Canada is committed to working cooperatively with our international partners to ensure that the Internet is kept open, safe, and accessible.

- An open, safe and accessible cyberspace is key to sustaining an innovative global digital economy, and a vibrant and connected global society.

- We recognise that some activity in cyberspace can potentially threaten international peace and security. However, in addressing these issues, it is critical that we avoid taking steps that would threaten the vibrancy and openness of cyberspace.

Norms for cyberspace

- Canada is strongly supportive of the United Kingdom's efforts to foster a multistakeholder dialogue on norms for cyberspace. Canada looks forward to advancing this dialogue in Hungary in 2012 and the Republic of Korea in 2013.

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

- Cyber norms would promote safe, predictable and consistent interactions while ensuring the Internet's unique accessibility and openness.

[redacted]

Cyber security

- Canada is concerned by the real and immediate threat posed by malicious cyber activity initiated by both state and non-state actors.

- In dealing with online threats, it is critical that states maintain strong legal checks and balances, judicial oversight and public accountability in order to safeguard human rights.

- We have shared interests in making cyberspace more secure. This is a global issue and will require strong international cooperation, not only among countries, but with the private sector as well.

Cybercrime

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

- Canada believes the general provisions of the Council of Europe *Convention on Cybercrime* are a useful model for domestic legislation and for international cooperation.

- Canada is committed to cracking down on computer-related crime, and is working to implement the domestic requirements that would allow Canada to ratify the Council of Europe *Convention on Cybercrime*.

April 2, 2012

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

s.15(1) - Int'l

s.15(1) - Subv

BRIEF ON CYBER ISSUES

ISSUE

The following provides a brief on cyber issues in advance of the 10th ASEAN Regional Forum Inter-Sessional Meeting on Counter Terrorism and Transnational Crime (10th ARF ISM on CTTC) in Quang Nam Province, Vietnam, on March 16-17, 2012.

[redacted]

BACKGROUND

Norms for cyberspace: At the UN General Assembly in 2011, Russia and China, supported by Tajikistan and Uzbekistan, introduced a non-binding "International Code of Conduct for Information Security." [redacted]

Separately, for the past decade, Russia has actively been pushing for the global adoption of an international information security treaty. Given cyberspace's revolutionary and destabilizing potential, Russia argues that a new international treaty is required to create an arms control regime to limit the proliferation of cyber weapons (however these are defined), and to prohibit cyber attacks and cyber terrorism under international law. [redacted]

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

The U.K., [redacted] has launched an international discussion on non-binding cyber norms, which would set out the broad "rules of the road" for interactions in cyberspace. This approach seeks to reemphasize the importance existing cyber norms, such as the support for the multistakeholder model for Internet governance, and garner support for the idea that existing principles of international law (e.g. human rights law, the law of armed conflict) apply equally in cyberspace. Underpinning this normative approach to cyberspace is the idea that no major structural modifications to the cyberspace governance model or the international system are required to address new cyber issues. The London Conference on Cyberspace (November 1-2, 2011) brought together representatives from over 60 countries, the private sector and civil society to discuss a vision of cyberspace based on these high-level principles. Hungary and South Korea have accepted to host the next iterations of the conference in 2012 and 2013 respectively.

Cyber Security: The Government of Canada released Canada's Cyber Security Strategy in October 2010. Over the first five-year timeframe, the Strategy will secure Government of Canada systems, enhance partnerships to secure vital cyber systems outside the federal Government, and help protect Canadians as they connect to each other and to the world.

As part of its efforts to implement the Strategy, the Government of Canada has:

- Updated its laws to reflect the realities of the digital world by passing the *Anti-Spam Act* and creating new *Criminal Code* provisions related to identity theft.
- Introduced Bill C-30, the *Protecting Children from Internet Predators Act*, which will bring Canada in line with its international partners on lawful interception capabilities and mutual legal assistance;
- Strengthened the Canadian Cyber Incident Response Centre (CCIRC) by making it the national computer emergency response team for provinces, territories and critical infrastructure sectors;

s.14(a)

- [redacted]
- Developed a cyber security awareness campaign.

Cybercrime: The only international instrument that deals with cybercrime is the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*). Canada signed the Convention in 2001. In order to permit ratification of the Convention, Canada needs to make amendments to its domestic legislation. These changes are included in Bill C-30. [redacted]

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

While the Convention is trumpeted as the gold standard to combat cybercrime among Western countries, a number of states have been reluctant join on the grounds that some of its core elements, such as the 24/7 information sharing network, are deemed to violate national sovereignty. It is also on sovereignty grounds that certain countries reject provisions in the Convention that allows Parties to access stored computer data with consent of the data's host or where it is publicly available.

Some countries also view it as politically unacceptable to accede to a largely European-centric treaty, having been negotiated between members and observers of the Council of Europe. These countries believe that a global cybercrime instrument, negotiated through a United Nations process, would be more representative of a global consensus. Currently, a U.N. study group, of which a Justice Canada official is the Rapporteur, is examining the issue of cybercrime and the viability of a global treaty. The U.N. report is not expected until 2013, at the earliest.

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

Cyber terrorism: Cyber terrorism is an ill-defined term. It is generally used as a catch all term to refer to any activity that terrorists conduct on the Internet. This includes activities such as recruitment, promotion of hate speech, coordination of activities, and financing. Canada generally refers to this as "terrorist use of the Internet," and efforts to counter these activities are part of Canada's counter-terrorism work.

[redacted]

KEY MESSAGES

Approach to cyber issues

- Canada is committed to working cooperatively with our international partners to ensure that the Internet is kept open, safe, and accessible.

- An open, safe and accessible cyberspace is key to sustaining an innovative global digital economy, and a vibrant and connected global society.

- We recognise that some activity in cyberspace can potentially threaten international peace and security. However, in addressing these issues, it is critical that we avoid taking steps that would threaten the vibrancy and openness of cyberspace.

Norms for cyberspace

- Canada is strongly supportive of the United Kingdom's efforts to foster a multistakeholder dialogue on norms for cyberspace. Canada looks forward to advancing this dialogue in Hungary in 2012 and the Republic of Korea in 2013.

- Cyber norms would promote safe, predictable and consistent interactions while ensuring the Internet's unique accessibility and openness.

- As we look to maintain the momentum on the norms dialogue, we believe that the ASEAN Regional Forum can play a key role in the development of cyber norms as they relate to regional peace and security issues.

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

[redacted]

Cyber security

- Canada is concerned by the real and immediate threat posed by malicious cyber activity initiated by both state and non-state actors.

- In dealing with online threats, it is critical that states maintain strong legal checks and balances, judicial oversight and public accountability in order to safeguard human rights.

- We have shared interests in making cyberspace more secure. This is a global issue and will require strong international cooperation, not only among countries, but with the private sector as well.

Cybercrime

- Canada believes the general provisions of the Council of Europe *Convention on Cybercrime* are a useful model for domestic legislation and for international cooperation.

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

- Canada is committed to cracking down on computer-related crime, and is working to implement the domestic requirements that would allow Canada to ratify the Council of Europe *Convention on Cybercrime*.

[redacted]

[redacted]

s.15(1) - Int'l

s.15(1) - Subv

April 10 2012

UNCLASSIFIED

CYBER SECURITY

Issue

- Information is a strategic asset, and Canada and a growing number of countries are putting in place national cyber security strategies to address this type of threat.

CANADIAN POSITION

- Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential to maintaining an innovative, prosperous economy and a secure society

- *Canada's Cyber Security Strategy* was announced by the Government in 2010. The Strategy unifies efforts across Government and reflects our view that cyber security is both an economic and a national security issue.

BACKGROUND

- Cyber systems – computers and the Internet – are fundamental for the effective operation of Government and national security, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians. A secure cyberspace is key to Canada's competitive advantage in the global marketplace, where industry relies on secure, stable and resilient digital infrastructure to transact business and protect personal and commercially sensitive information such as intellectual property.

- In recent years, there has been an alarming increase in the number of cyber incidents directed against all levels of society. The threats are often global in nature, and involve foreign states' military and intelligence agencies, transnational cyber criminals, industrial cyber espionage, and cyber terrorists looking to further military, economic and political objectives.

CYBER SECURITY – CANADA

- *Canada's Cyber Security Strategy* is now in its second year of implementation. It is designed to engage our international allies, as well as create partnerships with the private sector in promoting the cyber security of Canada's critical infrastructure sectors. Canada's Strategy is built on three pillars:

    - Securing Government systems to protect the information that Canadians and Canadian businesses entrust to us and to secure national security activities.

    - Partnering to secure vital cyber systems outside the federal government, including the systems that control our critical infrastructure and those that hold the valuable intellectual property of Canadian business. Early priorities include the governments of the provinces/territories and the energy, financial, and telecommunications sectors.

    - Helping Canadians to be secure online, We have started a national public

awareness campaign to get Canadians the information they need to protect themselves online.

- The Strategy is a whole-of-Government effort being led by Public Safety Canada, with roles being played by 11 other departments and agencies. It allocates $90 million in funding over five years (2010-2015), with $18 million in annual funding thereafter.

CYBER SECURITY – JAPAN

- Cyber security has quickly emerged as key concern in Japan following several high profile cyber incidents. Among those significant events in the past few years were a coordinated attack against the PlayStation 3 network in April 2011, which breached 77 million user accounts and cost Sony some ¥14 billion (Cdn$170 million).

- In September 2011, Mitsubishi Heavy Industries, Japan's largest defence contractor, admitted it was the victim of a significant cyber-incident, apparently aimed at accessing American military technology. According to reports the attackers used simplified Chinese characters; Beijing, however, publicly denied any Chinese involvement. Finally, in October 2011, news came to light that Japan's Parliament, the *Diet*, had its own networks breached and at least three members of the lower house were having their e-mail monitored.

- There were media reported that the United States government issued "stern warnings" to Japan following the Mitsubishi incident, and the Japanese Cabinet met specifically to discuss the issue.

- Cyber security in Japan is managed by the National Information Security Center. Operating as an agency of the Cabinet Office of the Prime Minister, it has historically been tasked with technical measures for cyber security, although its mandate has recently grown to include policy development and public-private coordination.

- NISC released Japan's first national cyber strategy in 2006, which was followed by a second strategy in 2009. The current strategy, "An Information Security Strategy to Protect the Nation" was released in 2010. Covering much of the same ground as Canada's Strategy, the Japanese plan addresses governance and internal coordination, international and domestic collaboration, and cooperation between the public and private sectors.

- Like Canada, Japan is also pursuing a digital economy strategy, "i-Japan 2015." Released in July 2009, it sets out three priority areas – electronic government; online healthcare; and education and human resources. "i-Japan" also includes sections on revitalizing industry and local communities, nurturing new industries and research, and calls for improving Japan's digital infrastructure.

- To date the Japanese military has only a limited role in cyber security, although in January 2012 it was revealed that the Defense Ministry's Technical Research and Development Institute had succeeded in a three-year effort to develop a "defensive cyber weapon," capable of following back an attack and disabling the offending computer. Japanese defence officials admitted the legality of actually using such a system are quite murky: cyber-attacks were not included in a 2005 Japanese Cabinet

decision outlining situations where the Constitutional right to self-defence can be exercised.

CYBER SECURITY – INTERNATIONAL POLICY

- Like Canada, Japan participated in the London Conference on Cyberspace. The London Conference launched a process strongly supported by Canada, which aims to define norms of conduct for behaviour in cyberspace. Follow-on conferences will be held in Budapest, Hungary in October of this year and in Seoul, South Korea in Fall 2013.

- Russia has promoted this approach at the G-8, the ASEAN Regional Forum, the International Telecommunications Union, and a variety of other security and economic organizations. The Russian view was recently formalized in a "Code of Conduct for Information Security" which it tabled at the United Nations in September 2011, as a potential model for a cyberspace treaty.

UNITED NATIONS GROUP OF GOVERNMENTAL EXPERTS

- Canada and Japan have both agreed to be among the 15 countries participating in a United Nations Group of Governmental Experts (GGE) dealing with the political and military aspects of cyberspace this summer. This will be the third GGE, and the first time either Japan or Canada has participated.

- The first GEE, which met in 2004-05 ended in deadlock between Russian and American representatives. The main point of contention was reportedly on whether current international law, and the laws of armed conflict, applied in cyberspace.

- The second GGE, co-chaired by the US and Russia in 2009-2010, seemed to signal a shift in international cyber politics. It was able to reach consensus, and issued a report with five recommendations. Chief among them was an explicit endorsement of "norms" for cyberspace – a tacit understanding that norms, as opposed to formal treaties, could be used to build confidence among countries operating in cyberspace. While this development is positive, Russia has not abandoned its request for a formal treaty regime for cyberspace.

Drafted by: Corey Dvorkin, Public Safety/ Cyber Policy, 990-9608
Date of Draft: 10 April 2012

CYBER SECURITY

KEY MESSAGES TO CONVEY

- Cyber security is recognized internationally as a national security issue demanding government attention. We all rely on information systems and technology, and there is no going back to paper based systems.

- But those networks and connections need to be safe if they are to continue to help fuel innovation and prosperity.

- Canada has recognized this and released its own Cyber Security Strategy in 2010, an element of which commits us to working with partners, both abroad and domestically.

- Our Strategy reflects our outlook that cyber security has elements of national security, of economic security as well as personal security and privacy.

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

- We see the upcoming meeting of the United Nations Group of Governmental Experts as a key opportunity to shape international policy.

Public Safety Canada | Sécurité publique Canada

Cyber Incident Management Framework

Presentation to Stakeholders

DATE: April 2012
RDIMS # 599599

Canada

Context (1/2)

- Growing magnitude and pervasiveness of cyber attacks requires improved national coordination in mitigating and responding to a significant cyber event
- Emergency Management is well defined and established
  - But there is no national framework for cyber incidents specifically
- National-level cyber incidents challenges traditional emergency management structures:
  - No geographical jurisdiction
  - No clear definition of first-responders
  - Significant response role for private sector

Context (2/2)

- Effective national cyber incident response (management) requires clarification of:
  - Governance and responsibilities
  - Stakeholders engaged in national cyber incident management
  - Response and recovery coordination processes
  - Communications (messaging) synchronization
    - Between stakeholders
    - To the public
- Key allies (US, UK and AUS) have published national cyber incident response plans

Existing Processes/Plans: Federal/Provincial/Territorial

- Emergency Management Framework for Canada
  - High level document establishes agreement on the components and principles of emergency management, the coherency of action among the signatories and the governance structure
  - Establishes a common approach for the various FPT emergency initiatives and a conceptual model of the four components of EM: mitigation/prevention, preparedness, response and recovery
- National Emergency Response System (NERS)
  - Provides for a harmonization of joint federal, provincial, territorial response to emergencies
  - Can be triggered by:
    - Request for federal support by a PT
    - PT support of federal response to an emergency under federal jurisdiction

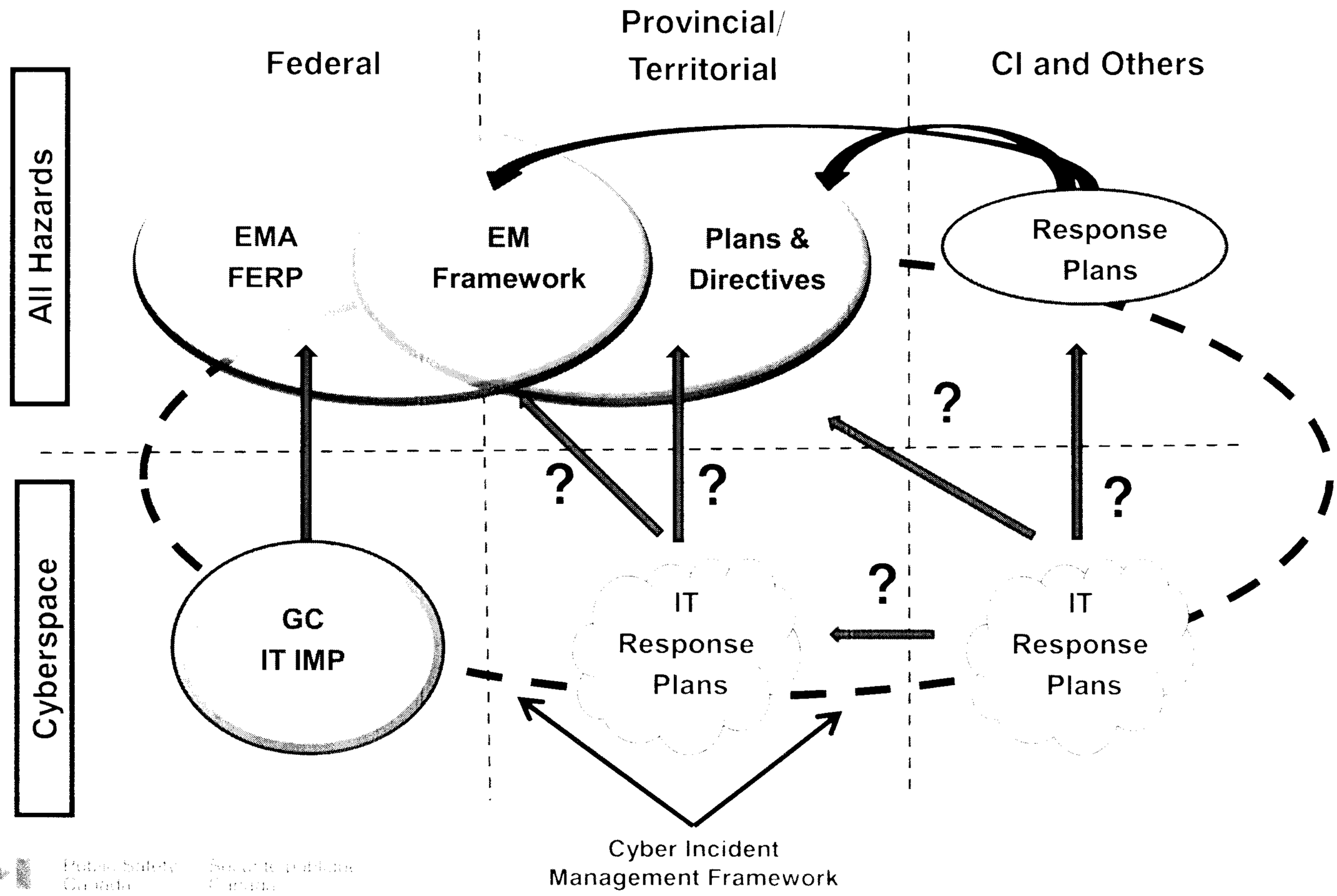
Existing Processes/Plans: Federal

- Emergency Management Act
  - Minister of Public Safety is responsible for coordinating the Government of Canada's response to an emergency
  - Clearly sets out roles and responsibilities of federal ministers and enhances Government of Canada readiness to respond to all types of emergencies
- Federal Emergency Response Plan
  - Outlines the processes and mechanisms to facilitate an integrated Government of Canada response to an emergency
  - Harmonizes federal emergency response efforts with those of the provinces and territories, non-government organizations and the private sector
- Government of Canada (GC) Information Technology Incident Management Plan
  - Reporting, response, and governance structure for a significant cyber event on a GC network

Existing Processes/Plans: Other

- Some sectors are developing arrangements and structures specific to their sector
  - Telecommunications Emergency Response (CTEPA/CTCP)
  - Industry specific (Canadian Electricity Association – GridEx)
- There may be other initiatives of which we are unaware

-Relationships



Proposal for a Cyber Incident Management Framework

- Ensure smooth national coordination and response to significant cyber events
- Clarify roles, responsibilities and expectations of all stakeholders
- Clarify linkages to national security and law enforcement activities
- Prevention of serious incidents
- Mitigate less serious incidents through information sharing and advice
- Integrate with NERS to ensure seamless integration and consequence management for those events that cascade out of the cyber domain

Proposed Components of the Framework

- Scope
- Concept of Operations
- Roles and Responsibilities
- Components:
  - Mitigation/Prevention
  - Preparedness
  - Response
  - Recovery
- Mechanisms:
  - CCIRC
  - MOU & Portal
  - Security clearances

Proposed Initial Stakeholders

- Federal Government
  - Key security and intelligence partners (RCMP, DND/CF, CSEC, CSIS, TBS, SSC)
- Provincial and Territorial Governments

s.14(a)
s.20(1)(d)

[redacted]

Approach to Development and Approval

- Will not seek a specific body to approve final document

Next 12 months

- Framework Ver 1.0 promulgated as a working document to which parties can sign on
- Initial set of stakeholders will collectively sign on and publicize
  - Present Framework at conference/events
- Considered an open document
  - All can link with access to CCIRC portal and MOU

Years 1-2

- Broader process after one year to revise and find new signatories
- In future, would consider appending voluntary codes of conduct, security standards, etc

Timeline

Information gathering - Assess interest with PT and industry partners - Assess existing related mechanisms and processes	Feb/Mar 2012	Underway
PS strawman review by proposed stakeholders	Apr/May 2012	Pending
PT partners - Consultation, exercise and validation	Apr/May 2012	
CI partners - Consultation, exercise and validation	May/June 2012	
Select Industry partners - Consult	Jul/Aug 2012	
Exercise with all partners	Oct 2012	
Final amendments	Nov 2012	
Initial Stakeholder Signoff	Jan-Mar 2013	
Final planning	Jan-Mar 2013	
Launch	Apr 2013	

UNCLASSIFIED

Date: 16/04/2012

File No.: 387047
RDIMS No.: 596638

MEMORANDUM FOR THE DIRECTOR GENERAL

UPDATE ON THE CRITICAL INFRASTRUCTURE AND CYBER SECURITY WORKSHOP

(Information only)

ISSUE

For your information, this note is presenting the adopted approach for the organization of the Critical Infrastructure and Cyber Security Workshop (the Workshop) scheduled for June 7-8, 2012, in Public Safety Canada's Executive Boardroom in Ottawa. In annexes, you will find the related documentation: the proposed agenda (**TAB A**), a draft invitation letter to invitees (**TAB B**), and the list of invitees (**TAB C**).

BACKGROUND

The Critical Infrastructure and Cyber Security Workshop will bring together some of the academic community working on issues related to critical infrastructure (CI) and cyber security with representatives from Public Safety Canada (PS) and other Government of Canada organizations. The key objectives of the Workshop are to:

- Facilitate a constructive dialogue on existing academic views/models in the area of CI and cyber security;
- Facilitate the establishment of a productive partnerships between academics and government; and,
- Raise awareness regarding the legislative/jurisdictional/resource landscape that may impact policy relevant research.

The Workshop will include sessions on the current landscape and future challenges facing CI, key trends in cyber security, cyber espionage, critical infrastructure interdependencies (focusing on cyber security issues), and creating a constructive and ongoing dialogue on critical infrastructure and cyber security issues.

CURRENT STATUS

To date, we have confirmed June 7 and 8 as the date of the Workshop and the Executive boardroom has been booked. A critical path (**TAB D**) including all the activities to make the Workshop successful was developed with CI and is updated at our weekly meetings.
National Cyber Security Directorate (NCSD) developed a list of speakers and participants for the Workshop drawing on the research papers contracted last fiscal year and consultation with Policy

.../2

and Issues Management, Technical Advice and CCIRC. As of yet only speakers (6) have been contacted and have agreed to participate in the Workshop. They are expecting more details from us by the second week of April. Among others, we will send them an official invitation, agenda, and their letter of agreement. These letters of agreement have been developed and require your signature (**TAB E**). To date, we estimate that travel costs at $3,500 for all speakers on cyber security.

For their part, CI has worked with us on the agenda and critical path, but their speakers are yet to be confirmed.

On the first day of the Workshop, the proposed agenda includes an overview of cyber security. We are proposing Canadian Security Intelligence Service (CSIS) or Communications Security Establishment Canada (CSEC) present an unclassified brief as part of the panel. Alternatively, should our partners decline to provide the presentation, we recommend that you present the unclassified deck prepared by CCIRC/Technical Advice (**TAB F**).

Regarding Official Languages, it is recommended that participants use the language of their choice and that the documentation is available in English and French simultaneously and of equal quantity.

With respect to the translation, we must obtain the approval of the speakers for their presentations to be translated, and all documentation should be sent to the Translation Bureau before the end of April to avoid additional costs.

Finally, a preliminary version of the briefing note to the Deputy Minister for hospitality has been developed (**TAB G**). The note will be completed during next week when we have more accurate estimates of travel costs and hospitalities. So far, we know that the hospitality cost will be shared between CI and NCSD and the costs are not expected to exceed $2,500 including taxes.

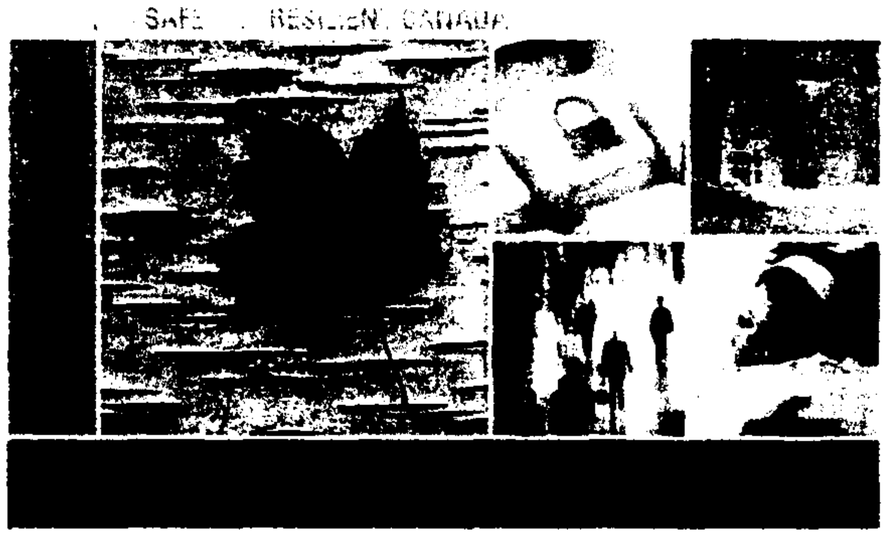
RECOMMENDATION

It is recommended that you approve the agenda, invitation, list of participants, and hospitality note. In addition a decision is required on whether you or Suki Wong will send the official invitation and agenda.

Your signature is also sought below for the letter of agreement to reimburse travel costs for the participants.

Should you require additional information, please do not hesitate to contact me at 613- 990-2655 or Jenifer Lévesque at 613-993-1418.

Sébastien Labelle
Director of Engagement and Partnerships
National Cyber Security



Conference on Critical Infrastructure and Cyber Security

269 Laurier West, Ottawa - June 7, 2012

8:00 - 8:30 a.m.	Registration
8:30 – 9:00 a.m.	Welcome & Introductions Speaker: Public Safety Canada
9:00 – 10:45 a.m.	**Session 1: Critical Infrastructure – Current Landscape** Speakers: CSIS/RCMP, Public Safety Canada, Andrew Graham, Kevin Quigley, and Martin Rudner • Threat overview • Policy challenges (e.g. jurisdiction/mandate issues) • Policy responses
10:45 – 11:00 a.m.	Break
11:00 – 12:15 a.m.	**Session 2: Cyber Security – Current Landscape** Speakers: CCIRC/CSEC, Christian Leuprecht, and Dave Lewis • Threat overview • Critical infrastructure exposure • Policy implications
12:15 – 1:30 p.m.	Lunch
1:30 – 2:45 p.m.	**Session 3: Critical Infrastructure Resilience – Future Challenges** Speakers: Stephen Flynn • Vulnerabilities • Emerging threats • Policy directions
2:45 – 3:00 p.m.	Break
3:00 – 4:30 p.m.	**Session 4: Cyber Security –Understanding the next 10 years** Speakers: Rafal Rohozinski, Benoit Dupont, and David Fewer • Key socioeconomic, technological and legal trends • Policy implications
4:30 – 5:00 p.m.	Summary/Wrap-up: Day 1 Speaker: Public Safety Canada

Conference on Critical Infrastructure and Cyber Security

269 Laurier West, Ottawa - June 8, 2012

8:00 - 8:10 a.m.	Registration
8:10 – 8:30 a.m.	Opening Remarks Speaker: Public Safety Canada
8:30 – 9:45 a.m.	**Session 5: Critical Infrastructure Dependencies – Cyber focus** Speakers: CCIRC, PS, Benoît Robert, José R. Martí, and Mark Fabro • Modelling dependencies • Response and Recovery • Supervisory control and data acquisition systems (SCADA)
9:45 – 10:00 a.m.	Break
10:05 – 10:45 a.m.	**Session 5 (continued)**
10:45 – 11:00 a.m.	Break
11:00 – 11:45 a.m.	**Session 6: Continuing the Conversation – How to Promote a Constructive Government and Academic Engagement** Speakers: Christian Leuprecht and DRDC (TBD) • Models and best practices
11:45 – 12:45 a.m.	Lunch
12:45 – 2:00 p.m.	**Session 6: Break out session – How to Promote a Constructive Government and Academic Engagement**
2:15 – 3:15 p.m.	**Session 6: Open session – How to Promote a Constructive Government and Academic Engagement** • Recommendations
3:15 – 3:30 p.m.	Closing Remarks Public Safety Canada

CRITICAL INFRASTRUCTURE – CYBER SECURITY CONFERENCE

June 7-8, 2012

Public Safety Canada
Deputy Minister's Boardroom, 19th Floor
269 Laurier Avenue West, Ottawa, Ontario

Information for Participants

Arrival and Registration
Please arrive by 8:00am each day to complete the visitor registration process.

Upon arrival, please present yourself to the reception desk with photo ID and state that you are here for the Critical Infrastructure – Cyber Security conference.
After the Commissionaire has confirmed your identification, you will receive your visitor's pass. A Public Safety Canada employee will escort you to the conference room.

Refreshments
Lunch and refreshments at two health breaks will be provided on both days. Please indicate whether you have any specific dietary requirements when you confirm your attendance.

Reimbursement of Travel and Accommodation Expenses
Public Safety Canada will be pleased to reimburse your travel and accommodation expenses, in accordance with Treasury Board guidelines. Further information will be provided once you confirm your attendance.

NCSD List of Participants for the Academic Conference

Non-government

Name	Contact
Benoit Dupont (Panelist)	École de criminologie Université de Montréal C.P. 6128, Succ. Centre-ville Montréal (Québec) H3C 3J7 Pavillon Lionel-Groulx 3150, rue Jean-Brillant, bureau C-4088 Téléphone : (514) 343-6111, poste 2586 Télécopieur : (514) 343-2269 benoit.dupont@umontreal.ca
David Fewer (Panelist)	Director CIPPIC, the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic University of Ottawa, Faculty of Law 57 Louis Pasteur St. Ottawa, Ontario K1N 6N5 Phone: (613)562-5800 (ext.2558) Fax: (613)562-5417 dfewer@uottawa.ca
Christian Leuprecht (Panelist)	Institute of Intergovernmental Relations Room 301 School of Policy Studies Queen's University Kingston, Ontario, Canada K7L 3N6 (613) 533-6633 (613) 533-2080 (secretary) (613) 533-6868 (fax) christian.leuprecht@queensu.ca
Mark Fabro (Panelist)	President and Chief Security Scientist Lofty Perch Inc. 1-888-GO-LOFTY (1-888-465-6389) Toronto • Austin • Washington D.C. • Sunshine Coast (AUS) mfabro@loftyperch.com
Rafal Rohozinski (Panelist)	Principal The SecDev Group World Exchange Plaza 45 O'Connor Street, Suite 1150 Ottawa, Ontario K1P 1A4 Office: +1 (613) 755-4007 Cell: (613) 883 5951 http://twitter.com/secdev
David Lewis (Panelist)	Liquidmatrix Security Digest 5016 Penman Lane Burlington, Ontario L7L 6J4 Dave.Lewis@amd.com

Paul C. Van Oorschot (Participant)	Canada Research Chair in Authentication and Computer Security School of Computer Science, Carleton University 1125 Colonel By Drive Ottawa, Ontario K1S 5B6 Canada Phone: (613)520-2600 x4356 Fax: (613)520-4334 paulv@scs.carleton.ca
Sara M. Smyth (Participant)	Assistant Professor Associate Director, International Cybercrime Research Centre (ICRC) School of Criminology Simon Fraser University Surrey Campus Office: 2764, Podium 2 250 - 13450 – 102nd Avenue Surrey, British Columbia V3T 0A3 Phone: 778-782-8844 sara_smyth@sfu.ca
Avner Levin (Participant)	Director, Privacy and Cyber Crime Institute Ted Rogers School of Management Ryerson University 350 Victoria Street Toronto, Ontario M5B 2K3 Phone:(416) 979-5000 x7690 Fax:(416) 979-5266 avner.levin@ryerson.ca http://www.ryerson.ca/privacyinstitute
Laura Huey (Participant)	Department of Sociology University of Western Ontario Room 5401, Social Science Centre London, Ontario N6A 5C2 Tel: 1-519-661-2111 ext. 87689 Fax: 1-519-661-3200 lhuey@uwo.ca

Government

Name	Contact
[redacted]	[redacted]
Dave Black RCMP, Manager, Cyber Crime Analysis Team, TCB	1426 St-Joseph blvd. Ottawa, ON K1A OR2 Dave.Black@rcmp-grc.gc.ca 613-993-6579
Tony Pickett RCMP, OIC, Technological Crime Program	1426 St-Joseph blvd. Ottawa, ON K1A OR2 Tony.Pickett@rcmp-grc.gc.ca 613-949-8905
Lesley Soper PCO, Senior Analyst	59 [redacted] Sparks Street Ottawa K1A 0A3 613-957-5359 613-957-5277 (fax) Lesley.Soper@pco-bcp.gc.ca
Ashley Anthony DRDC, DG, Centre for Security Science	222 Nepean Street Ottawa, ON K1A 0K2 Anthony.Ashley@forces.gc.ca 613-944-8195 ADMIN Christine Séguin: Christine.Seguin@forces.gc.ca 613-944-8196
[redacted]	[redacted]

Critical Path / "To Do" List Conference: Cyber + CI

Item	Lead	Status	Comments	March, 2012	April, 2012	May, 2012	June, 2012
Conference Proposal							
Set conference date	NCSD	Completed	June 7 & 8	March26-27			
Draft agenda	NCSD CI	In progress	NCSD approved	Week of March 26			
Senior Management approval of the Agenda	NCSD CI	In progress	NCSD Approved		Week of April 11 Hoping for the week of April 16		
Invitations							
Contact identified speakers, panelists, presenters	NCSD CI	In progress	Completed for NCSD	Week of March 26			
Create an invitation to explain the event	NCSD	Completed	Academia and participant	Week of March 26			
List of government and non government participants	NCSD CI	In progress	Completed for NCSD	Week of March 26			
Send out the agenda and the invitation to participants	NCSD	Delayed	A draft of the Agenda and the invitation was sent by email to NCSD speakers only NCSD DGO should send it on the week of the 23 of April		Wednesday April 11 Hoping for the week of April 16		
Create letter of agreement to be signed by DG (Domestic travel) ADM (International travel)	NCSD CI	In progress	NCSD letters signed				
Attach reimbursement form							
Have speakers sign letter of agreement (either prior to or at event)	NCSD CI	In progress	NCSD letters were sent and some are signed				

Critical Path / "To Do" List Conference: Cyber + CI

Item	Lead	Status	Comments	March, 2012	April, 2012	May, 2012	June, 2012
Request materials from speakers	NCSD	In progress	NCSD requested materials from the spearkers on April 11 Follow-up on April 25. Some presentation received and sent to translation				
Speakers have 60 days to return form and all receipts							
Request Biographies from the participants	NCSD CI	In progress	NCSD ask for the spearkers Biography on April 11				
Teleconference with the participants about the structure of the panel	NCSD CI	In progress					
Session 2: Cyber Security Current Landscape May 2, 2012, 11:00 teleconference for NCSD speakers	NCSD	In progress	NCSD is currently working on the logistics				
Session 4: Cyber Security Understanding the next 10 years May 2, 2012, 14:00 teleconference for NCSD speakers	NCSD	In progress	NCSD is currently working on the logistics				
Session 5: Critical Infrastructure Dependencies Cyber focus May 3, 2012, 11:00 teleconference for NCSD speakers	NCSD	In progress	NCSD is currently working on the logistics				
Session 6: Continuing the Conversation How to Promote a Constructive Government and Academic Engagement May 3, 2012, 14:00 teleconference for NCSD speakers	NCSD	In progress	NCSD is currently working on the logistics				
Venue/Hospitalities							
Note: For contracting purposes, it is preferable to request separate quotes for all aspects of Workshops. All transactions require a payment requisition form (9200)							
Confirm Event Date	NCSD	Completed		Week of March 26			
Hospitalities	NCSD	In progress	Breaks (break down of coffee, water, soft drinks, juices, crackers, cookies, etc.), Lunch The hospitality package is DM approved		Week of April 2nd		

Critical Path / "To Do" List Conference: Cyber + CI

Item	Lead	Status	Comments	March, 2012	April, 2012	May, 2012	June, 2012
BN on hospitalities	NCSD	Completed	Signed		Package to be sent to ADMO by April 11		
Create note to ADM for international travel reimbursement for speakers (this will likely accompany the $1500 hospitality request)	CI						
Inform recipients and prepare their travel to Ottawa - follow-up email including travel and hotel info.	NCSD	In progress	Suggestion for hotels were sent to NCSD speakers				
Organize an informal 5 à 7	NCSD	Completed	Reservation made at Tosca for 25 people at 5:30				
Logistic							
Translation of the invitation, the instructions and the agenda	NCSD	Completed			To be sent by April 11		
Confirm with participant if they need Interpretation services	NCSD		NCSD participants don't need interpretation		N/A		
If we need interpretation services:					N/A		
Send PWGSC official request form					N/A		
PWGSC will send confirmation by email					N/A		
Have confirmation signed off by DG					N/A		
Send confirmation back to PWGSC			(if Standing Offer does not currently exist in geographical area – inquire with PWGSC re: interpretation services)		N/A		
Send quotes to Contracting (Krystal Rockburn) and/or Finance (Greg Patterson) so they can review and write up contracts or "call up on standing offer" (if a standing offer exists between Government and company)					N/A		
Make sure the terms of individual quotes are not contingent on the fulfillment or promise of fulfillment of any other quotes			Provided by PWGSC		N/A		
Once quote has been signed off by DG, send to contracting					N/A		

Critical Path / "To Do" List Conference: Cyber + CI

Item	Lead	Status	Comments	March, 2012	April, 2012	May, 2012	June, 2012
Identify all translation needs and speak with translation to come to an arrangement about process and requests	CI						
Translation Need a quote Need agreement from presenters	NCSD		If we translate Speaking points it will have an impact on the cost. Need an email from the presenters saying they agree that we translate their presentations Need it by the end of April to avoid urgent fees				
Official language	NCSD	Completed	It is recommended that participants use the language of their choice and that the documentation is available in English and French simultaneously and of equal quantity.				
Audio-visual	NCSD	Completed	All the material need comes with the room				
Caterers	NCSD CI		DM approved. We need to start finding some quotes				
Material							
Print the decks. Bio's. Agenda	NCSD CI		Requested for the Cyber speakers				
Prepare a briefing binder for Robert	NCSD						
Draft speaking points for welcoming and closing remarks	NCSD				Week of April 16		
Print copies of the research papers	NCSD						
Event Activities							
Welcome participants	NCSD CI						
Take notes for each session	NCSD CI						
Clicker	NCSD CI						
Post-event/announcement Activities							
Send thank you letters to academia	NCSD CI						

Critical Path / "To Do" List Conference: Cyber + CI

Item	Lead	Status	Comments	March, 2012	April, 2012	May, 2012	June, 2012
Post event reports	NCSD/CI						

Date:

Avner Levin
Director, Privacy and Cyber Crime Institute
Ted Rogers School of Management
Ryerson University
350 Victoria Street
Toronto, Ontario M5B 2K3

Dear Mr. Levin,

This letter is to confirm that Public Safety Canada agrees to reimburse you an amount not to exceed $2,500.00 CDN, supported by all original receipts and in accordance with Treasury Board guidelines, to cover costs related to transportation, accommodation and meals to attend the Critical Infrastructure and Cyber Security Conference on June 7-8, 2012 at 269 Laurier Avenue West, Ottawa, ON. You will be reimbursed according to Appendix C of the National Joint Council Travel Directive at the Canadian rate (see attached guidelines). Please be aware that all expenses **must be paid by you and not by your employer** to qualify for reimbursement. Also, there is a deadline of 60 days from the date of this event to submit your travel expense claim and if received after this time period, Public Safety Canada will not reimburse.

This will also confirm that the liability of Public Safety Canada is limited to the reimbursement of those travel expenses listed above, for this event only. Upon completion of your travel, please forward your claim, including original receipts, to the attention of:

Sophie Fix
Office Manager
Public Safety Canada
11th Floor
340 Laurier Avenue, West
Ottawa, ON K1A 0P8

All reimbursements are subject to audit.

The Privacy Act applies to all personal information in any form held by Public Safety Canada, in connection with any services rendered pursuant to this agreement.

.../2

It is an explicit condition of this agreement that no Member of the House of Commons shall be admitted to any share or part of this agreement or to any benefit to arise therefrom.

By signing below, you agree to the above noted conditions. Please return a signed copy to Sophie Fix **(sophie.fix@ps-sp.gc.ca)** via scanned email or fax to 613-990-3287. Ms. Fix can be reached via telephone at 613-990-7055.

Sincerely,

Robert Dick
Director General
National Cyber Security Directorate

I have read and agree to the conditions set out above.

_____
Print Name of Attendee:

_____ _____
Signature of Attendee: Date

Enclosure: (1)

TRAVEL AND LIVING GUIDELINES: PER NATIONAL JOINT COUNCIL TRAVEL DIRECTIVE

Travel and living expenses are to be claimed in accordance with Treasury Board Travel Directive and not to exceed the guidelines as stated herein.
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_e.asp

MEALS

Breakfast	$15.60
Lunch	$14.85
Dinner	$40.85

For full calendar day status all meals and incidental $71.30.

Meals served in-flight and at conferences, meetings or workshops will not be reimbursed.

INCIDENTAL EXPENSES

Travellers may claim up to $17.30 per full and part calendar day in travel status.

ACCOMMODATION

At cost for the lowest negotiable rate for reasonable, non-luxury single commercial accommodation.

If private accommodation is used, up to $50.00 per night may be claimed.

TRANSPORTATION

At actual cost for economy or coach travel by air, bus or rail.

Public transit, airport buses, etc., are to be used for local transportation where practical.

Economy vehicles are to be used when car rentals are required unless the number of passengers or load justify a larger vehicle.

RECEIPTS AND VOUCHERS

Receipts and vouchers for accommodation and transportation are to be submitted with claims. No receipt or voucher is required for private accommodation.

For transportation charges under $10.00 (taxi, bus, etc.), receipts are not necessary but justification may be requested.

ENTERTAINMENT IS NOT AN ALLOWABLE COST

Date:

Laura Huey
Department of Sociology
University of Western Ontario
Room 5401, Social Science Centre
London, Ontario N6A 5C2

Dear Ms. Huey,

This letter is to confirm that Public Safety Canada agrees to reimburse you an amount not to exceed $2,500.00 CDN, supported by all original receipts and in accordance with Treasury Board guidelines, to cover costs related to transportation, accommodation and meals to attend the Critical Infrastructure and Cyber Security Conference on June 7-8, 2012 at 269 Laurier Avenue West, Ottawa, ON. You will be reimbursed according to Appendix C of the National Joint Council Travel Directive at the Canadian rate (see attached guidelines). Please be aware that all expenses **must be paid by you and not by your employer** to qualify for reimbursement. Also, there is a deadline of 60 days from the date of this event to submit your travel expense claim and if received after this time period, Public Safety Canada will not reimburse.

This will also confirm that the liability of Public Safety Canada is limited to the reimbursement of those travel expenses listed above, for this event only. Upon completion of your travel, please forward your claim, including original receipts, to the attention of:

Sophie Fix
Office Manager
Public Safety Canada
11th Floor
340 Laurier Avenue, West
Ottawa, ON K1A 0P8

All reimbursements are subject to audit.

The Privacy Act applies to all personal information in any form held by Public Safety Canada, in connection with any services rendered pursuant to this agreement.

.../2

It is an explicit condition of this agreement that no Member of the House of Commons shall be admitted to any share or part of this agreement or to any benefit to arise therefrom.

By signing below, you agree to the above noted conditions. Please return a signed copy to Sophie Fix (**sophie.fix@ps-sp.gc.ca**) via scanned email or fax to 613-990-3287. Ms. Fix can be reached via telephone at 613-990-7055.

Sincerely,

Robert Dick
Director General
National Cyber Security Directorate

I have read and agree to the conditions set out above.

_____
Print Name of Attendee:

_____ _____
Signature of Attendee: Date

Enclosure: (1)

TRAVEL AND LIVING GUIDELINES: PER NATIONAL JOINT COUNCIL TRAVEL DIRECTIVE

Travel and living expenses are to be claimed in accordance with Treasury Board Travel Directive and not to exceed the guidelines as stated herein.
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_e.asp

MEALS

Breakfast	$15.60
Lunch	$14.85
Dinner	$40.85

For full calendar day status all meals and incidental $71.30.

Meals served in-flight and at conferences, meetings or workshops will not be reimbursed.

INCIDENTAL EXPENSES

Travellers may claim up to $17.30 per full and part calendar day in travel status.

ACCOMMODATION

At cost for the lowest negotiable rate for reasonable, non-luxury single commercial accommodation.

If private accommodation is used, up to $50.00 per night may be claimed.

TRANSPORTATION

At actual cost for economy or coach travel by air, bus or rail.

Public transit, airport buses, etc., are to be used for local transportation where practical.

Economy vehicles are to be used when car rentals are required unless the number of passengers or load justify a larger vehicle.

RECEIPTS AND VOUCHERS

Receipts and vouchers for accommodation and transportation are to be submitted with claims. No receipt or voucher is required for private accommodation.

For transportation charges under $10.00 (taxi, bus, etc.), receipts are not necessary but justification may be requested.

ENTERTAINMENT IS NOT AN ALLOWABLE COST

Date:

G. Scott Knight
Associate Professor and Department Head
Department of Electrical and Computer Engineering
Royal Military College of Canada
PO Box 17000, Station Forces
Kingston, Ontario K7K 7B4

Dear Mr. Knight,

This letter is to confirm that Public Safety Canada agrees to reimburse you an amount not to exceed $2,500.00 CDN, supported by all original receipts and in accordance with Treasury Board guidelines, to cover costs related to transportation, accommodation and meals to attend the Critical Infrastructure and Cyber Security Conference on June 7-8, 2012 at 269 Laurier Avenue West, Ottawa, ON. You will be reimbursed according to Appendix C of the National Joint Council Travel Directive at the Canadian rate (see attached guidelines). Please be aware that all expenses **must be paid by you and not by your employer** to qualify for reimbursement. Also, there is a deadline of 60 days from the date of this event to submit your travel expense claim and if received after this time period, Public Safety Canada will not reimburse.

This will also confirm that the liability of Public Safety Canada is limited to the reimbursement of those travel expenses listed above, for this event only. Upon completion of your travel, please forward your claim, including original receipts, to the attention of:

Sophie Fix
Office Manager
Public Safety Canada
11th Floor
340 Laurier Avenue, West
Ottawa, ON K1A 0P8

All reimbursements are subject to audit.

The Privacy Act applies to all personal information in any form held by Public Safety Canada, in connection with any services rendered pursuant to this agreement.

.../2

It is an explicit condition of this agreement that no Member of the House of Commons shall be admitted to any share or part of this agreement or to any benefit to arise therefrom.

By signing below, you agree to the above noted conditions. Please return a signed copy to Sophie Fix (**sophie.fix@ps-sp.gc.ca**) via scanned email or fax to 613-990-3287. Ms. Fix can be reached via telephone at 613-990-7055.

Sincerely,

Robert Dick
Director General
National Cyber Security Directorate

I have read and agree to the conditions set out above.

_____
Print Name of Attendee:

_____ _____
Signature of Attendee: Date

Enclosure: (1)

TRAVEL AND LIVING GUIDELINES: PER NATIONAL JOINT COUNCIL TRAVEL DIRECTIVE

Travel and living expenses are to be claimed in accordance with Treasury Board Travel Directive and not to exceed the guidelines as stated herein.
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_e.asp

MEALS

Breakfast	$15.60
Lunch	$14.85
Dinner	$40.85

For full calendar day status all meals and incidental $71.30.

Meals served in-flight and at conferences, meetings or workshops will not be reimbursed.

INCIDENTAL EXPENSES

Travellers may claim up to $17.30 per full and part calendar day in travel status.

ACCOMMODATION

At cost for the lowest negotiable rate for reasonable, non-luxury single commercial accommodation.

If private accommodation is used, up to $50.00 per night may be claimed.

TRANSPORTATION

At actual cost for economy or coach travel by air, bus or rail.

Public transit, airport buses, etc., are to be used for local transportation where practical.

Economy vehicles are to be used when car rentals are required unless the number of passengers or load justify a larger vehicle.

RECEIPTS AND VOUCHERS

Receipts and vouchers for accommodation and transportation are to be submitted with claims. No receipt or voucher is required for private accommodation.

For transportation charges under $10.00 (taxi, bus, etc.), receipts are not necessary but justification may be requested.

ENTERTAINMENT IS NOT AN ALLOWABLE COST

Date:

Christian Leuprecht
Department of Political Science and Economics
Royal Military College of Canada
P.O. Box 17,000, Station Forces
Kingston, ON K7K 7B4

Dear Mr. Leuprecht,

This letter is to confirm that Public Safety Canada agrees to reimburse you an amount not to exceed $2,500.00 CDN, supported by all original receipts and in accordance with Treasury Board guidelines, to cover costs related to transportation, accommodation and meals to attend the Critical Infrastructure and Cyber Security Conference on June 7-8, 2012 at 269 Laurier Avenue West, Ottawa, ON. You will be reimbursed according to Appendix C of the National Joint Council Travel Directive at the Canadian rate (see attached guidelines). Please be aware that all expenses **must be paid by you and not by your employer** to qualify for reimbursement. Also, there is a deadline of 60 days from the date of this event to submit your travel expense claim and if received after this time period, Public Safety Canada will not reimburse.

This will also confirm that the liability of Public Safety Canada is limited to the reimbursement of those travel expenses listed above, for this event only. Upon completion of your travel, please forward your claim, including original receipts, to the attention of:

Sophie Fix
Office Manager
Public Safety Canada
11th Floor
340 Laurier Avenue, West
Ottawa, ON K1A 0P8

All reimbursements are subject to audit.

The Privacy Act applies to all personal information in any form held by Public Safety Canada, in connection with any services rendered pursuant to this agreement.

.../2

It is an explicit condition of this agreement that no Member of the House of Commons shall be admitted to any share or part of this agreement or to any benefit to arise therefrom.

By signing below, you agree to the above noted conditions. Please return a signed copy to Sophie Fix (**sophie.fix@ps-sp.gc.ca**) via scanned email or fax to 613-990-3287. Ms. Fix can be reached via telephone at 613-990-7055.

Sincerely,

Robert Dick
Director General
National Cyber Security Directorate

I have read and agree to the conditions set out above.

_____
Print Name of Attendee:

_____ _____
Signature of Attendee: Date

Enclosure: (1)

TRAVEL AND LIVING GUIDELINES: PER NATIONAL JOINT COUNCIL TRAVEL DIRECTIVE

Travel and living expenses are to be claimed in accordance with Treasury Board Travel Directive and not to exceed the guidelines as stated herein.
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_e.asp

MEALS

Breakfast	$15.60
Lunch	$14.85
Dinner	$40.85

For full calendar day status all meals and incidental $71.30.

Meals served in-flight and at conferences, meetings or workshops will not be reimbursed.

INCIDENTAL EXPENSES

Travellers may claim up to $17.30 per full and part calendar day in travel status.

ACCOMMODATION

At cost for the lowest negotiable rate for reasonable, non-luxury single commercial accommodation.

If private accommodation is used, up to $50.00 per night may be claimed.

TRANSPORTATION

At actual cost for economy or coach travel by air, bus or rail.

Public transit, airport buses, etc., are to be used for local transportation where practical.

Economy vehicles are to be used when car rentals are required unless the number of passengers or load justify a larger vehicle.

RECEIPTS AND VOUCHERS

Receipts and vouchers for accommodation and transportation are to be submitted with claims. No receipt or voucher is required for private accommodation.

For transportation charges under $10.00 (taxi, bus, etc.), receipts are not necessary but justification may be requested.

ENTERTAINMENT IS NOT AN ALLOWABLE COST

s.19(1)

Date:

Dave Lewis

[redacted]

Dear Mr. Lewis,

This letter is to confirm that Public Safety Canada agrees to reimburse you an amount not to exceed $2,500.00 CDN, supported by all original receipts and in accordance with Treasury Board guidelines, to cover costs related to transportation, accommodation and meals to attend the Critical Infrastructure and Cyber Security Conference on June 7-8, 2012 at 269 Laurier Avenue West, Ottawa, ON. You will be reimbursed according to Appendix C of the National Joint Council Travel Directive at the Canadian rate (see attached guidelines). Please be aware that all expenses **must be paid by you and not by your employer** to qualify for reimbursement. Also, there is a deadline of 60 days from the date of this event to submit your travel expense claim and if received after this time period, Public Safety Canada will not reimburse.

This will also confirm that the liability of Public Safety Canada is limited to the reimbursement of those travel expenses listed above, for this event only. Upon completion of your travel, please forward your claim, including original receipts, to the attention of:

Sophie Fix
Office Manager
Public Safety Canada
11th Floor
340 Laurier Avenue, West
Ottawa, ON K1A 0P8

All reimbursements are subject to audit.

The Privacy Act applies to all personal information in any form held by Public Safety Canada, in connection with any services rendered pursuant to this agreement.

.../2

It is an explicit condition of this agreement that no Member of the House of Commons shall be admitted to any share or part of this agreement or to any benefit to arise therefrom.

By signing below, you agree to the above noted conditions. Please return a signed copy to Sophie Fix (**sophie.fix@ps-sp.gc.ca**) via scanned email or fax to 613-990-3287. Ms. Fix can be reached via telephone at 613-990-7055.

Sincerely,

Robert Dick
Director General
National Cyber Security Directorate

I have read and agree to the conditions set out above.

_____
Print Name of Attendee:

_____ _____
Signature of Attendee: Date

Enclosure: (1)

TRAVEL AND LIVING GUIDELINES: PER NATIONAL JOINT COUNCIL TRAVEL DIRECTIVE

Travel and living expenses are to be claimed in accordance with Treasury Board Travel Directive and not to exceed the guidelines as stated herein.
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_e.asp

MEALS

Breakfast	$15.60
Lunch	$14.85
Dinner	$40.85

For full calendar day status all meals and incidental $71.30.

Meals served in-flight and at conferences, meetings or workshops will not be reimbursed.

INCIDENTAL EXPENSES

Travellers may claim up to $17.30 per full and part calendar day in travel status.

ACCOMMODATION

At cost for the lowest negotiable rate for reasonable, non-luxury single commercial accommodation.

If private accommodation is used, up to $50.00 per night may be claimed.

TRANSPORTATION

At actual cost for economy or coach travel by air, bus or rail.

Public transit, airport buses, etc., are to be used for local transportation where practical.

Economy vehicles are to be used when car rentals are required unless the number of passengers or load justify a larger vehicle.

RECEIPTS AND VOUCHERS

Receipts and vouchers for accommodation and transportation are to be submitted with claims. No receipt or voucher is required for private accommodation.

For transportation charges under $10.00 (taxi, bus, etc.), receipts are not necessary but justification may be requested.

ENTERTAINMENT IS NOT AN ALLOWABLE COST

Date:

Sara M. Smyth
Assistant Professor Associate Director
International Cybercrime Research Centre (ICRC)
School of Criminology
Simon Fraser University Surrey Campus Office: 2764, Podium 2
250 - 13450 – 102nd Avenue
Surrey, British Columbia V3T 0A3

Dear Ms. Smyth,

This letter is to confirm that Public Safety Canada agrees to reimburse you an amount not to exceed $2,500.00 CDN, supported by all original receipts and in accordance with Treasury Board guidelines, to cover costs related to transportation, accommodation and meals to attend the Critical Infrastructure and Cyber Security Conference on June 7-8, 2012 at 269 Laurier Avenue West, Ottawa, ON. You will be reimbursed according to Appendix C of the National Joint Council Travel Directive at the Canadian rate (see attached guidelines). Please be aware that all expenses **must be paid by you and not by your employer** to qualify for reimbursement. Also, there is a deadline of 60 days from the date of this event to submit your travel expense claim and if received after this time period, Public Safety Canada will not reimburse.

This will also confirm that the liability of Public Safety Canada is limited to the reimbursement of those travel expenses listed above, for this event only. Upon completion of your travel, please forward your claim, including original receipts, to the attention of:

Sophie Fix
Office Manager
Public Safety Canada
11th Floor
340 Laurier Avenue, West
Ottawa, ON K1A 0P8

All reimbursements are subject to audit.

The Privacy Act applies to all personal information in any form held by Public Safety Canada, in connection with any services rendered pursuant to this agreement.

…/2

It is an explicit condition of this agreement that no Member of the House of Commons shall be admitted to any share or part of this agreement or to any benefit to arise therefrom.

By signing below, you agree to the above noted conditions. Please return a signed copy to Sophie Fix (**sophie.fix@ps-sp.gc.ca**) via scanned email or fax to 613-990-3287. Ms. Fix can be reached via telephone at 613-990-7055.

Sincerely,

Robert Dick
Director General
National Cyber Security Directorate

I have read and agree to the conditions set out above.

_____
Print Name of Attendee:

_____ _____
Signature of Attendee: Date

Enclosure: (1)

TRAVEL AND LIVING GUIDELINES: PER NATIONAL JOINT COUNCIL TRAVEL DIRECTIVE

Travel and living expenses are to be claimed in accordance with Treasury Board Travel Directive and not to exceed the guidelines as stated herein.
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_e.asp

MEALS

Breakfast	$15.60
Lunch	$14.85
Dinner	$40.85

For full calendar day status all meals and incidental $71.30.

Meals served in-flight and at conferences, meetings or workshops will not be reimbursed.

INCIDENTAL EXPENSES

Travellers may claim up to $17.30 per full and part calendar day in travel status.

ACCOMMODATION

At cost for the lowest negotiable rate for reasonable, non-luxury single commercial accommodation.

If private accommodation is used, up to $50.00 per night may be claimed.

TRANSPORTATION

At actual cost for economy or coach travel by air, bus or rail.

Public transit, airport buses, etc., are to be used for local transportation where practical.

Economy vehicles are to be used when car rentals are required unless the number of passengers or load justify a larger vehicle.

RECEIPTS AND VOUCHERS

Receipts and vouchers for accommodation and transportation are to be submitted with claims. No receipt or voucher is required for private accommodation.

For transportation charges under $10.00 (taxi, bus, etc.), receipts are not necessary but justification may be requested.

ENTERTAINMENT IS NOT AN ALLOWABLE COST

Sécurité publique et Protection civile Canada
Public Safety and Emergency Preparedness Canada

269, avenue Laurier Ouest
Ottawa (Ontario)
K1A 0P8

Date

Benoit Dupont
École de criminologie
Pavillon Lionel-Groulx
3150, rue Jean-Brillant, bureau C-4088
Université de Montréal
C.P. 6128, Succ. Centre-ville
Montréal (Québec) H3C 3J7

Madame, Monsieur,

La présente a pour objet de vous informer que, conformément aux directives sur les voyages du Conseil du Trésor (ci-jointes), le ministère de la Sécurité publique et Protection civile a convenu de vous rembourser, jusqu'à concurrence de 2,500$, les frais accessoires et les dépenses (pour lesquelles vous devrez présenter les reçus originaux) que vous aurez engagés pour les déplacements, l'hébergement et les repas dans le cadre de ***(description de la réunion, date et lieu)***. Les repas fournis durant les réunions ne seront pas remboursés.

De plus, il est convenu que la responsabilité du ministère de la Sécurité publique et Protection civile se limite au remboursement des frais de déplacement susmentionnés engagés exclusivement dans le cadre de cette activité. Après votre retour, veuillez envoyer votre demande de remboursement, accompagnée des reçus originaux, à l'attention de ***(chargé de projet)*** au ministère de la Sécurité publique et Protection civile à l'adresse indiquée ci-dessus. Veuillez inscrire le numéro de référence ***(numéro d'engagement des fonds)*** sur votre demande. Tous les remboursements peuvent faire l'objet d'une vérification.

La *Loi sur la protection des renseignements personnels* s'applique à tous les renseignements personnels consignés sous quelque forme que ce soit par l'entrepreneur, l'organisme, le conseiller, etc. relativement aux services rendus dans le cadre de l'entente.

L'entente contient une condition explicite selon laquelle aucun membre de la Chambre des communes ne peut participer à l'entente ou en retirer des avantages.

Je vous prie d'agréer, Madame, Monsieur, mes salutations distinguées.

Canada

Sécurité publique et Protection civile Canada
Public Safety and Emergency Preparedness Canada

Gestionnaire du centre de coûts

Pièces jointes : (2)

Canada

LIGNES DIRECTRICES SUR LES VOYAGES ET L'HÉBERGEMENT

Les réclamations pour les frais de déplacement et d'hébergement doivent être conformes à la Directive du Conseil du Trésor concernant les voyages et ne doivent pas dépasser les montants indiqués ci-après :
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_f.asp

REPAS

Déjeuner	14,05 $
Dîner	13,50 $
Souper	38,40 $

Indemnité de repas pour une journée complète : 65,95 $

Les repas fournis à bord d'avions et aux conférences, réunions et ateliers ne sont pas remboursés.

FRAIS ACCESSOIRES

Pour chaque jour ou partie de jour passé en déplacement, le voyageur peut réclamer un maximum de 17,30 $.

HÉBERGEMENT

On remboursera les frais engagés au tarif négociable le plus bas pour un logement commercial (chambre individuelle) raisonnable et non luxueux.

S'il s'agit d'un logement privé, un montant maximal de 50 $ par nuit pourra être réclamé.

TRANSPORT

Remboursement des frais réels engagés pour un voyage en avion, en autobus ou en train en classe économique.

Le voyageur doit utiliser autant que possible les transports en commun, les navettes d'aéroport, etc., lorsque la situation s'y prête.

Lorsqu'il faut recourir à la location de véhicule, il faut louer des voitures compactes à moins que le nombre de passagers ou le poids des marchandises à transporter exige un plus gros véhicule.

REÇUS ET PIÈCES JUSTIFICATIVES

Les reçus et les pièces justificatives au titre de l'hébergement et du transport doivent être soumis avec les réclamations. Aucun reçu ou pièce justificative n'est nécessaire dans le cas de l'hébergement privé.

Il n'est pas nécessaire de présenter de reçus pour les frais de transport inférieurs à 10 $ (taxi, autobus, etc.), mais une justification peut être demandée.

LES FRAIS ENGAGÉS POUR LES DIVERTISSEMENTS NE SONT PAS ADMISSIBLES

Canada

Public Safety Canada / Sécurité publique Canada

SAFE RESILIENT CANADA

Cyber Threat Brief

RDIMS: 587908

Canada

The Cyber Environment Never Stops... Accelerating/Evolving/Expanding

SAFE RESILIENT CANADA

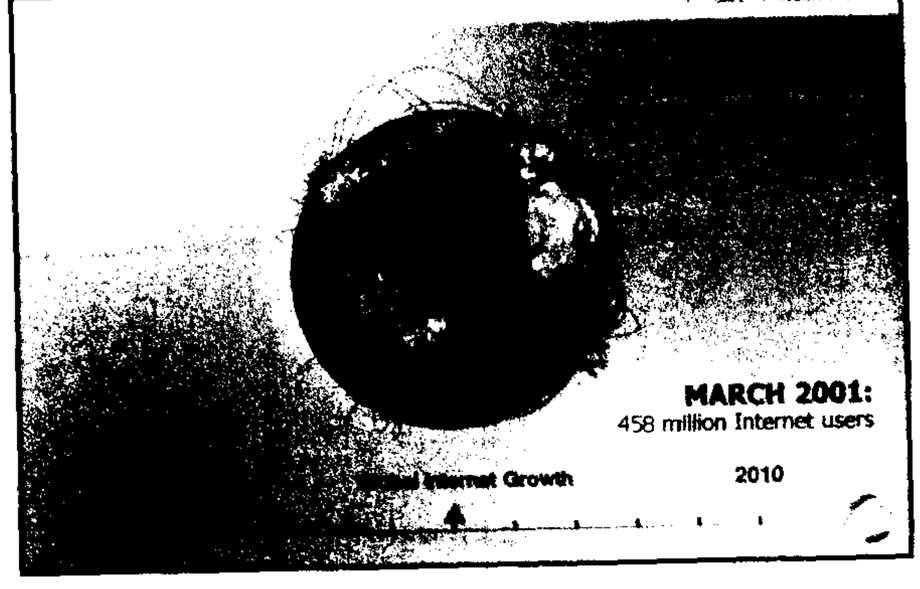
DECEMBER 1995:
16 million Internet users

1995 — Global Internet Growth — 2010

Public Safety Canada / Sécurité publique Canada

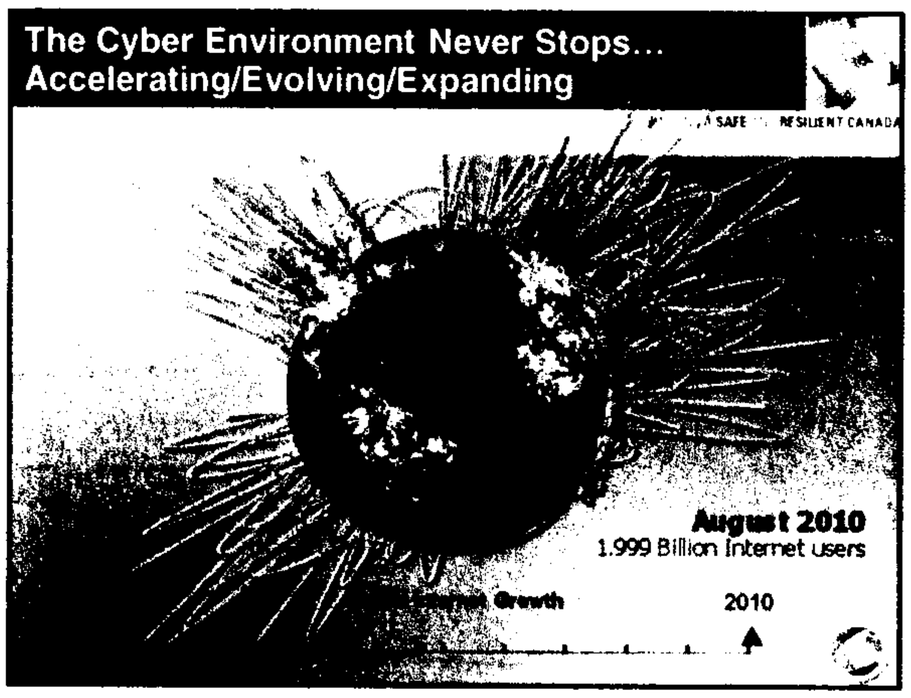
The Cyber Environment Never Stops... Accelerating/Evolving/Expanding

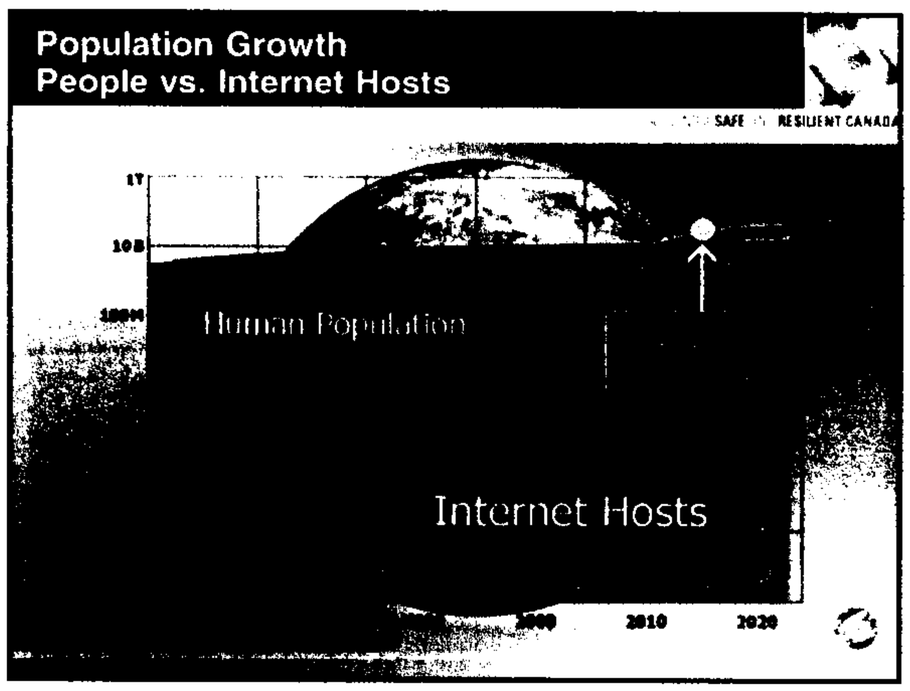
SAFE RESILIENT CANADA



MARCH 2001:
458 million Internet users

Global Internet Growth — 2010





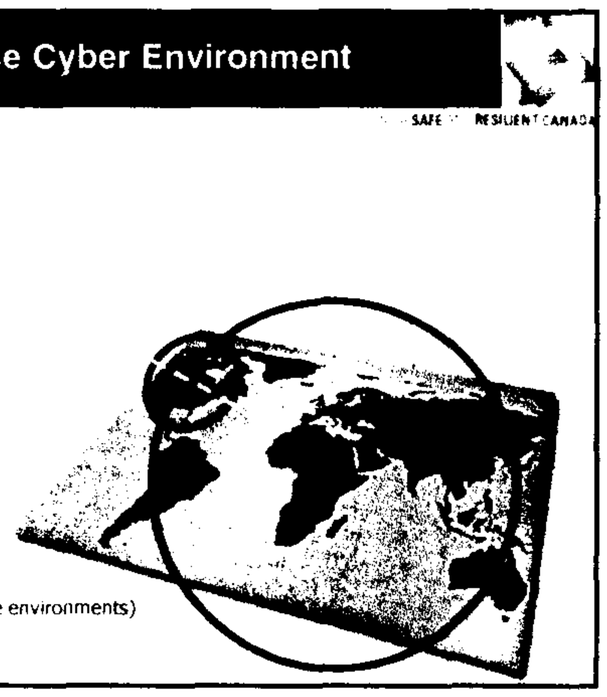
How important is cyber space?

SAFE RESILIENT CANADA

- Canadian economy relies heavily on the Internet
  - Canadian online sales in 2007 were $62.7b (est)
  - 87% of Canadian businesses used the Internet (2007)
- Canada's governments have become increasingly dependent on the Internet
  - 130 federal government services online
- Canadians are embracing cyberspace
  - 74% of Canadians had Internet service in 2008
  - 59% of Canadians filed income taxes electronically in 2008
  - 67% of Canadians banked online in 2009

Public Safety Canada | Sécurité publique Canada

Understanding the Cyber Environment

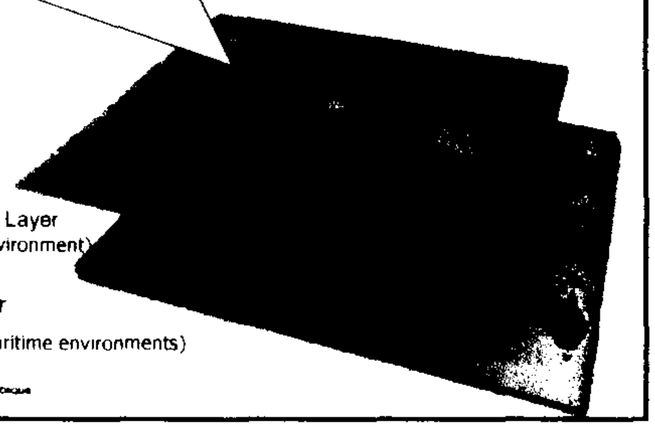


Geographic Layer

(Space, Air, Land, Maritime environments)

Understanding the Cyber Environment

- A man-made physical operating environment (the key terrain)
- Constantly changing, resilient and transnational
- Is not virtual or a cloud – Cyber exists in physical devices



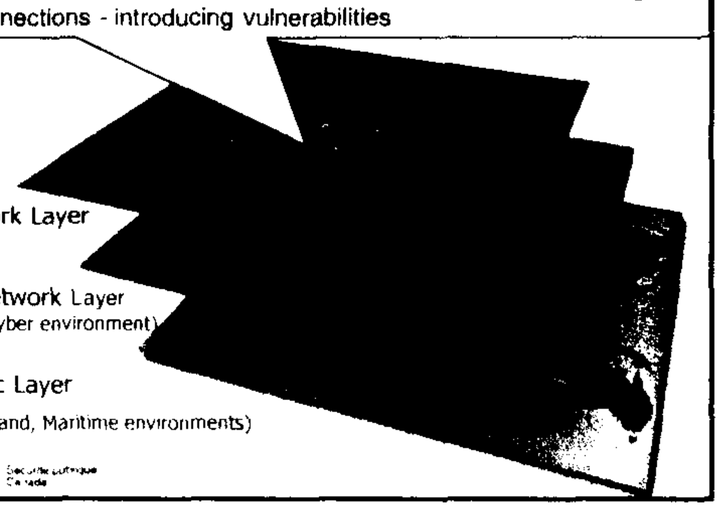
Physical Network Layer
(Man-made Cyber environment)

Geographic Layer

(Space, Air, Land, Maritime environments)

Understanding the Cyber Environment

Software-enabled functions with unforeseen outcomes and logical connections - introducing vulnerabilities

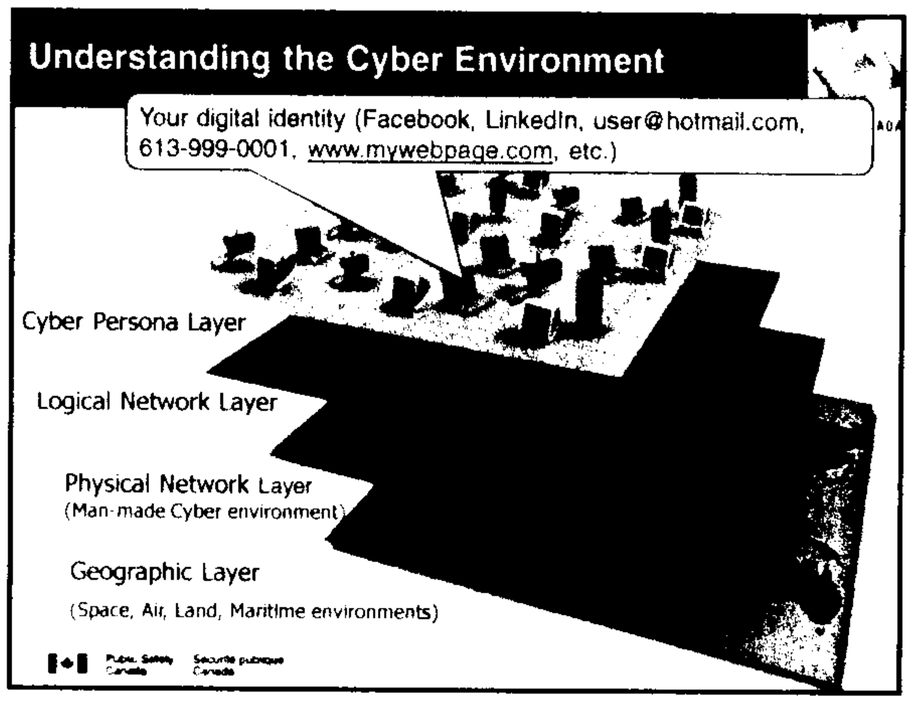


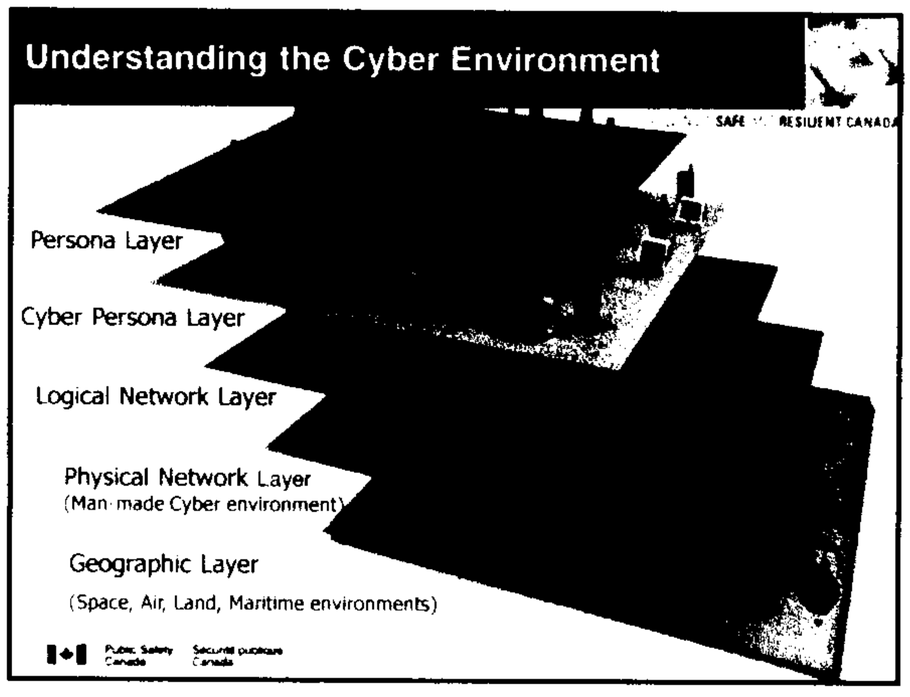
Logical Network Layer

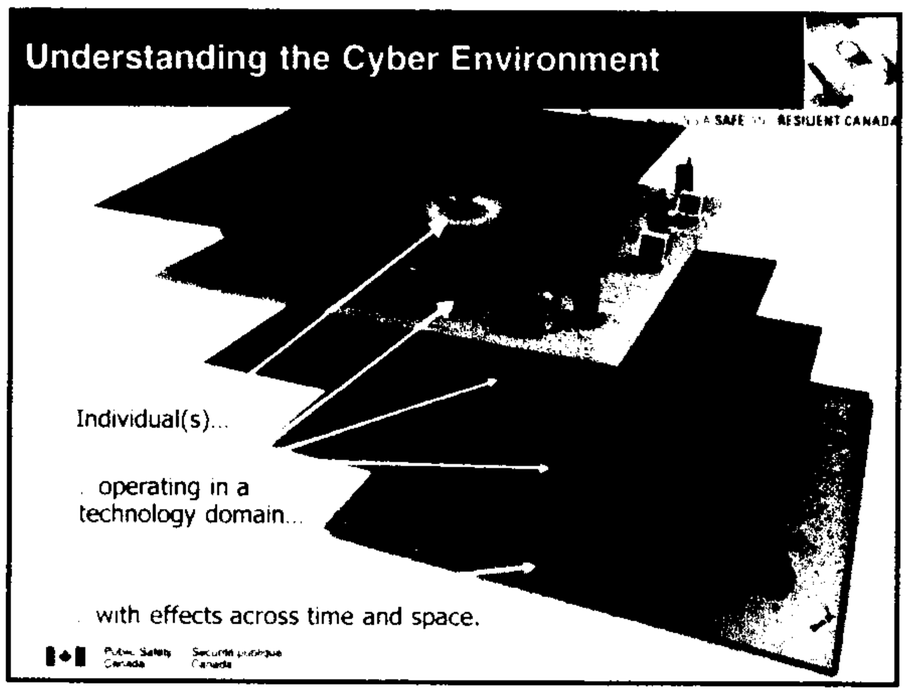
Physical Network Layer
(Man made Cyber environment)

Geographic Layer

(Space, Air, Land, Maritime environments)

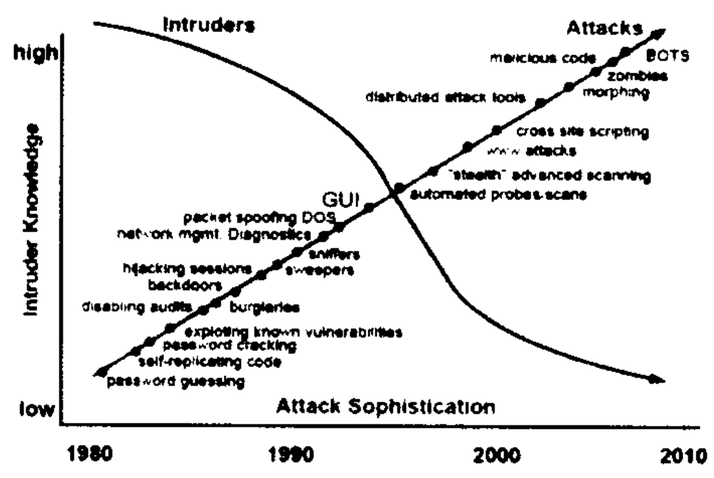






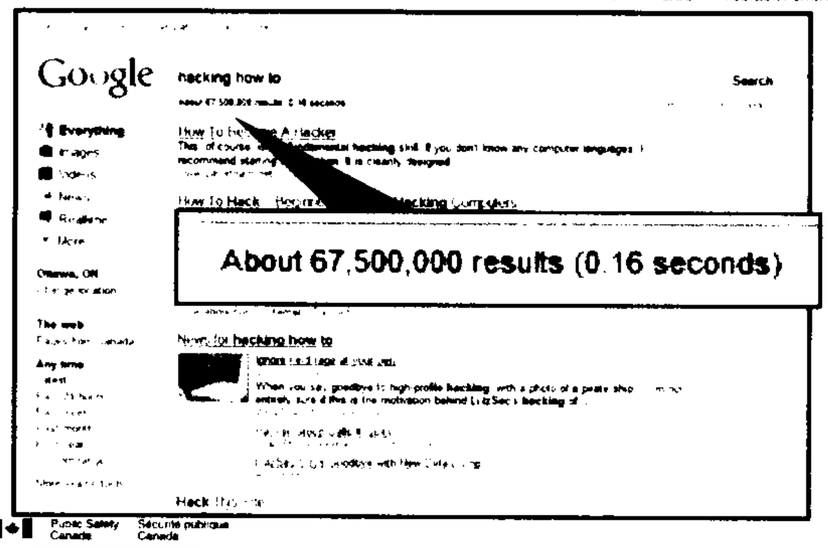
The Cyber Threat

Intruder Knowledge vs. Sophistication of Tools



Public Safety Canada / Sécurité publique Canada

Information Proliferation

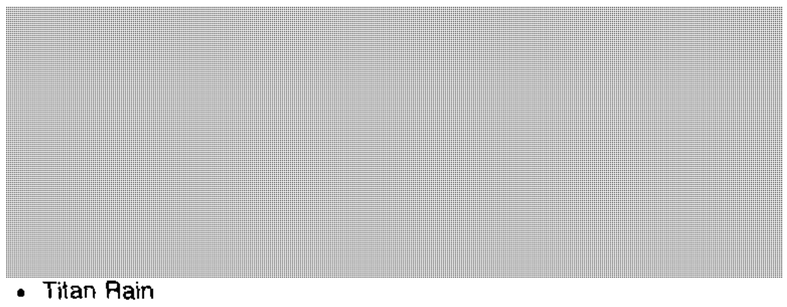


Public Safety Canada / Sécurité publique Canada

Foreign States
Hostile Foreign Intelligence

SAFE & RESILIENT CANADA

- "...pose a growing threat to national security as they target government, business, educational and private computer systems." *CSIS 2009-2010 Public Report*

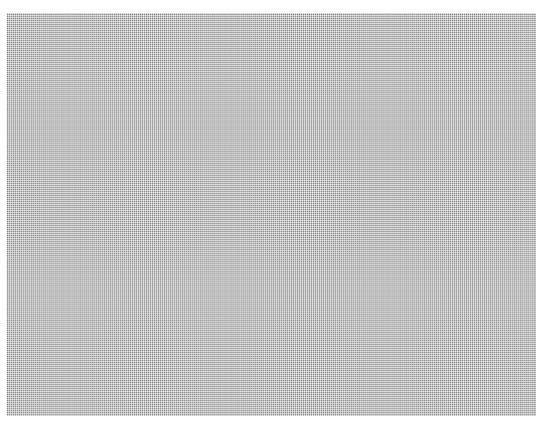


- Titan Rain

Public Safety Canada / Sécurité publique Canada

Foreign Collection Interests in Canada

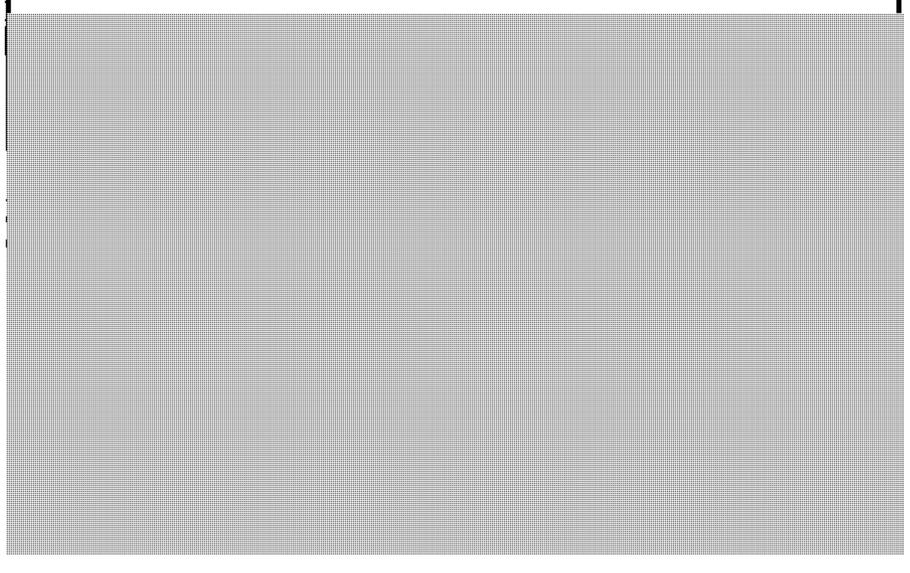
SAFE & RESILIENT CANADA



Public Safety Canada / Sécurité publique Canada

Cyber Capability: Global Operational Reach

SAFE & RESILIENT CANADA



Terrorist Groups

SAFE RESILIENT CANADA

- There are 36 terrorist groups listed on Canada's list of named entities

- What do Terrorist use the Internet for:
  - Propaganda
  - Fund Raising
  - Covert Communications
  - Open Web Forums
  - Targeting:

Public Safety Canada / Sécurité publique Canada

Hacker Groups

SAFE RESILIENT CANADA

- Many attacks originate from script kiddies
- Emergence of "Elite-Hacker"
  - Custom code, cutting edge, AV defeating, anti-forensics
- Hacker-for-hire seen with increased frequency
- Political hacktivism increasing

Public Safety Canada / Sécurité publique Canada

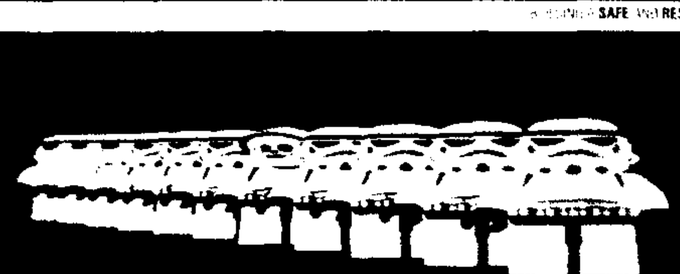
Criminal Element

SAFE RESILIENT CANADA

- Global electronic related crime has now surpassed drugs as the single largest profit generator for organized crime
- Increasing organization and complexity
  - Some out-pacing security community response efforts
- They do it for the money
- Moving towards mobile phone hacking
- Depending upon the immediate need they are:
  - Valid business organizations
  - Cyber criminals
  - Foreign intelligence agents

Public Safety Canada / Sécurité publique Canada

Insider Threat



Public Safety Canada / Sécurité publique Canada

Internal Threat

- Categories for classifying insider as threat agents, range from:
  - Explorers
  - Good Samaritans (accidental, non-malicious)
  - Hackers
  - Machiavellians
  - Avengers
  - Career thieves
  - Moles
- System administrators and users with full network privileges are always of concern as a potential insider threat

Public Safety Canada / Sécurité publique Canada

s.15(1) - Int'l

s.15(1) - Subv

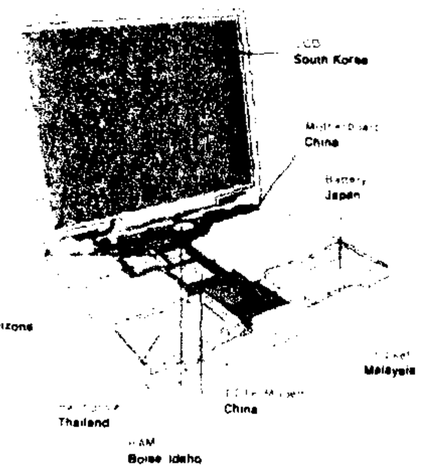
Internal Threat

- Insider threat incidents have had the greatest impact
- A smart insider is virtually impossible to catch

Public Safety Canada / Sécurité publique Canada

Supply Chain Issues

SAFE RESILIENT CANADA



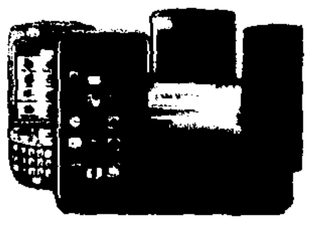
Origin of a 2007 Dell Laptop's components

Public Safety Canada / Sécurité publique Canada

What's Next...

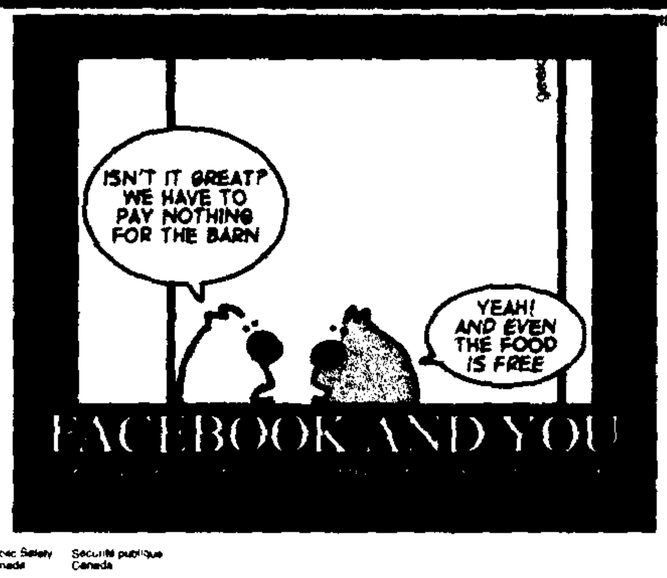
SAFE RESILIENT CANADA

- BYOD
- Mobile devices
- Cloud computing



Public Safety Canada / Sécurité publique Canada

RESILIENT CANADA



Public Safety Canada / Sécurité publique Canada

2012/04/17

UNCLASSIFIED

EUROPEAN UNION'S UPDATED DATA PROTECTION LEGISLATION

ISSUE

On January 25, 2012, the European Commission issued a proposal for a *General Data Protection Regulation* (the "Regulation") that seeks to offer protection to individuals with regard to the processing and movement of personal data (**TAB A**). The proposed legal framework also includes a Directive containing rules for the processing of personal data by law enforcement authorities for the purposes of detection, investigation, prevention or prosecution of criminal offences. The proposed Regulation is the most significant potential change to European data protection law since the adoption of the European Union (EU) *Data Protection Directive 95/46/EC* ("Directive 95/46") in 1998.

BACKGROUND

On November 4, 2010, the EU Directorate General Internal Market of the European Commission (which had jurisdiction over data protection policy at that time) published a report that concluded that while the principles of Directive 95/46 were still valid, the Directive was not sufficient given the evolution of technology. On November 29, 2011, and following extensive consultations with a variety of stakeholder groups, the Directorate General Justice (now responsible for data protection policy) circulated a draft version of the current proposed Regulation. Numerous changes and improvements were made to the proposal, which was issued on January 25, 2012, by the European Commission's Vice President for Justice.

ANALYSIS

Scope and jurisdiction

The territorial scope of the former and proposed EU data protection laws is limited to the protection of individuals residing in the EU, and applies to the processing of personal data by an establishment physically located in the EU. The current proposed Regulation, however, makes several significant jurisdictional changes with a view to holding more non-EU-based companies offering services over the Internet accountable to EU law. The Regulation proposes that data controllers not established in the EU may be subject to EU law when their processing activities are related to: the offering of goods and services to EU residents; or to the monitoring of the behaviour of EU residents through the creation of behavioural "profiles" by non-EU companies.

Consent, lawfulness and principles for data processing

With regard to data processing, the basic principles of Directive 95/46 remain in the proposed Regulation, with the addition of clearer language regarding minimizing the amount of data collected by a company. The Regulation states that data processing may only be undertaken on the basis of EU law or EU member state law, underscoring that the law of a non-EU country may not serve as the legal basis for processing the data of an EU resident.

With regard to consent, the Regulation states that it is the responsibility of the data processor to prove that an individual has consented to the processing of their personal data. Companies would henceforth need to develop mechanisms to obtain explicit consent from their clients.

Rights of the data subject

The "right to be forgotten and to erasure" is one of the more contentious provisions within the proposed Regulation. It is an extension of a provision under Directive 95/46 that allows a user to have their data erased, and would now place responsibility on data controllers to inform third parties processing the data that the user has requested that their data be erased. Google Inc. has argued that this provision makes unreasonable demands on search engines and hosting platforms, such as YouTube and Facebook, to delete content. Google Inc. argues that users that upload information online should ultimately be the ones responsible for deleting it; however, the Office of the Justice Commissioner draws a distinction between such services and the platforms that simply host content, such as Dropbox.

Additionally, a new right to data portability would allow individuals to change online services more easily by giving them the right to obtain a copy of their data from the online service provider; however, the feasibility of applying this provision in practice has been criticized. There may be little that European law enforcement and other supervisory bodies can do to enforce the law outside of the EU unless effective cross-border enforcement mechanisms are in place. Therefore, in reality, non-EU data controllers' compliance with the Regulation may be voluntary.

Duties of data controllers

The proposed Regulation contains a number of provisions concerning data security, including a requirement for general data breach notification, whereby data controllers would be responsible for informing users of all personal data breaches. The United Kingdom's Office of the Information Commissioner has criticized this provision by stating that it is unrealistic that companies should have to report all personal data breaches, arguing that notification should only have to be issued after certain triggers, such as financial loss.

Penalities

The proposed Regulation outlines a new regime of penalties and administrative fines for any intentional or negligent violation of certain provisions of the Regulation. Under Directive 95/46, the determination of the dollar amount of fines and administrative fees was left to the discretion and decision of EU member states. In the proposed Regulation, the fines would range from 0.5 percent to 2 percent of a company's annual worldwide revenue. Essentially, the proposed Regulation seeks to elevate the importance of data protection to the same level as other key corporate issues such as competition laws and money laundering requirements.

s.21(1)(a)

s.21(1)(b)

CONSIDERATIONS

[redacted]

In Canada, the Minister of Industry introduced Bill C-12, the *Safeguarding Canadians' Personal Information Act*, on September 29, 2011. Bill C-12 would add mandatory breach notification to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Similar to the EU proposal, the Bill would oblige an organization seeking consent to share an individual's personal information to reasonably describe the implications of consent to the user. [redacted]

s.21(1)(a)

s.21(1)(b)

[redacted] On April 12, 2011, Senators John Kerry and John McCain introduced a privacy bill that would require companies to notify consumers in clear language when their data is being collected and would oblige those companies to keep that data safe. That bill, and bills proposed by other Senators, has not progressed in the U.S. Senate due to businesses, consumer groups and privacy advocates arguing that it would potentially damage an already-fragile U.S. economy.

[redacted]

CONCLUSION

The proposed Regulation represents a strong effort by the EU to modernize data protection law by increasing the effectiveness and efficiency of its legal framework to strengthen the protection of fundamental privacy-related rights.

The EU proposal is being passed to the European Parliament and EU member states for discussion and approval in the coming months. It would take effect two years after being adopted.

Public Safety Canada will be added to the EU Embassy distribution list regarding development in data protection and privacy policy as follow-up to the recent meeting between the Senior Assistant Deputy Minister of National Security, Public Safety Canada, and the European Network and Information Security Agency.

Prepared by: Melanie Mohammed
Approved by: Mark Matz

Enclosure: (1)

EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

This explanatory memorandum presents in further detail the proposed new legal framework for the protection of personal data in the EU as set out in Communication COM (2012) 9 final[1]. The proposed new legal framework consists of two legislative proposals:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and

- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data[2].

This explanatory memorandum concerns the legislative proposal for a General Data Protection Regulation.

The centrepiece of existing EU legislation on personal data protection, Directive 95/46/EC[3], was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. It was complemented by Framework Decision 2008/977/JHA as a general instrument at Union level for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters[4].

Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life.

Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services. This risks slowing down the development of innovative uses of new technologies. Personal data protection therefore plays

---

1 "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century" COM(2012) 9 final.

2 COM(2012) 10 final.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p.31.

4 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60 ('Framework Decision').

a central role in the Digital Agenda for Europe[5], and more generally in the Europe 2020 Strategy[6].

Article 16(1) of Treaty on the Functioning of the European Union (TFEU), as introduced by the Lisbon Treaty, establishes the principle that everyone has the right to the protection of personal data concerning him or her. Moreover, with Article 16(2) TFEU, the Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data. Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right.

The European Council invited the Commission to evaluate the functioning of EU instruments on data protection and to present, where necessary, further legislative and non-legislative initiatives[7]. In its resolution on the Stockholm Programme, the European Parliament[8] welcomed a comprehensive data protection scheme in the EU and among others called for the revision of the Framework Decision. The Commission stressed in its Action Plan implementing the Stockholm Programme[9] the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies.

In its Communication on "A comprehensive approach on personal data protection in the European Union"[10], the Commission concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection.

The current framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity[11]. This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.

2. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENT

This initiative is the result of extensive consultations with all major stakeholders on a review of the current legal framework for the protection of personal data, which lasted for more than two years and included a high level conference in May 2009[12] and two phases of public consultation:

---

5 COM(2010)245 final.

6 COM(2010)2020 final.

7 "The Stockholm Programme — An open and secure Europe serving and protecting citizens", OJ C 115, 4.5.2010, p.1.

8 Resolution of the European Parliament on the on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme adopted 25 November 2009 (P7_TA(2009)0090).

9 COM(2010)171 final.

10 COM(2010)609 final.

11 Special Eurobarometer (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf .

12 http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm.

- From 9 July to 31 December 2009, the *Consultation on the legal framework for the fundamental right to the protection of personal data*. The Commission received 168 responses, 127 from individuals, business organisations and associations and 12 from public authorities.[13]

- From 4 November 2010 to 15 January 2011, the *Consultation on the Commission's comprehensive approach on personal data protection in the European Union*. The Commission received 305 responses, of which 54 from citizens, 31 from public authorities and 220 from private organisations, in particular business associations and non-governmental organisations.[14]

Targeted consultations were also conducted with key stakeholders; specific events were organised in June and July 2010 with Member State authorities and with private sector stakeholders, as well as privacy, data protection and consumers' organisations[15]. In November 2010, European Commission's Vice-President Reding organised a roundtable on the data protection reform. On 28 January 2011 (Data Protection Day), the European Commission and the Council of Europe co-organised a high level conference to discuss issues related to the reform of the EU legal framework as well as to the need for common data protection standards worldwide[16]. Two conferences on data protection were hosted by the Hungarian and Polish Presidencies of the Council on 16-17 June 2011 and on 21 September 2011 respectively.

Dedicated workshops and seminars on specific issues were held throughout 2011. In January ENISA[17] organised a workshop on data breach notifications in Europe[18]. In February, the Commission convened a workshop with Member States' authorities to discuss data protection issues in the area of police co-operation and judicial co-operation in criminal matters, including the implementation of the Framework Decision, and the Fundamental Rights Agency held a stakeholder consultation meeting on "Data Protection and Privacy". A discussion on key issues of the reform was held on 13 July 2011 with national Data Protection Authorities. EU citizens were consulted through a Eurobarometer survey held in November-December 2010[19]. A number of studies were also launched.[20] The "Article 29 Working Party"[21] provided several opinions and useful input to the Commission[22]. The European Data

---

13 The non-confidential contributions can be consulted on the Commission's website: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

14 The non-confidential contributions can be consulted on the Commission's website: http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

15 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm.

16 http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_en.asp.

17 European Network and Information Security Agency, dealing with security issues related to communication networks and information systems.

18 See http://www.enisa.europa.eu/act/it/data-breach-notification.

19 Special Eurobarometer (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

20 See the *Study on the economic benefits of privacy enhancing technologies* and the *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments,* January 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf)..

21 The Working Party was set up in 1996 (by Article 29 of Directive 95/46/EC) with advisory status and composed of representatives of national Data Protection Supervisory Authorities (DPAs), the European Data Protection Supervisor (EDPS) and the Commission. For more information on its activities see http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

Protection Supervisor also issued a comprehensive opinion on the issues raised in the Commission's November 2010 Communication[23].

The European Parliament approved by its resolution of 6 July 2011 a report that supported the Commission's approach to reforming the data protection framework.[24] The Council of the European Union adopted conclusions on 24 February 2011 in which it broadly supports the Commission's intention to reform the data protection framework and agrees with many elements of the Commission's approach. The European Economic and Social Committee likewise supported the Commission's aim to ensure a more consistent application of EU data [25]protection rules across all Member States an appropriate revision of Directive 95/46/EC.[26]

During the consultations on the comprehensive approach, a large majority of stakeholders agreed that the general principles remain valid but that there is a need to adapt the current framework in order to better respond to challenges posed by the rapid development of new technologies (particularly online) and increasing globalisation, while maintaining the technological neutrality of the legal framework. Heavy criticism has been expressed regarding the current fragmentation of personal data protection in the Union, in particular by economic stakeholders who asked for increased legal certainty and harmonisation of the rules on the protection of personal data. The complexity of the rules on international transfers of personal data is considered as constituting a substantial impediment to their operations as they regularly need to transfer personal data from the EU to other parts of the world.

In line with its "Better Regulation" policy, the Commission conducted an impact assessment of policy alternatives. The impact assessment was based on the three policy objectives of improving the internal market dimension of data protection, making the exercise of data protection rights by individuals more effective and creating a comprehensive and coherent framework covering all areas of Union competence, including police co-operation and judicial co-operation in criminal matters. Three policy options of different degrees of intervention were assessed: the first option consisted of minimal legislative amendments and the use of interpretative Communications and policy support measures such as funding programmes and technical tools; the second option comprised a set of legislative provisions addressing each of the issues identified in the analysis and the third option was the centralisation of data protection at EU level through precise and detailed rules for all sectors and the establishment of an EU agency for monitoring and enforcement of the provisions.

According to the Commission's established methodology, each policy option was assessed, with the help of an Interservice steering group, against its effectiveness to achieve the policy objectives, its economic impact on stakeholders (including on the budget of the EU

---

22 See in particular the following opinions: on the "Future of Privacy" (2009, WP 168); on the concepts of "controller" and "processor" (1/2010, WP 169); on online behavioural advertising (2/2010, WP 171); on the principle of accountability (3/2010, WP 173); on applicable law (8/2010, WP 179); and on consent (15/2011, WP 187). Upon the Commission's request, it adopted also the three following Advice Papers: on notifications, on sensitive data and on the practical implementation of Article 28(6) of the Data Protection Directive. They can all be accessed at: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

23 Available on the EDPS website: http://www.edps.europa.eu/EDPSWEB.

24 EP resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244 (rapporteur: MEP Axel Voss (EPP/DE).

25 SEC(2012)72.

26 CESE 999/2011.

institutions), its social impact and effect on fundamental rights. Environmental impacts were not observed. The analysis of the overall impact led to the development of the preferred policy option which is based on the second option with some elements from the other two options and incorporated in the present proposal. According to the impact assessment, its implementation will lead *inter alia* to considerable improvements regarding legal certainty for data controllers and citizens, reduction of administrative burden, consistency of data protection enforcement in the Union, the effective possibility of individuals to exercise their data protection rights to the protection of personal data within the EU and the efficiency of data protection supervision and enforcement. Implementation of the preferred policy options are also expected to contribute to the Commission's objective of simplification and reduction of administrative burden and to the objectives of the Digital Agenda for Europe, the Stockholm Action Plan and the Europe 2020 strategy.

The Impact Assessment Board delivered an opinion on the draft impact assessment on 9 September 2011. Following the IAB opinion, the following changes were made to the impact assessment:

- The objectives of the current legal framework (to what extent they were achieved, and to what extent they were not), as well as the objectives of the envisaged reform were clarified;

- More evidence and additional explanations/clarification were added to the problems' definition section;

- A section on proportionality was added;

- All calculations and estimations related to administrative burden in the baseline scenario and in the preferred option have been entirely reviewed and revised, and the relation between the costs of notifications and the overall fragmentation costs has been clarified (including Annex 10);

- Impacts on micro, small and medium enterprises, particularly of data protection officers and data protection impact assessments have been better specified.

The impact assessment report and an executive summary are published with the proposals.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. Legal Basis

This proposal is based on Article 16 TFEU, which is the new legal basis for the adoption of data protection rules introduced by the Lisbon Treaty. This provision allows the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Member States when carrying out activities which fall within the scope of Union law. It also allows the adoption of rules relating to the free movement of personal data, including personal data processed by Member States or private parties.

A Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection

of fundamental rights of individuals and contributing to the functioning of the Internal Market.

The reference to Article 114(1) TFEU is only necessary for amending Directive 2002/58/EC to the extent that that Directive also provides for the protection of the legitimate interests of subscribers who are legal persons.

3.2. Subsidiarity and proportionality

According to the principle of subsidiarity (Article 5(3) TEU), action at Union level shall be taken only if and in so far as the objectives envisaged cannot be achieved sufficiently by Member States, but can rather, by reason of the scale or effects of the proposed action, be better achieved by the Union. In the light of the problems outlined above, the analysis of subsidiarity indicates the necessity of EU-level action on the following grounds:

- The right to the protection of personal data, enshrined in Article 8 of the Charter of Fundamental Rights, requires the same level of data protection throughout the Union. The absence of common EU rules would create the risk of different levels of protection in the Member States and create restrictions on cross-border flows of personal data between Member States with different standards.

- Personal data are transferred across national boundaries, both internal and external borders, at rapidly increasing rates. In addition, there are practical challenges to enforcing data protection legislation and a need for co-operation between Member States and their authorities, which needs to be organised at EU level to ensure unity of application of Union law. The EU is also best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries.

- Member States cannot alone reduce the problems in the current situation, particularly those due to the fragmentation in national legislations. Thus, there is a specific need to establish a harmonised and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection for all individuals across the EU.

- The proposed EU legislative actions will be more effective than similar actions at the level of Member States because of the nature and scale of the problems, which are not confined to the level of one or several Member States.

The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal.

3.3. Summary of fundamental rights issues

The right to protection of personal data is established by Article 8 of the Charter and Article 16 TFEU and in Article 8 of the ECHR. As underlined by the Court of Justice of the EU[27], the right to the protection of personal data is not an absolute right, but must be considered in

---

[27] Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

relation to its function in society[28]. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by Article 1(1) of Directive 95/46/EC which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

Other potentially affected fundamental rights enshrined in the Charter are the following: freedom of expression (Article 11 of the Charter); freedom to conduct a business (Article 16); the right to property and in particular the protection of intellectual property (Article 17(2)); the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24); the right to a high level of human health care (Article 35); the right of access to documents (Article 42); the right to an effective remedy and a fair trial (Article 47).

3.4. Detailed explanation of the proposal

3.4.1. CHAPTER I - GENERAL PROVISIONS

Article 1 defines subject matter of the Regulation, and, as in Article 1 of Directive 95/46/EC, sets out the two objectives of the Regulation.

Article 2 determines the material scope of the Regulation.

Article 3 determines the territorial scope of the Regulation.

Article 4 contains definitions of terms used in the Regulation. While some definitions are taken over from Directive 95/46/EC, others are modified, complemented with additional elements, or newly introduced ('personal data breach' based on Article 2(h) of the e-privacy Directive 2002/58/EC[29] as amended by Directive 2009/136/EC[30], 'genetic data', 'biometric data', 'data concerning health', 'main establishment', 'representative', 'enterprise', 'group of undertakings', 'binding corporate rules', and of a 'child' which is based on the United Nation's Convention on the Rights of the Child[31], and 'supervisory authority').

---

28 In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

29 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002, p. 37.

30 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance; OJ L 337 , 18.12.2009, p. 11.

31 Adopted and opened for signature, ratification and accession by the United Nations General Assembly resolution 44/25 of 20.11.1989.

In the definition of consent, the criterion 'explicit' is added to avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent.

3.4.2. CHAPTER II - PRINCIPLES

Article 5 sets out the principles relating to personal data processing, which correspond to those in Article 6 of Directive 95/46/EC. Additional new elements are in particular the transparency principle, the clarification of the data minimisation principle and the establishment of a comprehensive responsibility and liability of the controller.

Article 6 sets out, based on Article 7 of Directive 95/46/EC, the criteria for lawful processing, which are further specified as regards the balance of interest criterion, and the compliance with legal obligations and public interest.

Article 7 clarifies the conditions for consent to be valid as a legal ground for lawful processing.

Article 8 sets out further conditions for the lawfulness of the processing of personal data of children in relation to information society services offered directly to them.

Article 9 sets out the general prohibition for processing special categories of personal data and the exceptions from this general rule, building on Article 8 of the Directive 95/46/EC.

Article 10 clarifies that the controller is not obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

3.4.3. CHAPTER III - RIGHTS OF THE DATA SUBJECT

3.4.3.1. Section 1 – Transparency and modalities

Article 11 introduces the obligation on controllers to provide transparent and easily accessible and understandable information, inspired in particular by the Madrid Resolution on international standards on the protection of personal data and privacy[32].

Article 12 obliges the controller to provide procedures and mechanism for exercising the data subject's rights, including means for electronic requests, requiring response to the data subject's request within a defined deadline, and the motivation of refusals.

Article 13 provides rights in relation to recipients, based on Article 12(c) of Directive 95/46/EC, extended to all recipients, including joint controllers and processors.

3.4.3.2. Section 2 – Information and access to data

Article 14 further specifies the controller's information obligations towards the data subject, building on Articles 10 and 11 of Directive 95/46/EC, providing additional information to the data subject, including on the storage period, the right to lodge a complaint, in relation to

---

[32] Adopted by the International Conference of Data Protection and Privacy Commissioners on 5 November 2009. Cf. also Article 13(3) of the proposal for a Regulation on a Common European Sales Law (COM(2011)635final).

international transfers and to the source from which the data are originating. It also maintains the possible derogations in Directive 95/46/EC, e.g. there will be no such obligation if the recording or disclosure are expressly provided by law. This could apply for example in proceedings by competition authorities, tax or customs administrations, or services competent for social security matters.

Article 15 provides the data subject's right of access to their personal data, building on Article 12(a) of Directive 95/46/EC and adding new elements, such as to inform the data subjects of the storage period, and of the rights to rectification and to erasure and to lodge a complaint.

3.4.3.3. Section 3 – Rectification and erasure

Article 16 sets out the data subject's right to rectification, based on Article 12(b) of Directive 95/46/EC.

Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology "blocking".

Article 18 introduces the data subject's right to data portability, i.e. to transfer data from one electronic processing system to and into another, without being prevented from doing so by the controller. As a precondition and in order to further improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format.

3.4.3.4. Section 4 – Right to object and profiling

Article 19 provides for the data subject's rights to object. It is based on Article 14 of Directive 95/46/EC, with some modifications, including as regards the burden of proof and its application to direct marketing.

Article 20 concerns the data subject's right not to be subject to a measure based on profiling. It builds on, with modifications and additional safeguards, Article 15(1) of Directive 95/46 on automated individual decisions, and takes account of the Council of Europe's recommendation on profiling[33].

3.4.3.5. Section 5 – Restrictions

Article 21 clarifies the empowerment for the Union or Member States to maintain or introduce restrictions of principles laid down in Article 5 and of the data subject's rights laid down in Articles 11 to 20 and in Article 32. This provision is based on Article 13 of Directive 95/46/EC and on the requirements stemming from the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the EU and the European Court of Human Rights.

---

33 CM/Rec (2010)13.

3.4.4. CHAPTER IV - CONTROLLER AND PROCESSOR

3.4.4.1. Section 1 – General obligations

Article 22 takes account of the debate on a "principle of accountability" and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance.

Article 23 sets out the obligations of the controller arising from the principles of data protection by design and by default.

Article 24 on joint controllers clarifies the responsibilities of joint controllers as regards their internal relationship and towards the data subject.

Article 25 obliges under certain conditions controllers not established in the Union, where the Regulation applies to their processing activities, to designate a representative in the Union.

Article 26 clarifies the position and obligation of processors, partly based on Article 17(2) of Directive 95/46/EC, and adding new elements, including that a processor who processes data beyond the controller's instructions is to be considered as a joint controller.

Article 27 on the processing under the authority of the controller and processor is based on Article 16 of Directive 95/46/EC.

Article 28 introduces the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility, instead of a general notification to the supervisory authority required by Articles 18(1) and 19 of Directive 95/46/EC.

Article 29 clarifies the obligations of the controller and the processor for the co-operation with the supervisory authority.

3.4.4.2. Section 2 – Data security

Article 30 obliges the controller and the processor to implement appropriate measures for the security of processing, based on Article 17(1) of Directive 95/46/EC, extending that obligation to processors, irrespective of the contract with the controller.

Articles 31 and 32 introduce an obligation to notify personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC.

3.4.4.3. Section 3 – Data protection impact assessment and prior authorisation

Article 33 introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations.

Article 34 concerns the cases where authorisation by, and consultation of, the supervisory authority is mandatory prior to the processing, building on the concept of prior checking in Article 20 of Directive 95/46/EC.

3.4.4.4. Section 4 – Data protection officer

Article 35 introduces a mandatory data protection officer for the public sector, and, in the private sector, for large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring. This builds on Article 18(2) of Directive 95/46/EC which provided the possibility for Member States to introduce such requirement as a surrogate of a general notification requirement.

Article 36 sets out the position of the data protection officer.

Article 37 provides the core tasks of the data protection officer.

3.4.4.5. Section 5 – Codes of conduct and certification

Article 38 concerns codes of conduct, building on the concept of Article 27(1) of Directive 95/46/EC, clarifying the content of the codes and the procedures and providing for the empowerment of the Commission to decide on the general validity of codes of conduct.

Article 39 introduces the possibility to establish certification mechanisms and data protection seals and marks.

3.4.5. CHAPTER V - TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40 spells out, as a general principle, that the compliance with the obligations in that chapter are mandatory for any transfers of personal data to third countries or international organisations, including onward transfers.

Article 41 sets out the criteria, conditions and procedures for the adoption of an adequacy decision by the Commission, based on Article 25 of Directive 95/46/EC. The criteria which shall be taken into account for the Commission's assessment of an adequate or not adequate level of protection include expressly the rule of law, judicial redress and independent supervision. The article now confirms explicitly the possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country.

Article 42 requires for transfers to third countries, where no adequacy decision has been adopted by the Commission, to adduce appropriate safeguards, in particular standard data protection clauses, binding corporate rules and contractual clauses. The possibility of making use of Commission standard data protection clauses is based on Article 26(4) of Directive 95/46/EC. As a new component, such standard data protection clauses may now also be adopted by a supervisory authority and be declared generally valid by the Commission. Binding corporate rules are now specifically mentioned in the legal text. The option of contractual clauses gives certain flexibility to the controller or processor, but is subject to prior authorisation by supervisory authorities.

Article 43 describes in further detail the conditions for transfers by way of binding corporate rules, based on the current practices and requirements of supervisory authorities.

Article 44 spells out and clarifies the derogations for a data transfer, based on the existing provisions of Article 26 of Directive 95/46/EC. This applies in particular to data transfers required and necessary for the protection of important grounds of public interest, for example

in cases of international data transfers between competition authorities, tax or customs administrations, or between services competent for social security matters or for fisheries management. In addition, a data transfer may, under limited circumstances, be justified on a legitimate interest of the controller or processor, but only after having assessed and documented the circumstances of that transfer operation.

Article 45 explicitly provides for international co-operation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries, in particular those considered offering an adequate level of protection, taking into account the Recommendation by the Organisation for Economic Co-operation and Development (OECD) on cross-border co-operation in the enforcement of laws protecting privacy of 12 June 2007.

3.4.6. CHAPTER VI - INDEPENDENT SUPERVISORY AUTHORITIES

3.4.6.1. Section 1 – Independent status

Article 46 obliges Member States to establish supervisory authorities, based on Article 28(1) of Directive 95/46/EC and enlarging the mission of the supervisory authorities to co-operation with each other and with the Commission.

Article 47 clarifies the conditions for the independence of supervisory authorities, implementing case law by the Court of Justice of the European Union[34], inspired also by Article 44 of Regulation (EC) No 45/2001[35].

Article 48 provides general conditions for the members of the supervisory authority, implementing the relevant case law[36] and inspired also by Article 42(2) to (6) of Regulation (EC) 45/2001.

Article 49 sets out rules on the establishment of the supervisory authority to be provided by the Member States by law.

Article 50 lays down professional secrecy of the members and staff of the supervisory authority and is based on Article 28(7) of Directive 95/46/EC.

3.4.6.2. Section 2 – Duties and powers

Article 51 sets out the competence of the supervisory authorities. The general rule, based on Article 28(6) of Directive 95/46/EC (competency on the territory of its own Member State), is complemented by the new competence as lead authority in case that a controller or processor is established in several Member States, to ensure unity of application ('one-stop shop'). Courts, when acting in their judicial authority, are exempted from the monitoring by the supervisory authority, but not from the application of the substantive rules on data protection.

Article 52 provides the duties of the supervisory authority, including hearing and investigating complaints and promoting the awareness of the public of risks, rules, safeguards and rights.

---

34 Court of Justice of the EU, judgment of 9.3.2010, Commission / Germany, CaseC-518/07, ECR 2010 p. I-1885.

35 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; OJ L 008 , 12/01/2001, p.1.

36 Op. cit, footnote 34.

Article 53 provides the powers of the supervisory authority, in parts building on Article 28(3) of Directive 95/46/EC and Article 47 of Regulation (EC) 45/2001, and adding some new elements, including the power to sanction administrative offences.

Article 54 obliges the supervisory authorities to draw up annual activity reports, based on Article 28(5) of Directive 95/46/EC.

3.4.7. CHAPTER VII - CO-OPERATION AND CONSISTENCY

3.4.7.1. Section 1 – Co-operation

Article 55 introduces explicit rules on mandatory mutual assistance, including consequences for non-compliance with the request of another supervisory, building on Article 28(6), second subparagraph, of Directive 95/46/EC.

Article 56 introduces rules on joint operations, inspired by Article 17 of Council Decision 2008/615/JHA[37], including a right of supervisory authorities to participate in such operations.

3.4.7.2. Section 2 – Consistency

Article 57 introduces a consistency mechanism for ensuring unity of application in relation to processing operations which may concern data subjects in several Member States.

Article 58 sets out the procedures and conditions for an opinion of the European Data Protection Board.

Article 59 concerns Commission opinions on matters dealt within the consistency mechanism, which may either reinforce the opinion of the European Data Protection Board or express a divergence with that opinion, and the draft measure of the supervisory authority. Where the matter has been raised by the European Data Protection Board under Article 58(3) it can be expected that the Commission will exercise its discretion and deliver an opinion whenever necessary.

Article 60 concerns Commission decisions requiring the competent authority to suspend its draft measure when this is necessary to ensure the correct application of this Regulation.

Article 61 provides for a possibility for the adoption of provisional measures, in an urgency procedure.

Article 62 sets out the requirements for Commission implementing acts under the consistency mechanism.

Article 63 provides the obligation to enforce measures of a supervisory authority in all Member States concerned, and sets out that the application of the consistency mechanism is a precondition for the legal validity and enforcement of the respective measure.

---

[37] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1.

3.4.7.3. Section 3 – European Data Protection Board

Article 64 establishes the European Data Protection Board, consisting of the heads of the supervisory authority of each Member State and of the European Data Protection Supervisor. The European Data Protection Board replaces the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC. It is clarified that the Commission is not a member of the European Data Protection Board, but has the right to participate in the activities and to be represented.

Article 65 underlines and clarifies the independence of the European Data Protection Board.

Article 66 describes the tasks of the European Data Protection Board, based on Article 30(1) of Directive 95/46/EC, and provides for additional elements, reflecting the increased scope of activities of the European Data Protection Board, within the Union and beyond. In order to be able to react in urgent situations, it provides the Commission with the possibility to ask for an opinion within a specific time-limit.

Article 67 requires the European Data Protection Board to report annually on its activities, building on Article 30(6) of Directive 95/46/EC.

Article 68 sets out the European Data Protection Board's decision making procedures, including the obligation to adopt rules of procedure which should extend also to operational arrangements.

Article 69 contains the provisions on the chair and on the deputy chairs of the European Data Protection Board.

Article 70 sets out the tasks of the chair.

Article 71 sets out that the secretariat of the European Data Protection Board shall be provided by the European Data Protection Supervisor, and specifies the tasks of the secretariat.

Article 72 provides for rules on the confidentiality.

3.4.8. CHAPTER VIII - REMEDIES, LIABILITY AND SANCTIONS

Article 73 provides the right of any data subject to lodge a complaint with a supervisory authority, based on Article 28(4) of Directive 95/46/EC. It specifies also the bodies, organisations or associations which may lodge a complaint on behalf of the data subject or, in case of a personal data breach, independently of a data subject's complaint.

Article 74 concerns the right of judicial remedy against a supervisory authority. It builds on the general provision of Article 28(3) of Directive 95/46/EC. It provides specifically a judicial remedy obliging the supervisory authority to act on a complaint, and clarifies the competence of the courts of the Member State where the supervisory authority is established. It provides also the possibility that the supervisory authority of the Member State in which the data subject is residing, may bring on behalf of the data subject proceedings before the courts of another Member State where the competent supervisory authority is established.

Article 75 concerns the right to a judicial remedy against a controller or processor, building on Article 22 of Directive 95/46/EC, and providing a choice to go to court in the Member

State where the defendant is established or where the data subject is residing. Where proceedings concerning the same matter are pending in the consistency mechanism, the court may suspend its proceedings, except in case of urgency.

Article 76 lays down common rules for court proceedings, including the rights of bodies, organisations or associations to represent data subjects before the courts, the right of supervisory authorities to engage in legal proceedings and the information of the courts on parallel proceedings in another Member State, and the possibility for the courts to suspend in such case the proceedings.[38] There is an obligation on Member States to ensure rapid court actions.[39]

Article 77 sets out the right to compensation and liability. It builds on Article 23 of Directive 95/46/EC, extends this right to damages caused by processors and clarifies the liability of joint controllers and joint processors.

Article 78 obliges Member States to lay down rules on penalties, to sanction infringements of the Regulation, and to ensure their implementation.

Article 79 obliges each supervisory authority to sanction the administrative offences listed in the catalogues set out in this provision, imposing fines up to maximum amounts, with due regard to circumstances of each individual case.

3.4.9. CHAPTER IX - PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80 obliges Member States to adopt exemptions and derogations from specific provisions of the Regulation where necessary to reconcile the right to the protection of personal data with the right of freedom of expression. It is based on Article 9 of Directive 95/46/EC, as interpreted by the Court of Justice of the EU.[40]

Article 81 obliges Member States, further to the conditions for special categories of data, to ensure specific safeguards for processing for health purposes.

Article 82 provides an empowerment for Member States to adopt specific laws for processing personal data in the employment context.

Article 83 sets out specific conditions for processing personal data for historical, statistical and scientific research purposes.

---

38 Building on Article 5(1) of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, OJ L 328, 15/12/2009, p. 42; and Article 13(1) of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 04.01.2003, p.1.

39 Building on Article 18(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1.

40 Cf. for the interpretation, e.g. Court of Justice of the EU, judgment of 16 December 2008, Satakunnan Markkinapörssi and Satamedia (C-73/07, ECR 2008 p. I-9831).

Article 84 empowers Member States to adopt specific rules on the access of supervisory authorities to personal data and to premises, where controllers are subject to obligations of secrecy.

Article 85 allows in the light of Article 17 of the Treaty on the Functioning of the European Union for the continuous application of existing comprehensive data protection rules of churches if brought in line with this Regulation.

3.4.10. CHAPTER X - DELEGATED ACTS AND IMPLEMENTING ACTS

Article 86 contains the standard provisions for the exercise of the delegations in line with Article 290 TFEU. This allows the legislator to delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act (quasi-legislative acts).

Article 87 contains the provision for the Committee procedure needed for conferring implementing powers on the Commission in the cases where in accordance with Article 291 TFEU uniform conditions for implementing legally binding acts of the Union are needed. The examination procedure applies.

3.4.11. CHAPTER XI - FINAL PROVISIONS

Article 88 repeals Directive 95/46/EC.

Article 89 clarifies the relationship to, and amends, the e-privacy Directive 2002/58/EC.

Article 90 obliges the Commission to evaluate the Regulation and submit related reports.

Article 91 sets out the date of the entry into force of the Regulation and a transitional phase as regards the date of its application.

4. BUDGETARY IMPLICATION

The specific budgetary implications of the proposal relate to the tasks allocated to the European Data Protection Supervisor as specified in the legislative financial statements accompanying this proposal. These implications require reprogramming of Heading 5 of the Financial Perspective.

The proposal has no implications on operational expenditure.

The legislative financial statement accompanying this proposal for a Regulation covers the budgetary impacts for the Regulation itself and for the Directive on police and justice data protection.

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) and Article 114(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee[41],

After consulting the European Data Protection Supervisor[42],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.

(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.

---

41 OJ C , , p. .

42 OJ C , , p. .

(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[43] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.

(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.

(6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.

(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules

---

[43] OJ L 281, 23.11.1995, p. 31.

for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.

(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.

(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.

(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.

(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions,

bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001[44], or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. The exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.

(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY).

(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation.

(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.

(21) In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

---

[44] OJ L 8, 12.1.2001, p. 1.

(22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.

(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore

no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.

(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.

(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.

(30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.

(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.

(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.

(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.

(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.

(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the

principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.

(41) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.

(43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.

(44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. In case of a request for access, the controller should be entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks.

(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.

(47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.

(50) However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

(51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

(52) The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.

(53) Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of

freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.

(56) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

(57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked..

(58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.

(59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data

subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation.

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.

(65) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be

protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In

such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(73) Data protection impact assessments should be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.

(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.

(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently.

(76) Associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors.

(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.

(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.

(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.

(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.

(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.

(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority.

(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

(87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences.

(88) Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. . Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.

(91) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory

authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.

(92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.

(94) Each supervisory authority should be provided with the adequate financial and human resources, premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.

(95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.

(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.

(98) The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment.

(99) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.

(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.

(101) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.

(103) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.

(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.

(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, , or to the monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a simple majority of its

members so decides or if so requested by any supervisory authority or the Commission.

(107) In order to ensure compliance with this Regulation, the Commission may adopt an opinion on this matter, or a decision, requiring the supervisory authority to suspend its draft measure.

(108) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

(109) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.

(110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

(111) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.

(113) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established.

(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of data subjects in relation to

the protection of their data to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.

(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.

(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority acting in the exercise of its public powers.

(117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.

(118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure.

(119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.

(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.

(121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be

adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

(122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.

(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.

(124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the processing of personal data in the employment sector.

(125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.

(126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take

into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area.

(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.

(128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation. Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.

(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to

the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[45]. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(131) The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;, the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.

(132) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.

(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on

---

45 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13.

European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force.

(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.

(136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[46].

(137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[47].

(138) As regards Liechtenstein, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[48].

(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the

---

46 OJ L 176, 10.7.1999, p. 36.
47 OJ L 53, 27.2.2008, p. 52.
48 OJ L 160 of 18.6.2011, p. 19.

freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.

HAVE ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Article 2
Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;

(b) by the Union institutions, bodies, offices and agencies;

(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;

(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;

(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3
Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

(a) the offering of goods or services to such data subjects in the Union; or

(b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Article 4
Definitions

For the purposes of this Regulation:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information relating to a data subject;

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or

the specific criteria for his nomination may be designated by Union law or by Member State law;

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;

(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;

(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;

(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the

Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(18) 'child' means any person below the age of 18 years;

(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.

CHAPTER II
PRINCIPLES

Article 5
Principles relating to personal data processing

Personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;

(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

Article 6
Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

Article 7
Conditions for consent

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

Article 8
Processing of personal data of a child

1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 9
Processing of special categories of personal data

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.

2. Paragraph 1 shall not apply where:

(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or

(e) the processing relates to personal data which are manifestly made public by the data subject; or

(f) processing is necessary for the establishment, exercise or defence of legal claims; or

(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or

(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or

(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or

(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.

Article 10
Processing not allowing identification

If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

SECTION 1
TRANSPARENCY AND MODALITIES

Article 11
Transparent information and communication

1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

Article 12
Procedures and mechanisms for exercising the rights of the data subject

1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.

6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 13
Rights in relation to recipients

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

SECTION 2
INFORMATION AND ACCESS TO DATA

Article 14
Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

   (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;

   (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

   (c) the period for which the personal data will be stored;

   (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

   (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(f) the recipients or categories of recipients of the personal data;

(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) at the time when the personal data are obtained from the data subject; or

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further

information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 15

Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

   (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;

   (d) the period for which the personal data will be stored;

   (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

   (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

   (g) communication of the personal data undergoing processing and of any available information as to their source;

   (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3
RECTIFICATION AND ERASURE

Article 16
Right to rectification

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

Article 17
Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

   (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

   (c) the data subject objects to the processing of personal data pursuant to Article 19;

   (d) the processing of the data does not comply with this Regulation for other reasons.

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

(b) for reasons of public interest in the area of public health in accordance with Article 81;

(c) for historical, statistical and scientific research purposes in accordance with Article 83;

(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;

(e) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall restrict processing of personal data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;

(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;

(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

Article 18
Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 4
RIGHT TO OBJECT AND PROFILING

Article 19
Right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

Article 20
Measures based on profiling

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

   (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

   (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

   (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

SECTION 5
RESTRICTIONS

Article 21
Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(a) public security;

(b) the prevention, investigation, detection and prosecution of criminal offences;

(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);

(f) the protection of the data subject or the rights and freedoms of others.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 22
Responsibility of the controller

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include:

(a) keeping the documentation pursuant to Article 28;

(b) implementing the data security requirements laid down in Article 30;

(c) performing a data protection impact assessment pursuant to Article 33;

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e) designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

Article 23
Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 24
Joint controllers

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Article 25
Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. This obligation shall not apply to:

(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

(b) an enterprise employing fewer than 250 persons; or

(c) a public authority or body; or

(d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Article 26
Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;

(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

Article 27
Processing under the authority of the controller and processor

The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

Article 28
Documentation

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

2. The documentation shall contain at least the following information:

(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

(b) the name and contact details of the data protection officer, if any;

(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(d) a description of categories of data subjects and of the categories of personal data relating to them;

(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

(g) a general indication of the time limits for erasure of the different categories of data;

(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:

(a) a natural person processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 29

Co-operation with the supervisory authority

1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

SECTION 2
DATA SECURITY

Article 30
Security of processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

   (a) prevent any unauthorised access to personal data;

   (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

   (c) ensure the verification of the lawfulness of processing operations.

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 31
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

3. The notification referred to in paragraph 1 must at least:

(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

(d) describe the consequences of the personal data breach;

(e) describe the measures proposed or taken by the controller to address the personal data breach.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 32

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such

technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 3
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION

Article 33
Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The following processing operations in particular present specific risks referred to in paragraph 1:

(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;

(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;

(d) personal data in large scale filing systems on children, genetic data or biometric data;

(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 34

Prior authorisation and prior consultation

1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

SECTION 4
DATA PROTECTION OFFICER

Article 35
Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

   (a) the processing is carried out by a public authority or body; or

   (b) the processing is carried out by an enterprise employing 250 persons or more; or

   (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

Article 36

Position of the data protection officer

1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

   (a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

   (b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;

   (c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;

   (d) to ensure that the documentation referred to in Article 28 is maintained;

   (e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 38
Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) fair and transparent data processing;

(b) the collection of data;

(c) the information of the public and of data subjects;

(d) requests of data subjects in exercise of their rights;

(e) information and protection of children;

(f) transfer of data to third countries or international organisations;

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend

existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Article 39
Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40
General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

Article 41
Transfers with an adequacy decision

1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

   (a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

   (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

   (c) the international commitments the third country or international organisation in question has entered into.

3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).

6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.

8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.

Article 42

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

   (a) binding corporate rules in accordance with Article 43; or

   (b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

Article 43

Transfers by way of binding corporate rules

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:

(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;

(b) expressly confer enforceable rights on data subjects;

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify:

(a) the structure and contact details of the group of undertakings and its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;

(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;

(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 44
Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important grounds of public interest; or

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the

transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.

4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

Article 45

International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

   (a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;

   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

   (c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

   (d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in

particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 46
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 47
Independence

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to

be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.

6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.

7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.

Article 48

General conditions for the members of the supervisory authority

1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.

4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.

5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.

Article 49

Rules on the establishment of the supervisory authority

Each Member State shall provide by law within the limits of this Regulation:

(a) the establishment and status of the supervisory authority;

(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;

(c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office;

(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period

where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether the members of the supervisory authority shall be eligible for reappointment;

(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;

(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

Article 50
Professional secrecy

The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

SECTION 2
DUTIES AND POWERS

Article 51
Competence

1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.

2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 52
Duties

1. The supervisory authority shall:

(a) monitor and ensure the application of this Regulation;

(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;

(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;

(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(g) authorise and be consulted on the processing operations referred to in Article 34;

(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);

(i) approve binding corporate rules pursuant to Article 43;

(j) participate in the activities of the European Data Protection Board.

2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.

5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.

6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.

Article 53
Powers

1. Each supervisory authority shall have the power:

(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;

(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;

(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;

(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;

(e) to warn or admonish the controller or the processor;

(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;

(g) to impose a temporary or definitive ban on processing;

(h) to suspend data flows to a recipient in a third country or to an international organisation;

(i) to issue opinions on any issue related to the protection of personal data;

(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:

(a) access to all personal data and to all information necessary for the performance of its duties;

(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.

The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.

3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

Article 54
Activity report

Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.

CHAPTER VII
CO-OPERATION AND CONSISTENCY

SECTION 1
CO-OPERATION

Article 55
Mutual assistance

1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations.

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.

3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.

4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

   (a) it is not competent for the request; or

   (b) compliance with the request would be incompatible with the provisions of this Regulation.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.

6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.

7. No fee shall be charged for any action taken following a request for mutual assistance.

8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.

9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 56
Joint operations of supervisory authorities

1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.

2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay.

3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding

supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.

4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.

5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).

6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.

SECTION 2
CONSISTENCY

Article 57
Consistency mechanism

For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.

Article 58
Opinion by the European Data Protection Board

1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

   (a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or

   (b) may substantially affect the free movement of personal data within the Union; or

   (c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or

(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

(f) aims to approve binding corporate rules within the meaning of Article 43.

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.

5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.

6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.

8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

Article 59
Opinion by the Commission

1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to

ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.

2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.

3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.

4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

Article 60
Suspension of a draft measure

1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:

   (a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or

   (b) adopt a measure pursuant to point (a) of Article 62(1).

2. The Commission shall specify the duration of the suspension which shall not exceed 12 months.

3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.

Article 61
Urgency procedure

1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.

3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.

4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Article 62
Implementing acts

1. The Commission may adopt implementing acts for:

(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;

(b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity;

(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;

(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.

3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.

Article 63
Enforcement

1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.

2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 64
European Data Protection Board

1. A European Data Protection Board is hereby set up.

2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.

4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

Article 65
Independence

1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

Article 66
Tasks of the European Data Protection Board

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

Article 67
Reports

1. The European Data Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries.

   The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.

Article 68
Procedure

1. The European Data Protection Board shall take decisions by a simple majority of its members.

2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.

Article 69
Chair

1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.

2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.

Article 70
Tasks of the chair

1. The chair shall have the following tasks:

   (a) to convene the meetings of the European Data Protection Board and prepare its agenda;

   (b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.

2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.

Article 71
Secretariat

1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat.

2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair.

3. The secretariat shall be responsible in particular for:

   (a) the day-to-day business of the European Data Protection Board;

(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;

(c) the use of electronic means for the internal and external communication;

(d) the translation of relevant information;

(e) the preparation and follow-up of the meetings of the European Data Protection Board;

(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.

Article 72
Confidentiality

1. The discussions of the European Data Protection Board shall be confidential.

2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.

3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.

CHAPTER VIII
REMEDIES, LIABILITY AND SANCTIONS

Article 73
Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.

2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.

3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

Article 74
Right to a judicial remedy against a supervisory authority

1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.

2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.

5. The Member States shall enforce final decisions by the courts referred to in this Article.

Article 75
Right to a judicial remedy against a controller or processor

1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.

3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.

4. The Member States shall enforce final decisions by the courts referred to in this Article.

Article 76
Common rules for court proceedings

1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.

2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.

3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.

4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.

5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

Article 77
Right to compensation and liability

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.

2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.

3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

Article 78
Penalties

1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the

obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.

2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 79
Administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.

3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:

(a) a natural person is processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.

4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);

(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).

5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;

(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;

(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;

(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;

(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;

(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);

(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.

6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;

(b) processes special categories of data in violation of Articles 9 and 81;

(c) does not comply with an objection or the requirement pursuant to Article 19;

(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;

(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;

(f) does not designate a representative pursuant to Article 25;

(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;

(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;

(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;

(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;

(k) misuses a data protection seal or mark in the meaning of Article 39;

(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);

(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);

(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.

CHAPTER IX
PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

Article 80
Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

Article 81
Processing of personal data concerning health

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or

(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or

(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 82
Processing in the employment context

1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or

collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Article 83
Processing for historical, statistical and scientific research purposes

1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:

   (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

   (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:

   (a) the data subject has given consent, subject to the conditions laid down in Article 7;

   (b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or

   (c) the data subject has made the data public.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

Article 84
Obligations of secrecy

1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules

established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Article 85
Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.

CHAPTER X
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 86
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official*

Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Article 87
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI
FINAL PROVISIONS

Article 88
Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 89
Relationship to and amendment of Directive 2002/58/EC

1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2 Article 1(2) of Directive 2002/58/EC shall be deleted.

Article 90
Evaluation

The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.

Article 91
Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union.*

2. It shall apply from [*two years from the date referred to in paragraph 1*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned in the ABM/ABB structure

1.3. Nature of the proposal/initiative

1.4. Objective(s)

1.5. Grounds for the proposal/initiative

1.6. Duration and financial impact

1.7. Management method(s) envisaged

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

3.2.2. Estimated impact on operational appropriations

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party participation in financing

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

This financial statement indicates in more detail the requirements in terms of administrative expenditure in order to put in practice the data protection reform, as explained in the corresponding impact assessment. The reform includes two legislative proposals, a general Data Protection Regulation and a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This financial statement covers the budgetary impact of both instruments.

According to the distribution of tasks, resources are required by the Commission and by the European Data Protection Supervisor (EDPS).

As regards the Commission, the necessary resources are already included in the proposed financial perspective 2014-2020. Data protection is one of the objectives of the Rights and Citizenship' programme, which will also support measures to put the legal framework into practice. The administrative appropriations including staff requirements are included in the administrative budget for DG JUST.

As regards the EDPS, the necessary resources will need to be taken into account in the respective annual budgets for the EDPS. The resources are detailed in the annex of this financial statement. In order to provide the resources required for the new tasks of the European Data Protection Board, for which the EDPS will provide the secretariat, reprogramming of Heading 5 of the financial perspective 2014-2020 will be required.

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free flow of such data (General Data Protection Regulation).

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

1.2. Policy area(s) concerned in the ABM/ABB structure[49]

Justice – Protection of Personal Data

The budgetary impact concerns the Commission and the EDPS. The impact on the Commission budget is detailed in the tables of this financial statement. Operational

[49] ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

expenditure is part of the Rights and Citizenship Programme and has been taken into account in the financial statement for that programme already, as administrative expenditure is within the envelope for DG Justice. The elements concerning the EDPS are shown in the Annex.

1.3. Nature of the proposal/initiative

☐ The proposal/initiative relates to **a new action**

☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**[50]

☑ The proposal/initiative relates to **the extension of an existing action**

☐ The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objectives

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/initiative

The reform aims at completing the achievement of the original objectives, taking account of new developments and challenges, i.e.:

- increasing the effectiveness of the fundamental right to data protection and putting individuals in control of their data, particularly in the context of technological developments and increased globalisation;

- enhancing the internal market dimension of data protection by reducing fragmentation, strengthening consistency and simplifying the regulatory environment, thus eliminating unnecessary costs and reducing the administrative burden.

In addition, the entry into force of the Lisbon Treaty - and in particular the introduction of a new legal basis (Article 16 TFEU) - offers the opportunity to achieve a new objective, i.e.

- to establish a comprehensive data protection framework covering all areas.

1.4.2. Specific objective(s) and ABM/ABB activity(ies) concerned

Specific objective No 1

To ensure consistent enforcement of data protection rules

Specific objective No 2

To rationalise the current governance system to help ensuring a more consistent enforcement

ABM/ABB activity(ies) concerned

[...]

50 As referred to in Article 49(6)(a) or (b) of the Financial Regulation.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

As regards data controllers, both public and private entities shall benefit from more legal certainty by harmonised and clarified EU data protection rules and procedures creating a level playing field and ensuring consistent enforcement of data protection rules, as well as a considerable reduction of administrative burden.

Individuals will enjoy better control of their personal data and trust the digital environment and will remain protected including when their personal data are processed abroad. They will also encounter reinforced accountability of those processing personal data.

A comprehensive data protection system will also cover the areas of police and justice, including and beyond the former 3rd pillar.

1.4.4. Indicators of results and impact

Specify the indicators for monitoring implementation of the proposal/initiative.

(cf. Impact Assessment, Section 8)

Indicators shall be evaluated periodically and shall include the following elements:

- Time and costs spent by data controllers in complying with legislation in 'other Member States'
- Resources allocated to DPAs,
- established DPOs in public and private organisations,
- Use made of DPIA,
- number of complaints made by data subjects and compensation received by data subjects,
- number of cases leading to prosecution of data controllers,
- fines imposed on data controllers responsible for breaches of data protection.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term

The current divergences in the implementation, interpretation and enforcement of the Directive by Member States ***hamper the functioning of the internal market and co-operation between public authorities in relation to EU policies.*** This goes against the fundamental objective of the Directive of facilitating the free flow of personal data in the internal market. The rapid development of new technologies and globalisation further exacerbates this problem.

Individuals enjoy different data protection rights, due to fragmentation and inconsistent implementation and enforcement in different Member States. Furthermore, ***individuals are often neither aware nor in control of what happens to their personal data*** and therefore fail to exercise their rights effectively.

1.5.2. Added value of EU involvement

Member States alone cannot reduce the problems in the current situation. This is particularly the case for those problems that arise from the fragmentation in national legislations implementing the EU data protection regulatory framework. Thus, there is a strong rationale for a legal framework for data protection at EU level. There is a particular need to establish a harmonised and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection to all individuals across the EU.

1.5.3. Lessons learned from similar experiences in the past

The present proposals build on the experience with Directive 95/46/EC and the problems encountered due to fragmented transposition and implementation of that Directive, which have blocked it from achieving both its objectives, i.e. a high level of data protection and a single market for data protection.

1.5.4. Coherence and possible synergy with other relevant instruments

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level - technologically neutral, and future proof for the decades to come. It will benefit individuals – by strengthening their data protection rights, particularly in the digital environment - and will simplify the legal environment for businesses and the public sector, thus stimulating the development of the digital economy across the EU internal market and beyond, in line with the objectives of the Europe 2020 strategy.

The core of the data protection reform package consists of:

– a Regulation replacing Directive 95/46/EC;

– a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, detection, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

These legislative proposals are accompanied by a report on the implementation by Member States of what is currently the main EU data protection instrument in the areas of police co-operation and judicial co-operation in criminal matters, the Framework Decision 2008/977/JHA.

1.6. Duration and financial impact

☐ Proposal/initiative of **limited duration**

1. ☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

2. ☐ Financial impact from YYYY to YYYY

☑ Proposal/initiative of **unlimited duration**

1. Implementation with a start-up period from 2014 to 2016,

2. followed by full-scale operation.

1.7. Management mode(s) envisaged[51]

☑ **Centralised direct management** by the Commission

☐ **Centralised indirect management** with the delegation of implementation tasks to:

3. ☐ executive agencies

4. ☐ bodies set up by the Communities[52]

5. ☐ national public-sector bodies/bodies with public-service mission

3. ☐ persons entrusted with the implementation of specific actions pursuant to Title V of the Treaty on European Union and identified in the relevant basic act within the meaning of Article 49 of the Financial Regulation

☐ **Shared management** with the Member States

☐ **Decentralised management** with third countries

☐ **Joint management** with international organisations ***(to be specified)***

If more than one management mode is indicated, please provide details in the "Comments" section.

Comments

//

---

51 Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

52 As referred to in Article 185 of the Financial Regulation.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The first evaluation will take place 4 years after the entry into force of the legal instruments. An explicit review clause, by which the Commission will evaluate the implementation, is included in the legal instruments. The Commission will subsequently report to the European Parliament and the Council on its evaluation. Further evaluations will have to take place every four years. The Commission methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted studies on the implementation of the legal instruments, questionnaires to national data protection authorities, expert discussions, workshops, Eurobarometer surveys, and so forth.

2.2. Management and control system

2.2.1. Risk(s) identified

An Impact Assessment has been carried out for the reform of the data protection framework in the EU to accompany the proposals for the Regulations and the Directive

The new legal instrument will introduce a consistency mechanism, ensuring that independent supervisory authorities in Member States apply the framework in a consistent and coherent manner. The mechanism will operate through the European Data Protection Board composed of the heads of the national supervisory authorities and of the European Data Protection Supervisor (EDPS), which will replace the current Article 29 Working Party. The EDPS will provide the secretariat for this body.

In case of possibly divergent decisions by Member States' authorities, the European Data Protection Board will be consulted in order to issue an opinion on the matter. Should this procedure fail, or if a supervisory authority refuses to comply with the opinion, the Commission might, in order to ensure correct and consistent application of this Regulation, may issue an opinion or, where necessary, adopt a decision, where it has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application.

The consistency mechanism requires additional resources for the EDPS (12 FTE and adequate administrative and operative appropriations, e.g., for IT systems and operations) for providing the secretariat and for the Commission (5 FTE and related administrative and operational appropriations) for the handling of consistency cases.

2.2.2. Control method(s) envisaged

Existing control methods applied by the EDPS and by the Commission will cover the additional appropriations.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures

Existing fraud prevention measures applied by the EDPS and by the Commission will cover the additional appropriations.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

1. Existing expenditure budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Description... ... ...]	Diff./non-diff. (53)	from EFTA[54] countries	from candidate countries[55]	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to 3 decimal places)

Heading of multiannual financial framework:	Number	

			Year N[56]= 2014	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
• Operational appropriations										
Number of budget line	Commitments	(1)								
	Payments	(2)								

53 Diff. = Differentiated appropriations / Non-diff. = Non-Differentiated Appropriations

54 EFTA: European Free Trade Association.

55 Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

56 Year N is the year in which implementation of the proposal/initiative starts.

Number of budget line	Commitments	(1a)								
	Payments	(2a)								
Appropriations of an administrative nature financed from the envelope for specific programmes[57]										
Number of budget line		(3)								
TOTAL appropriations for DG	Commitments	=1+1a +3								
	Payments	=2+2a +3								

• TOTAL operational appropriations	Commitments	(4)								
	Payments	(5)								
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADING 3 of the multiannual financial framework	Commitments	=4+ 6								
	Payments	=5+ 6								

If more than one heading is affected by the proposal / initiative:

• TOTAL operational appropriations	Commitments	(4)								
	Payments	(5)								
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADINGS 1 to 4 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6								
	Payments	=5+ 6								

Heading of multiannual financial framework:	**5**	" Administrative expenditure "

[57] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former "BA" lines), indirect research, direct research.

EUR million (to 3 decimal places)

		Year N= 2014	Year 2015	Year 2016	Year 2017	Year 2018	Year 2019	Year 2020	TOTAL
DG: JUST									
• Human resources		2.922	2.922	2.922	2.922	2.922	2.922	2.922	**20.454**
• Other administrative expenditure		0.555	0.555	0.555	0.555	0.555	0.555	0.555	**3.885**
TOTAL DG JUST		**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**24.339**

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**24.339**

EUR million (to 3 decimal places)

		Year N[58]	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**24.339**
	Payments	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**24.339**

58 Year N is the year in which implementation of the proposal/initiative starts.

3.2.2. Estimated impact on operational appropriations

6. ☑ The proposal/initiative does not require the use of operational appropriations

A high level of protection of personal data is also one of the objectives of the Rights and Citizenships Programme.

7. ☐ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to 3 decimal places)

Indicate objectives and outputs ⇩			Year **N=2014**		Year **N+1**		Year **N+2**		Year **N+3**		... enter as many years as necessary to show the duration of the impact (see point 1.6)				**TOTAL**	
			OUTPUTS													
	Type of output[59]	Average cost of the output	**Number of outputs**	**Cost**	**Number of outputs**	**Cost**	**Number of outputs**	**Cost**	**Number of outputs**	**Cost**	**Number of outputs**	**Cost**	**Number of outputs**	**Cost**	**Total number of outputs**	**Total cost**
SPECIFIC OBJECTIVE No 1																
- Output	Files[60]															
Sub-total for specific objective N°1																
SPECIFIC OBJECTIVE No 2																
- Output	Cases[61]															
Sub-total for specific objective N°2																
TOTAL COST																

59 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

60 Opinions, decisions, procedures meetings of the board.

61 Cases treated under the consistency mechanism

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.3.1. Summary

8. ☐ The proposal/initiative does not require the use of administrative appropriations

9. ☑ The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to 3 decimal places)

	Year N [62] 2014	Year 2015	Year 2016	Year 2017	Year 2018	Year 2019	Year 2020	TOTAL
HEADING 5 of the multiannual financial framework								
Human resources	2.922	2.922	2.922	2.922	2.922	2.922	2.922	**20.454**
Other administrative expenditure	0.555	0.555	0.555	0.555	0.555	0.555	0.555	**3.885**
Subtotal HEADING 5 of the multiannual financial framework	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**3.477**	**24.339**
Outside HEADING 5 of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature								
Subtotal outside HEADING 5 of the multiannual financial framework								
TOTAL	3.477	3.477	3.477	3.477	3.477	3.477	3.477	24.339

62 Year N is the year in which implementation of the proposal/initiative starts.

63 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former "BA" lines), indirect research, direct research.

3.2.3.2. Estimated requirements of human resources

10. ☐ The proposal/initiative does not require the use of human resources

11. ☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units (or at most to one decimal place)

		Year **2014**	Year **2015**	Year **2016**	Year **2017**	Year **2018**	Year **2019**	Year **2020**
• **Establishment plan posts (officials and temporary agents)**								
XX 01 01 01 (Headquarters and Commission's Representation Offices)		22	22	22	22	22	22	22
XX 01 01 02 (Delegations)								
• **External personnel (in Full Time Equivalent unit: FTE)**[64]								
XX 01 02 01 (CA, INT, SNE from the "global envelope")		2	2	2	2	2	2	2
XX 01 02 02 (CA, INT, JED, LA and SNE in the delegations)								
XX 01 04 *yy* [65]	- at Headquarters[66]							
	- in delegations							
XX 01 05 02 (CA, INT, SNE - Indirect research)								
10 01 05 02 (CA, INT, SNE - Direct research)								
Other budget lines (specify)								
TOTAL		**24**	**24**	**24**	**24**	**24**	**24**	**24**

XX is the policy area or budget title concerned.

With the reform, the Commission will have to perform new tasks in the area of the protection of individuals regarding the processing of personal data, in addition to those currently performed. The additional tasks mainly concern the implementation of the new consistency mechanism which will ensure coherent application of harmonised data protection law, the adequacy assessment of third countries for which the Commission will have sole responsibility, and the preparation of implementing measures and delegated acts. The other tasks currently performed by the Commission (e.g. policy development, monitoring transposition, awareness raising, complaints etc), will continue to be performed.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the

---

64 CA= Contract Agent; INT= agency staff (*"Intérimaire"*); JED= *"Jeune Expert en Délégation"* (Young Experts in Delegations); LA= Local Agent; SNE= Seconded National Expert;

65 Under the ceiling for external personnel from operational appropriations (former "BA" lines).

66 Essentially for Structural Funds, European Agricultural Fund for Rural Development (EAFRD) and European Fisheries Fund (EFF).

managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary agents	Case handlers, operating the data protection consistency mechanism to ensure unity of application of EU data protection rules. Tasks include investigation and research of cases submitted for decision from Member States' authorities, negotiation with Member States and preparation of Commission decisions. Based on recent experience, 5 to 10 cases per year may require invocation of the consistency mechanism. The handling of adequacy requests requires direct interaction with the requesting country, possibly the management of expert studies on the conditions in the country, assessment of the conditions, preparation of the relevant Commission decisions and of the process, including of the Committee assisting the Commission and any expert bodies as appropriate. Based on current experience, up to 4 adequacy requests can be expected per year. The process of adopting implementing measures includes preparatory measures, such as issue papers, research and public consultations, as well as the drafting of the actual instrument and management of the negotiation process in the relevant Committees and other groups, as well as stakeholder contacts in general. Across the areas requiring more precise guidance, up to three implementing measures may be handled per year, while the process may take up to 24 months, depending on the intensity of consultations.
External personnel	Administrative and secretarial support

3.2.4. Compatibility with the current multiannual financial framework

12. ☐ Proposal/initiative is compatible with the *next* multiannual financial framework.

13. ☑ Proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

The table below indicates the amounts of financial resources required annually by the EDPS for its new tasks of providing the secretariat of the European Data Protection Board and the related procedures and tools over the period of the next financial perspective, in addition to those already included in the planning.

Year	2014	2015	2016	2017	2018	2019	2020	Total
Staff etc	1.555	1.555	1.543	1.543	1.543	1.543	1.543	10.823
Operations	0.850	1.500	1.900	1.900	1.500	1.200	1.400	10.250
Total	**2.405**	**3.055**	**3.443**	**3.443**	**3.043**	**2.743**	**2.943**	**21.073**

14. ☐ Proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[67].

[67] See points 19 and 24 of the Interinstitutional Agreement.

3.2.5. *Third-party contributions*

15. ☑ The proposal/initiative does not provide for co-financing by third parties

16. ☐ The proposal/initiative provides for the co-financing estimated below:

Appropriations in EUR million (to 3 decimal places)

	Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	... enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations cofinanced								

3.3. Estimated impact on revenue

17. ☑ Proposal/initiative has no financial impact on revenue.

18. ☐ Proposal/initiative has the following financial impact:

- ☐ on own resources
- ☐ on miscellaneous revenue

EUR million (to 3 decimal places)

Budget revenue line:	Appropriations available for the ongoing budget year	Impact of the proposal/initiative[68]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	... insert as many columns as necessary in order to reflect the duration of the impact (see point 1.6)		

For miscellaneous assigned revenue, specify the budget expenditure line(s) affected.
Specify the method for calculating the impact on revenue.

[68] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 25% for collection costs.

Annex to Legislative Financial Statement for proposal for a Regulation of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data.

Applied methodology and main underlying assumptions

The costs related to the new tasks to be carried out by the European Data Protection Supervisor (EDPS) stemming from the two proposals have been estimated for staff expenditure on the basis of the costs incurred by the Commission currently for similar tasks.

The EDPS will host the secretariat of the European Data Protection Board replacing the Article 29 Working Party. On the basis of the Commission current workload for this task, this results in the need for 3 additional FTE plus corresponding administrative and operational expenditure. This workload will commence from the entry into force of the Regulation.

Furthermore, the EDPS will have a role in the consistency mechanism which is expected to require 5 FTEs, and in developing and operating a common IT tool for national DPAs, which will require 2 additional staff members.

The calculation of the increase in the required staff budget for the first seven years is presented in more detail in the table below. A second table shows the required operational budget. This will be reflected in the Budget of the EU in Section IX EDPS.

Cost type	**Calculation**	**Amount (in thousands)**							
		2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
Salaries and allowances									
- of EDPB Chair		0.300	0.300	0.300	0.300	0.300	0.300	0.300	2.100
- of which officials and temporary agents	=7*0.127	0.889	0.889	0.889	0.889	0.889	0.889	0.889	6.223
- of which SNEs	=1*0.073	0.073	0.073	0.073	0.073	0.073	0.073	0.073	0.511
- of which contract agents	=2*0.064	0.128	0.128	0.128	0.128	0.128	0.128	0.128	0.896
Expenditure related to recruitment	=10*0.005	0.025	0.025	0.013	0.013	0.013	0.013	0.013	0.113
Mission expenses		0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.630
Other expenses, training	=10*0.005	0.050	0.050	0.050	0.050	0.050	0.050	0.050	0.350
Total Administrative expenditure		**1.555**	**1.555**	**1.543**	**1.543**	**1.543**	**1.543**	**1.543**	**10.823**

Description of tasks to be carried out:

Officials and temporary agents	Desk officers in charge of the secretariat of the Data Protection Board. Apart from logistics support, including budgetary and contractual issues, this includes the preparation of meeting agendas and expert invitations, research on subjects on the agenda of the group, management of the documents relating to the work of the group including the relevant data protection, confidentiality and public access requirements. Including all subgroups and expert groups, up to 50 meetings and decision procedures may have to be organised every year. Case handlers, operating the data protection consistency mechanism to ensure unity of application of EU data protection rules. Tasks include investigation and research of cases submitted for decision from Member States' authorities, negotiation with Member States and preparation of Commission decisions. Based on recent experience, there may be 5 to 10 cases per year requiring invocation of the consistency mechanism. The IT tool shall simplify the operational interaction between national DPAs and data controllers obliged to share information with the public authorities. The responsible staff member(s) will ensure quality control, project management and budgetary follow-up of the IT processes on requirements engineering, implementation and operation of the systems.
External personnel	Administrative and secretarial support

Expenditure for EDPS relating to specific tasks

Indicate objectives and outputs ⇩			Year N=2014		Year N+1		Year N+2		Year N+3		enter as many years as necessary to show the duration of the impact (see point 1.6)						TOTAL	
			OUTPUTS															
	Type of output[69]	Average cost of the output	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Total number of outputs	Total cost
SPECIFIC OBJECTIVE No 1[70]			Secretariat to DP Board															
- Output	Cases[71]	0.010	30	0.300	40	0.400	50	0.500	50	0.500	50	0.500	50	0.500	50	0.500	320	3.200
Sub-total for specific objective N°1			30	0.300	40	0.400	50	0.500	50	0.500	50	0.500	50	0.500	50	0.500	320	3.200
SPECIFIC OBJECTIVE No 2			Consistency Mechanism															
- Output	Files[72]	0.050	5	0.250	10	0.500	10	0.500	10	0.500	8	0.400	8	0.400	8	0.400	59	2.950
Sub-total for specific objective N°2			5	0.250	10	0.500	10	0.500	10	0.500	8	0.400	8	0.400	8	0.400	59	2.950
SPECIFIC OBJECTIVE No 3			Common IT tool for DPAs (EDPS)															
- Output	Cases[73]	0.100	3	0.300	6	0.600	9	0.900	9	0.900	6	0.600	3	0.300	5	0.500	41	4.100
Sub-total for specific objective N°3			3	0.300	6	0.600	9	0.900	9	0.900	6	0.600	3	0.300	5	0.500	41	4.100
TOTAL COST			38	0.850	56	1.500	69	1.900	69	1.900	64	1.500	61	1.200	63	1.400	420	10.250

69 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

70 As described in Section 1.4.2. "Specific objective(s)..."

71 Cases treated under the consistency mechanism

72 Opinions, decisions, procedures meetings of the board.

73 The totals for each year estimate the efforts for developing and operating the IT tools

EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 10 final

2012/0010 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

{SEC(2012) 72 final}
{SEC(2012) 73 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

This explanatory memorandum further details the approach for the new legal framework for the protection of personal data in the EU as presented in Communication COM (2012) 9 final. The legal framework consists of two legislative proposals:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and

- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

This explanatory memorandum concerns the latter legislative proposal.

The centrepiece of existing EU legislation on personal data protection, Directive 95/46/EC[1], was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. It was complemented by several instruments providing specific data protection rules in the area of police and judicial co-operation in criminal matters[2] (ex-third pillar), including Framework Decision 2008/977/JHA[3].

The European Council invited the Commission to evaluate the functioning of EU instruments on data protection and to present, where necessary, further legislative and non-legislative initiatives[4]. In its resolution on the Stockholm Programme, the European Parliament[5] welcomed a comprehensive data protection scheme in the EU and among others called for the revision of the Framework Decision. The Commission stressed in its Action Plan implementing the Stockholm Programme[6] the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies. The Action Plan underlined that *"in a global society characterised by rapid technological change where information exchange knows no borders, it is particularly important that privacy must be preserved. The Union must ensure that the fundamental right to data protection is consistently applied. We need to strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations."*

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/95, p.31.

2 See the full list in Annex 3 to the Impact Assessment (SEC(2012)72).

3 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

4 In the Stockholm Programme, OJ C 115, 4.5.2010, p. 1.

5 See the Resolution of the European Parliament on the Stockholm Programme adopted on 25 November 2009.

6 COM(2010)171final.

In its Communication on "A comprehensive approach on personal data protection in the European Union"[7], the Commission concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection.

Framework Decision 2008/977/JHA has a limited scope of application, since it only applies to cross-border data processing and not to processing activities by the police and judiciary authorities at purely national level. This is liable to create difficulties for police and other competent authorities in the areas of judicial co-operation in criminal matters and police co-operation. They are not always able to easily distinguish between purely domestic and cross-border processing or to foresee whether certain personal data may become the object of a cross-border exchange at a later stage(see Section 2 below). Moreover, because of its nature and content, the Framework Decision leaves a large room for manoeuvre to Member States' national laws in implementing its provisions. Additionally, it does not contain any mechanism or advisory group similar to the Article 29 Working Party supporting common interpretation of its provisions, nor foresees any implementing powers for the Commission to ensure a common approach in its implementation.

Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) establishes the principle that everyone has the right to the protection of personal data. Moreover, with Article 16 (2) TFEU, the Lisbon Treaty introduces a specific legal basis for the adoption of rules on the protection of personal data that also applies to judicial co-operation in criminal matters and police co-operation. Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right. Article 16 TFEU requires the legislator to lay down rules relating to the protection of individuals with regard to the processing of personal data also in the areas of judicial co-operation in criminal matters and police co-operation, covering both cross-border and domestic processing of personal data. This will allow protecting the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, ensuring at the same time the exchange of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This will contribute to facilitating the co-operation in the fight against crime in Europe.

Due to the specific nature of the field of police and judicial co-operation in criminal matters it was acknowledged in Declaration 21[8] that specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 TFEU may prove necessary.

2. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENTS

This initiative is the result of extensive consultations with all major stakeholders on a review of the existing legal framework for the protection of personal data, which included two phases of public consultation:

---

7 European Commission, Communication on "A comprehensive approach on personal data protection in the European Union", COM(2010)609 final, 4 November 2010.

8 Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, 13.12.2007).

- From 9 July to 31 December 2009, the *Consultation on the legal framework for the fundamental right to the protection of personal data*. The Commission received 168 responses, 127 from individuals, business organisations and associations and 12 from public authorities. The non-confidential contributions can be consulted on the Commission's website[9].

- From 4 November 2010 to 15 January 2011, the *Consultation on the Commission's comprehensive approach on personal data protection in the European Union*. The Commission received 305 responses, of which 54 from citizens, 31 from public authorities and 220 from private organisations, in particular business associations and non-governmental organisations. The non-confidential contributions can be consulted on the Commission's website[10].

Whereas those consultations focused largely on the review of Directive 95/46/EC, targeted consultations were conducted with law enforcement stakeholders; in particular, a workshop was organised on 29 June 2010 with Member States' authorities on the application of data protection rules to public authorities, including in the area of police co-operation and judicial co-operation in criminal matters. Furthermore, on 2 February 2011, the Commission convened a workshop with Member States' authorities to discuss the implementation of Framework Decision 2008/977/JHA and, more generally, data protection issues in the area of police co-operation and judicial co-operation in criminal matters.

EU citizens were consulted through a Eurobarometer survey held in November-December 2010[11]. A number of studies were also launched.[12] The "Article 29 Working Party"[13] provided several opinions and useful input to the Commission[14]. The European Data Protection Supervisor also issued a comprehensive opinion on the issues raised in the Commission's November 2010 Communication.[15]

The European Parliament approved by its resolution of 6 July 2011 a report that supported the Commission's approach to reforming the data protection framework.[16] The Council of the

---

9 http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

11 Special Eurobarometer (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

12 See the *Study on the economic benefits of privacy enhancing technologies* or the *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, January 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

13 The Working Party was set up in 1996 (by Article 29 of the Directive) with advisory status and composed of representatives of national Data Protection Supervisory Authorities (DPAs), the European Data Protection Supervisor (EDPS) and the Commission. For more information on its activities see http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

14 See in particular the following opinions: on the "Future of Privacy" (2009, WP 168); on the concepts of "controller" and "processor" (1/2010, WP 169); on online behavioural advertising (2/2010, WP 171); on the principle of accountability (3/2010, WP 173); on applicable law (8/2010, WP 179); and on consent (15/2011, WP 187). Upon the Commission's request, it adopted also the three following Advice Papers: on notifications, on sensitive data and on the practical implementation of Article 28(6) of the Directive 95/46/EC. They can all be accessed at: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

15 Available on the EDPS website: http://www.edps.europa.eu/EDPSWEB/.

16 EP resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244 (rapporteur: MEP Axel Voss (EPP/DE).

European Union adopted conclusions on 24 February 2011 in which it broadly supports the Commission's intention to reform the data protection framework and agrees with many elements of the Commission's approach. The European Economic and Social Committee likewise supported the Commission's general thrust to ensure a more consistent application of EU data protection rules across all Member States and an appropriate revision of the Directive 95/46/EC.[17]

In line with its "Better Regulation" policy, the Commission conducted an impact assessment of policy alternatives[18]. The impact assessment was based on the three policy objectives of improving the internal market dimension of data protection, making the exercise of data protection rights by individuals more effective and creating a comprehensive and coherent framework covering all areas of Union competence, including police co-operation and judicial co-operation in criminal matters. As regards this latter objective in particular, two policy options were assessed: a first one basically extending the scope of data protection rules in this area and addressing the gaps and other issues raised by the Framework Decision, and a second more far-reaching one with very prescriptive and stringent rules, which would also entail the immediate amendment of all other "former third pillar" instruments. A third "minimalistic" option based largely on interpretative Communications and policy support measures, such as funding programmes and technical tools, with minimum legislative intervention, was not considered appropriate to address the issues identified in this area in relation to data protection.

According to the Commission's established methodology, each policy option was assessed, with the help of an inter-service steering group, against its effectiveness to achieve the policy objectives, its economic impact on stakeholders (including on the budget of the EU institutions), its social impact and effect on fundamental rights. Environmental impacts were not observed.

The analysis of the overall impact led to the development of the preferred policy option which is incorporated in the present proposal. According to the assessment, its implementation will lead to further strengthening data protection in this policy area in particular by including domestic data processing, thereby also enhancing legal certainty for competent authorities in the areas of judicial co-operation in criminal matters and police co-operation.

The Impact Assessment Board (IAB) delivered an opinion on the draft impact assessment on 9 September 2011. Following the IAB's opinion, in particular the following changes were made to the impact assessment:

– The objectives of the current legal framework (to what extent they were achieved and to what extent they were not), as well as the objectives of the envisaged reform, were clarified;

– More evidence and additional explanations/clarifications were added to the problems' definition section.

The Commission also prepared an Implementation Report related to Framework Decision 2008/977/JHA, based on its Article 29(2), which is to be adopted as part of the present data

---

17 CESE 999/2011.
18 SEC(2012)72.

protection package[19]. The findings of the report, based on input from Member States, also fed into the preparation of the Impact Assessment.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. Legal Basis

The proposal is based on Article 16(2) TFEU, which is a new, specific legal basis introduced by the Lisbon Treaty for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

The proposal aims to ensure a consistent and high level of data protection in this field, thereby enhancing mutual trust between police and judicial authorities of different Member States and facilitating the free flow of data and co-operation between police and judicial authorities.

3.2. Subsidiarity and proportionality

According to the principle of subsidiarity (Article 5(3) TEU), action at Union level shall be taken only if and in so far as the objectives envisaged cannot be achieved sufficiently by Member States, but can rather, by reason of the scale or effects of the proposed action, be better achieved by the Union. In the light of the problems outlined above, the analysis of subsidiarity indicates the necessity of EU-level action in the areas of police and criminal justice on the following grounds:

- The right to the protection of personal data, enshrined in Article 8 of the Charter of Fundamental Rights and in Article 16(1) TFEU, requires the same level of data protection throughout the Union. It requires the same level of protection for data exchanged and data processed at domestic level.

- There is a growing need for law enforcement authorities in Member States to process and exchange at rapidly increasing rates for the purposes of preventing and combating transnational crime and terrorism. In this context, clear and consistent rules on data protection at EU level will help fostering co-operation between such authorities.

- In addition, there are practical challenges to enforcing data protection legislation and a need for co-operation between Member States and their authorities, which need to be organised at EU level to ensure unity of application of Union law. In certain situations, the EU is best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries.

- Member States cannot alone reduce the problems in the current situation, particularly those due to the fragmentation in national legislations. Thus, there is a specific need to establish a harmonised and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection for all individuals across the EU.

---

19 COM(2012)12.

– The proposed EU legislative action is likely to be more effective than similar actions at the level of Member States because of the nature and scale of the problems, which are not confined to the level of one or several Member States.

The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal, from the identification and evaluation of alternative policy options to the drafting of the legislative proposal.

A Directive is therefore the best instrument to ensure harmonisation at EU level in this area while at the same time leaving the necessary flexibility to Member States when implementing the principles, the rules and their exemptions at national level. Given the complexity of the current national rules for the protection of personal data processed in the area of police co-operation and judicial co-operation in criminal matters, and the objective of comprehensive harmonisation of these rules by way of this Directive, the Commission will need to request Member States to provide explanatory documents explaining the relationship between the components of the Directive and the corresponding parts of national transposition instruments in order to be able to carry out its task of overseeing the transposition of this Directive.

3.3. Summary of fundamental rights issues

The right to protection of personal data is established by Article 8 of the Charter on Fundamental Rights of the EU and Article 16 TFEU as well in Article 8 of the ECHR. As underlined by the Court of Justice of the EU[20], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[21]. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected in Article 1(1) of Directive 95/46/EC, which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

Other potentially affected fundamental rights enshrined in the Charter are the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24) and the right to an effective remedy before a tribunal and a fair trial (Article 47).

3.4. Detailed explanation of the proposal

3.4.1. CHAPTER I – GENERAL PROVISIONS

Article 1 defines the subject matter of the Directive, i.e. rules relating to processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences, and sets out the Directive's two-fold objective, i.e. to protect the fundamental rights and freedoms of natural persons and in

---

20 Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

21 In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

particular their right to the protection of personal data while guaranteeing a high level of public safety, and to ensure the exchange of personal data between competent authorities within the Union.

Article 2 defines the scope of application of the Directive. The scope of the Directive is not limited to cross-border data processing but applies to all processing activities carried out by 'competent authorities' (as defined in Article 3(14)) for the purposes of the Directive. The Directive applies neither to processing in the course of an activity which falls outside the scope of Union law, nor to processing by Union institutions, bodies, offices and agencies, which is subject to Regulation (EC) No 45/2001 and other specific legislation.

Article 3 contains definitions of terms used in the Directive. While some definitions are taken over from Directive 95/46/EC and Framework Decision 2008/977/JHA, others are modified, complemented with additional or newly introduced elements. New definitions are those of 'personal data breach', 'genetic data' and 'biometric data', 'competent authorities' (based on Article 87 TFEU and Article 2(h) of Framework Decision 2008/977/JHA) and, of a 'child', based on the UN Convention on the Rights of the Child[22].

3.4.2. CHAPTER II – PRINCIPLES

Article 4 sets out the principles relating to processing of personal data reflecting Article 6 of Directive 95/46/EC and Article 3 of Framework Decision 2008/977/JHA, while adjusting them to the particular context of this Directive.

Article 5 requires the distinction, as far as possible; between personal data of different categories of data subjects. This is a new provision, included neither in Directive 95/46/EC nor in Framework Decision 2008/977/JHA, but which had been proposed by the Commission in its original proposal for the Framework Decision[23]. It is inspired by the Council of Europe's Recommendation No R (87)15. Similar rules already exist for Europol[24] and Eurojust[25].

Article 6 on different degrees of accuracy and reliability reflects principle 3.2 of Council of Europe Recommendation No R (87)15. Similar rules, as also included in the Commission's proposal for the Framework Decision, exist for Europol[26].

Article 7 sets out the grounds for lawful processing, when necessary for the performance of a task carried out by a competent authority based on national law, to comply with a legal obligation to which the data controller is subject, in order to protect the vital interests of the data subject or another person or to prevent an immediate and serious threat to public security. The other grounds for lawful processing in Article 7 of Directive 95/46/EC are not appropriate for the processing in the area of police and criminal justice.

Article 8 sets out a general prohibition of processing special categories of personal data and the exceptions from this general rule, building on Article 8 of Directive 95/46/EC and adding genetic data, following ECtHR case law[27].

---

22 Referred to also in Article 2 (a) of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1.

23 COM(2005) 475 final.

24 Article 14 Europol Decision 2009/371/JHA.

25 Article 15 Eurojust Decision 2009/426/JHA.

26 Article 14 Europol Decision 2009/371/JHA.

Article 9 establishes a prohibition of measures based solely on automated processing of personal data if not authorised by law providing appropriate safeguards, in line with Article 7 of Framework Decision 2008/977/JHA.

3.4.3. CHAPTER III - RIGHTS OF THE DATA SUBJECT

Article 10 introduces the obligation for Member States to ensure easily accessible and understandable information, inspired in particular by principle 10 of the Madrid Resolution on international standards on the protection of personal data and privacy[28], and to oblige controllers to provide procedures and mechanisms for facilitating the exercise of the data subject's rights. This includes the requirement that the exercise of the rights shall be in principle free of charge.

Article 11 specifies the obligation for Member States to ensure the information towards the data subject. These obligations are building on Articles 10 and 11 of Directive 95/46/EC, without separate articles differentiating whether the information is collected from the data subject or not, and enlarging the information to be provided. It lays down exemptions from the obligation to inform, when such exemptions are proportionate and necessary in a democratic society for the exercise of the tasks of competent authorities (inspired by Article 13 of Directive 95/46/EC and Article 17 Framework Decision 2008/977/JHA).

Article 12 provides the obligation for Member States to ensure the data subject's right of access to their personal data. It follows Article 12(a) of Directive 95/46/EC, adding new elements for the information of the data subjects (on the storage period, their rights to rectification, erasure, or restriction and to lodge a complaint).

Article 13 provides that Member States may adopt legislative measures restricting the right of access if required by the specific nature of data processing in the areas of police and criminal justice, and on the information of the data subject on a restriction of access, following Article 17(2) and (3) of Framework Decision 2008/977/JHA.

Article 14 introduces the rule that in cases where direct access is restricted, the data subject must be informed on the possibility of indirect access via the supervisory authority, which should exercise the right on their behalf and must inform the data subject on the outcome of its verifications.

Article 15 on the right to rectification follows Article 12(b) of Directive 95/46/EC, and, as regards the obligations in case of a refusal, Article 18(1) of Framework Decision 2008/977/JHA.

Article 16 on the right to erasure follows Article 12(b) of Directive 95/46, and, as regards the obligations in case of a refusal, Article 18(1) of Framework Decision 2008/977/JHA. It integrates also the right to have the processing marked in certain cases, replacing the ambiguous terminology "blocking", used by Article 12(b) of Directive 95/46/EC and Article 18(1) of Framework Decision 2008/977/JHA.

Article 17 on the rectification, erasure and restriction of processing in judicial proceedings provides clarification based on Article 4(4) of Framework Decision 2008/977/JHA.

---

27 ECtHR, judgment of 4.12.2008, S. and Marper v. UK (Application nos. 30562/04 and 30566/04).

28 Adopted by the International Conference of Data Protection and Privacy Commissioners on 5.11.2009.

3.4.4. CHAPTER IV - CONTROLLER AND PROCESSOR

3.4.4.1. SECTION 1 GENERAL OBLIGATIONS

Article 18 describes the responsibility of the controller to comply with this Directive and to ensure compliance, including the adoption of policies and mechanisms for ensuring compliance.

Article 19 sets out that the Member States must ensure the compliance of the controller with the obligations arising from the principles of data protection by design and by default.

Article 20 on joint controllers clarifies the status of joint controllers as regards their internal relationship.

Article 21 clarifies the position and obligation of processors, following partly Article 17(2) of Directive 95/46/EC, and adding new elements, including that a processor that processes data beyond the controller's instructions is to be considered a co-controller.

Article 22 on processing under the authority of the controller and processor follows Article 16 of Directive 95/46/EC.

Article 23 introduces the obligation for controllers and processors to maintain documentation of all processing systems and procedures under their responsibility.

Article 24 concerns the keeping of records, in line with Article 10(1) of Framework Decision 2008/977, whilst providing further clarifications.

Article 25 clarifies the obligations of the controller and the processor regarding co-operation with the supervisory authority.

Article 26 concerns the cases where consultation with the supervisory authority is mandatory prior to the processing, based on Article 23 of Framework Decision 2008/977/JHA.

3.4.4.2. SECTION 2 DATA SECURITY

Article 27 on the security of processing is based on the current Article 17(1) of Directive 95/46 on the security of processing, and Article 22 of Framework Decision 2008/977/JHA, extending the related obligations to processors, irrespective of their contract with the controller.

Articles 28 and 29 introduce an obligation to notify personal data breaches, inspired by the personal data breach notification in Article 4(3) of the e-Privacy Directive 2002/58/EC, clarifying and separating the obligations to notify the supervisory authority (Article 28) and to communicate, in qualified circumstances, to the data subject (Article 29). Article 29 also provides for exemptions by referring to Article 11(4).

3.4.4.3. SECTION 3 DATA PROTECTION OFFICER

Article 30 introduces an obligation for the controller to appoint a mandatory data protection officer who should fulfil the tasks listed in Article 32. Where several competent authorities are acting under the supervision of a central authority, functioning as controller, at least this central authority should designate such a data protection officer. Article 18(2) of Directive

95/46/EC provided the possibility for Member States to introduce such requirement as a surrogate to the general notification requirement of that Directive.

Article 31 sets out the standing of the data protection officer.

Article 32 provides the tasks of the data protection officer.

3.4.5. *CHAPTER V - TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS*

Article 33 sets out the general principles for data transfers to third countries or international organisations in the area of police co-operation and judicial co-operation in criminal matters, including onward transfers. It clarifies that transfers to third countries may take place only if the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties..

Article 34 lays down that transfers to a third country may take place in relation to which the Commission has adopted an adequacy decision under Regulation ..../../201X or specifically in the area of police co-operation and judicial co-operation in criminal matters, or, in the absence of such decisions, where appropriate safeguards are in place. As long as adequacy decisions do not exist, the Directive ensures that transfers can continue to take place on the basis of appropriate safeguards and derogations. It furthermore sets out the criteria for the Commission's assessment of an adequate or not adequate level of protection, and expressly includes the rule of law, judicial redress and independent supervision. The article also provides for the possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country. It introduces that a general adequacy decision adopted, following the procedures under Article 38 of the General Data Protection Regulation, shall be applicable within the scope of this Directive. Alternatively an adequacy decision can be adopted by the Commission exclusively for the purposes of this Directive.

Article 35 defines the appropriate safeguards needed prior to international transfers, in the absence of a Commission adequacy decision. These safeguards may be adduced by a legally binding instrument such as an international agreement. Alternatively, the data controller may on the basis of an assessment of the circumstances surrounding the transfer conclude that they exist.

Article 36 spells out the derogations for data transfer based on Article 26 of Directive 95/46/EC and Article 13 of Framework Decision 2008/977/JHA.

Article 37 obliges Member States to provide that the controller informs the recipient of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met by recipients of the personal data in the third country or international organisation.

Article 38 explicitly provides for international co-operation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries, in particular those considered offering an adequate level of protection, taking into account the OECD's Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of 12 June 2007.

CHAPTER VI - NATIONAL SUPERVISORY AUTHORITIES

3.4.5.1. SECTION 1 INDEPENDENT STATUS

Article 39 obliges Member States to establish supervisory authorities, following Article 28(1) of Directive 95/46/EC and Article 25 Framework Decision 2008/977/JHA, enlarging the mission of these authorities to contribute to the consistent application of the Directive throughout the Union, which may be the supervisory authority established under the General Data Protection Regulation.

Article 40 clarifies the conditions for the independence of supervisory authorities, implementing case law of the Court of Justice of the EU[29], inspired also by Article 44 of Regulation (EC) No 45/2001[30].

Article 41 provides general conditions for the members of the supervisory authority, implementing the relevant case law[31], inspired also by Article 42(2)-(6) of Regulation (EC) 45/2001.

Article 42 sets out rules on the establishment of the supervisory authority, including on conditions for its members, to be provided by the Member States by law.

Article 43 on professional secrecy of the members and staff of the supervisory authority follows Article 28(7) of Directive 95/46/EC and Article 25(4) Framework Decision 2008/977/JHA.

3.4.5.2. SECTION 2 DUTIES AND POWERS

Article 44 sets out the competence of the supervisory authorities, based on Article 28(6) of Directive 95/46/EC and Article 25(1) Framework Decision 2008/977/JHA. Courts, when acting in their judicial authority, are exempted from the monitoring by the supervisory authority, but not from the application of the substantive rules on data protection.

Article 45 provides the obligation of Member States to provide for the duties of the supervisory authority, including hearing and investigating complaints and promoting the awareness of the public on risk, rules, safeguards and rights. A particular duty of the supervisory authorities in the context of this Directive is, where direct access is refused or restricted, to exercise the right of access on behalf of data subjects and to check the lawfulness of the data processing.

Article 46 provides the powers of the supervisory authority, based on Article 28(3) of Directive 95/46/EC, Article 25(2) and (3) of Framework Decision 2008/977/JHA.Article 47 obliges the supervisory authorities to draw up annual activity reports, based on Article 28(5) of Directive 95/46/EC.

---

29 Court of Justice of the EU, judgment of 9.3.2010, Commission / Germany (C-518/07, ECR 2010 p. I-1885)

30 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; OJ L 008 , 12/.01/.2001, p.1.

31 Op. cit., footnote 27.

3.4.6. CHAPTER VII – CO-OPERATION

Article 48 introduces rules on mandatory mutual assistance whereas Article 28 (6)2 of Directive 95/46/EC provided simply a general obligation to co-operate, without specifying further.

Article 49 provides that the European Data Protection Advisory Board, established by the General Data Protection Regulation, exercises its tasks also in relation to processing activities within the scope of this Directive. In order to provide complementary support, the Commission will seek the advice of representatives of authorities competent for the prevention, investigation, detection and prosecution of criminal penalties of the Member States, as well as representatives of Europol and Eurojust, by means of an expert group on the law-enforcement related aspects of data protection.

3.4.7. CHAPTER VIII - REMEDIES, LIABILITY AND SANCTIONS

Article 50 provides the right of any data subject to lodge a complaint with a supervisory authority, based on Article 28(4) of Directive 95/46/EC, and relates to any infringement of the Directive in relation to the complainant. It also specifies the bodies, organisations or associations which may lodge a complaint on behalf of the data subject and also in case of a personal data breach independently of a data subject's complaint.

Article 51 concerns the right to a judicial remedy against a supervisory authority. It builds on the general provision of Article 28(3) of Directive 95/46/EC and provides specifically that the data subject may launch a court action for obliging the supervisory authority to act on a complaint.

Article 52 concerns the right to a judicial remedy against a controller or processor, based on Article 22 of Directive 95/46/EC and Article 20 of Framework Decision 2008/977/JHA.

Article 53 introduces common rules for court proceedings, including the rights of bodies, organisations or associations to represent data subjects before the courts, and the right of supervisory authorities to engage in legal proceedings. The obligation of Member States to ensure rapid court actions is inspired by Article 18(1) of the e-Commerce Directive 2000/31/EC[32].

Article 54 obliges Member States to provide for the right to compensation. It builds on Article 23 of Directive 95/46/EC and Article 19(1) of Framework Decision 2008/977/JHA, extends this right on damages caused by processors and clarifies the liability of co-controllers and co-processors.

Article 55 obliges Member States to lay down rules on penalties, to sanction infringements of the Directive, and to ensure their implementation.

---

32 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'); OJ L 178, 17.7.2000, p. 1.

3.4.8. CHAPTER IX – DELEGATED ACTS AND IMPLEMENTING ACTS

Article 56 contains standard provisions for the exercise of delegations in line with Article 290 TFEU. This allows the legislator to delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act (quasi-legislative acts).

Article 57 contains the provision for the Committee procedure needed for conferring implementing powers on the Commission in cases where, in accordance with Article 291 TFEU, uniform conditions for implementing legally binding acts of the Union are needed. The examination procedure applies.

3.4.9. CHAPTER X – FINAL PROVISIONS

Article 58 repeals Framework Decision 2008/977/JHA.

Article 59 sets out that specific provisions with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in Union acts, regulating the processing of personal data or the access to information systems within the scope of the Directive, and adopted prior to the adoption of this Directive, remain unaffected.

Article 60 clarifies the relationship of this Directive with previously concluded international agreements by Member States in the field of judicial co-operation in criminal matters and police co-operation.

Article 61 provides for the obligation of the Commission to evaluate and report on the implementation of the Directive, in order to assess the need to align the previously adopted specific provisions referred to in Article 59 with this Directive.

Article 62 sets out the obligation of the Member States to transpose the Directive in their national law and notify to the Commission the provisions adopted pursuant to the Directive.

Article 63 determines the date of the entry into force of the Directive.

Article 64 lays down the addressees of this Directive.

4. BUDGETARY IMPLICATIONS

The legislative financial statement accompanying the proposal for the General Data Protection Regulation covers the budgetary impacts for the Regulation and this Directive.

2012/0010 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

After consulting the European Data Protection Supervisor[33],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her.

(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows competent authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

---

33 OJ C... , p. .

(4) This requires facilitating the free flow of data between competent authorities within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[34] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation.

(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[35] applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

(8) Article 16(2) of the Treaty on the Functioning of the European Union provides that the European Parliament and the Council should lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) On that basis, Regulation EU ...../2012 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect of individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the Conference acknowledged that specific rules on the protection of personal data and the free

---

34 OJ L 281, 23.11.1995, p. 31.
35 OJ L 350, 30.12.2008, p. 60.

movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.

(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data in the areas of judicial co-operation in criminal matters and police co-operation.

(13) This Directive allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Directive.

(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.

(15) The protection of individuals should be technological neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Directive. This Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, in particular concerning national security, or to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust.

(16) The principles of protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

(17) Personal data relating to health should include in particular all data pertaining to the health status of a data subject, information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on, for example; a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

(18) Any processing of personal data must be fair and lawful in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit.

(19) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to retain and process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.

(20) Personal data should not be processed for purposes incompatible with the purpose for which it was collected. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. Every reasonable step should be taken to ensure that personal data which are inaccurate should be rectified or erased.

(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(22) In the interpretation and application of the general principles relating to personal data processing by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, account should be taken of the specificities of the sector, including the specific objectives pursued.

(23) It is inherent to the processing of personal data in the areas of judicial co-operation in criminal matters and police co-operation that personal data relating to different categories of data subjects are processed. Therefore a clear distinction should as far as possible be made between personal data of different categories of data subjects such as suspects, persons convicted of a criminal offence, victims and third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals.

(24) As far as possible personal data should be distinguished according to the degree of their accuracy and reliability. Facts should be distinguished from personal assessments, in order to ensure both the protection of individuals and the quality and reliability of the information processed by the competent authorities.

(25) In order to be lawful, the processing of personal data should be necessary for compliance with a legal obligation to which the controller is subject, for the performance of a task carried out in the public interest by a competent authority based on law or in order to protect the vital interests of the data subject or of another person, or for the prevention of an immediate and serious threat to public security.

(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights or privacy, including genetic data, deserve specific protection.

Such data should not be processed, unless processing is specifically authorised by a law which provides for suitable measures to safeguard the data subject's legitimate interests; or processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject.

(27) Every natural person should have the right not to be subject to a measure which is based solely on automated processing if it produces an adverse legal effect for that person, unless authorised by law and subject to suitable measures to safeguard the data subject's legitimate interests.

(28) In order to exercise their rights, any information to the data subject should be easily accessible and easy to understand, including the use of clear and plain language.

(29) Modalities should be provided for facilitating the data subject's exercise of their rights under this Directive, including mechanisms to request, free of charge, in particular access to data, rectification and erasure. The controller should be obliged to respond to requests of the data subject without undue delay.

(30) The principle of fair processing requires that the data subjects should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

(31) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not obtained from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.

(32) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, for what period, which recipients receive the data, including in third countries Data subjects should be allowed to receive a copy of their personal data which are being processed.

(33) Member States should be allowed to adopt legislative measures delaying, restricting or omitting the information of data subjects or the access to their personal data to the extent that and as long as such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties, to protect public security or national security, or, to protect the data subject or the rights and freedoms of others.

(34) Any refusal or restriction of access should be set out in writing to the data subject including the factual or legal reasons on which the decision is based.

(35) Where Member States have adopted legislative measures restricting wholly or partly the right to access, the data subject should have the right to request that the competent national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When access is exercised by the supervisory authority on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications by the supervisory authority have taken place and of the result as regards to the lawfulness of the processing in question.

(36) Any person should have the right to have inaccurate personal data concerning them rectified and the right of erasure where the processing of such data is not in compliance with the main principles laid down in this Directive. Where the personal data are processed in the course of a criminal investigation and proceedings,, rectification, the rights of information, access, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.

(37) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure the compliance of processing operations with the rules adopted pursuant to this Directive.

(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to ensure compliance with the provisions adopted pursuant to this Directive, the controller should adopt policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.

(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear attribution of the responsibilities under this Directive, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(40) Processing activities should be documented by the controller or processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation available upon request, so that it might serve for monitoring processing operations. .

(41) In order to ensure effective protection of the rights and freedoms of data subjects by way of preventive actions, the controller or processor should consult with the supervisory authority in certain cases prior to the processing.

(42) A personal data breach may, if not addressed in an adequate and timely manner, result in harm, including reputational damage to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The individuals whose personal data or privacy could be adversely affected by the breach should be notified without undue

delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of an individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the processing of personal data.

(43) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of misuse. Moreover, such rules and procedures should take into account the legitimate interests of competent authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(44) The controller or the processor should designate a person who would assist the controller or processor to monitor compliance with the provisions adopted pursuant to this Directive. A data protection officer may be appointed jointly by several entities of the competent authority. The data protection officers must be in a position to perform their duties and tasks independently and effectively.

(45) Member States should ensure that a transfer to a third country only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced.

(46) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how the rule of law, access to justice, as well as international human rights norms and standards, in that third country are respected.

(48) The Commission should equally be able to recognise that a third country, or a territory or a processing sector within a third country, or an international organisation, does not offer an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards or on the basis of a derogation laid down in the Directive.

(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims.

(50) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions pursuant to this Directive and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

(52) Member States may entrust a supervisory authority already established in Member States under Regulation (EU)..../2012 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with adequate financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.

(54) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.

(55) While this Directive applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when they are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law.

(56) In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have the same duties and effective powers in each Member State, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings.

(57) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

(58) The supervisory authorities should assist one another in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(59) The European Data Protection Board established by Regulation (EU)..../2012 should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the co-operation of the supervisory authorities throughout the Union.

(60) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Directive are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(61) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint or exercise the right to a judicial remedy on behalf of data subjects if duly mandated by them, or to lodge, independently of a data subject's complaint, its own complaint where it considers that a personal data breach has occurred.

(62) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established.

(63) Member States should ensure that court actions, in order to be effective, allow the rapid adoption of measures to remedy or prevent an infringement of this Directive.

(64) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where they establish fault on the part of the data subject or in case of force majeure.

(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.

(66) In order to fulfil the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of notifications of a personal data breach to the supervisory authority. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

(67) In order to ensure uniform conditions for the implementation of this Directive as regards documentation by controllers and processors, security of processing, notably in relation to encryption standards, notification of a personal data breach to the supervisory authority, and the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[36].

(68) The examination procedure should be used for the adoption of measures as regards documentation by controllers and processors, security of processing, notification of a personal data breach to the supervisory authority, and the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation, given that those acts are of general scope.

(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection, imperative grounds of urgency so require.

(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by

---

36 OJ L 55, 28.2.2011, p. 13.

reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective

(71) Framework Decision 2008/977/JHA should be repealed by this Directive.

(72) Specific provisions with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected. The Commission should evaluate the situation with regard to the relation between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive.

(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by Member States prior to the entry force of this Directive should be amended in line with this Directive.

(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011.[37]

(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland shall not be bound by the rules laid down in this Directive where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.

(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by this Directive or subject to its application. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.

(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of

---

37 OJ L335, 17.12.2011, p. 1.

the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[38].

(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[39].

(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[40].

(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(81) In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.

---

38 OJ L 176, 10.7.1999, p. 36.
39 OJ L 53, 27.2.2008, p. 52.
40 OJ L 160 of 18.6.2011, p. 19.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and objectives

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

2. In accordance with this Directive, Member States shall:

   (a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and

   (b) ensure that the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Article *2*
Scope

1. This Directive applies to the processing of personal data by competent authorities for the purposes referred to in Article 1(1).

2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

3. This Directive shall not apply to the processing of personal data:

   (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;

   (b) by the Union institutions, bodies, offices and agencies.

Article 3
Definitions

For the purposes of this Directive:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an

identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information relating to a data subject;

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(5) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(6) 'controller' means the competent public authority which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(8) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13) 'child' means any person below the age of 18 years;

(14) 'competent authorities' means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(15) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 39.

CHAPTER II
PRINCIPLES

Article 4
Principles relating to personal data processing

Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed;

(f) processed under the responsibility and liability of the controller, who shall ensure compliance with the provisions adopted pursuant to this Directive.

.

Article 5
Distinction between different categories of data subjects

1. Member States shall provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;

(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal

offences, or a contact or associate to one of the persons mentioned in (a) and (b); and

(e) persons who do not fall within any of the categories referred to above.

Article 6
Different degrees of accuracy and reliability of personal data

1. Member States shall ensure that, as far as possible, the different categories of personal data undergoing processing are distinguished in accordance with their degree of accuracy and reliability.

2. Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments.

Article 7
Lawfulness of processing

Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary:

(a) for the performance of a task carried out by a competent authority, based on law for the purposes set out in Article 1(1); or

(b) for compliance with a legal obligation to which the controller is subject; or

(c) in order to protect the vital interests of the data subject or of another person; or

(d) for the prevention of an immediate and serious threat to public security.

Article 8
Processing of special categories of personal data

1. Member States shall prohibit the processing of personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, of genetic data or of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the processing is authorised by a law providing appropriate safeguards; or

(b) the processing is necessary to protect the vital interests of the data subject or of another person; or

(c) the processing relates to data which are manifestly made public by the data subject.

Article 9

Measures based on profiling and automated processing

1. Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 10

Modalities for exercising the rights of the data subject

1. Member States shall provide that the controller takes all reasonable steps to have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of the data subjects' rights.

2. Member States shall provide that any information and any communication relating to the processing of personal data are to be provided by the controller to the data subject in an intelligible form, using clear and plain language.

3. Member States shall provide that the controller takes all reasonable steps to establish procedures for providing the information referred to in Article 11 and for the exercise of the rights of data subjects referred to in Articles 12 to 17.

4. Member States shall provide that the controller informs the data subject about the follow-up given to their request without undue delay.

5. Member States shall provide that the information and any action taken by the controller following a request referred to in paragraphs 3 and 4 are free of charge. Where requests are vexatious, in particular because of their repetitive character, or the size or volume of the request, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the vexatious character of the request.

Article 11

Information to the data subject

1. Where personal data relating to a data subject are collected, Member States shall ensure that the controller takes all appropriate measures to provide the data subject with at least the following information:

(a) the identity and the contact details of the controller and of the data protection officer;

(b) the purposes of the processing for which the personal data are intended;

(c) the period for which the personal data will be stored;

(d) the existence of the right to request from the controller access to and rectification, erasure or restriction of processing of the personal data concerning the data subject;

(e) the right to lodge a complaint to the supervisory authority referred to in Article 39 and its contact details;

(f) the recipients or categories of recipients of the personal data, including in third countries or international organisations;

(g) any further information in so far as such further information is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

3. The controller shall provide the information referred to in paragraph 1:

(a) at the time when the personal data are obtained from the data subject, or

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.

4. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject to the extent that, and as long as, such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned:

(a) to avoid obstructing official or legal inquiries, investigations or procedures ;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;

(c) to protect public security;

(d) to protect national security;

(e) to protect the rights and freedoms of others.

5. Member States may determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 4.

Article 12
Right of access for the data subject

1. Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data relating to them are being processed. Where such personal data are being processed, the controller shall provide the following information:

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

   (c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular the recipients in third countries;

   (d) the period for which the personal data will be stored;

   (e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;

   (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

   (g) communication of the personal data undergoing processing and of any available information as to their source.

2. Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing.

Article 13
Limitations to the right of access

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned:

   (a) to avoid obstructing official or legal inquiries, investigations or procedures;

   (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties;

   (c) to protect public security;

   (d) to protect national security;

   (e) to protect the rights and freedoms of others.

2. Member States may determine by law categories of data processing which may wholly or partly fall under the exemptions of paragraph 1.

3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject in writing on any refusal or restriction of access, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. The information on factual or legal reasons on which the decision is based may be omitted where the provision of such information would undermine a purpose under paragraph 1.

4. Member States shall ensure that the controller documents the grounds for omitting the communication of the factual or legal reasons on which the decision is based.

Article 14
Modalities for exercising the right of access

1. Member States shall provide for the right of the data subject to request, in particular in cases referred to in Article 13, that the supervisory authority checks the lawfulness of the processing.

2. Member State shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1.

3. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.

Article 15
Right to rectification

1. Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, in particular by way of a corrective statement.

2. Member States shall provide that the controller informs the data subject in writing on any refusal of rectification, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

Article 16
Right to erasure

1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e), 7 and 8 of this Directive.

2. The controller shall carry out the erasure without delay.

3. Instead of erasure, the controller shall mark the personal data where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the personal data have to be maintained for purposes of proof;

(c) the data subject opposes their erasure and requests the restriction of their use instead.

4. Member States shall provide that the controller informs the data subject in writing of any refusal of erasure or marking of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

Article 17
Rights of the data subject in criminal investigations and proceedings

Member States may provide that the rights of information, access, rectification, erasure and restriction of processing referred to in Articles 11 to 16 are carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 18
Responsibility of the controller

1. Member States shall provide that the controller adopts policies and implements appropriate measures to ensure that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive.

2. The measures referred to in paragraph 1 shall in particular include:

(a) keeping the documentation referred to in Article 23;

(b) complying with the requirements for prior consultation pursuant to Article 26;

(c) implementing the data security requirements laid down in Article 27;

(d) designating a data protection officer pursuant to Article 30.

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraph 1 of this Article. If proportionate, this verification shall be carried out by independent internal or external auditors.

Article 19
Data protection by design and by default

1. Member States shall provide that, having regard to the state of the art and the cost of implementation, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed.

Article 20
Joint controllers

Member States shall provide that where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers must determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Article 21
Processor

1. Member States shall provide that where a processing operation is carried out on behalf of a controller, the controller must choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.

2. Member States shall provide that the carrying out of processing by a processor must be governed by a legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited.

3. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 20.

Article 22
Processing under the authority of the controller and processor

Member States shall provide that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, may only process them on instructions from the controller or where required by Union or Member State law.

Article 23
Documentation

1. Member States shall provide that each controller and processor maintains documentation of all processing systems and procedures under their responsibility.

2. The documentation shall contain at least the following information:

   (a) the name and contact details of the controller, or any joint controller or processor;

   (b) the purposes of the processing;

   (c) the recipients or categories of recipients of the personal data;

   (d) transfers of data to a third country or an international organisation, including the identification of that third country or international organisation.

3. The controller and the processor shall make the documentation available, on request, to the supervisory authority.

Article 24
Keeping of records

1. Member States shall ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show in particular the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed personal data.

2. The records shall be used solely for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security.

Article 25
Cooperation with the supervisory authority

1. Member States shall provide that the controller and the processor shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing all information necessary for the supervisory authority to perform its duties.

2. In response to the supervisory authority's exercise of its powers under points (a)and (b) of Article 46, the controller and the processor shall reply to the supervisory authority within a reasonable period. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

Article 26
Prior consultation of the supervisory authority

1. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data which will form part of a new filing system to be created where:

   (a) special categories of data referred to in Article 8 are to be processed;

   (b) the type of processing, in particular using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.

2. Member States may provide that the supervisory authority establishes a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

SECTION 2
DATA SECURITY

Article 27
Security of processing

1. Member States shall provide that the controller and the processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks, implements measures designed to:

   (a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

   (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

   (c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

   (d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

   (e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

   (f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, notably encryption standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

Article 28

Notification of a personal data breach to the supervisory authority

1. Member States shall provide that in the case of a personal data breach, the controller notifies, without undue delay and, where feasible, not later than 24 hours after having become aware of it, the personal data breach to the supervisory authority. The controller shall provide, on request, to the supervisory authority a reasoned justification in cases where the notification is not made within 24 hours.

2. The processor shall alert and inform the controller immediately after having become aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) communicate the identity and contact details of the data protection officer referred to in Article 30 or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

(d) describe the possible consequences of the personal data breach;

(e) describe the measures proposed or taken by the controller to address the personal data breach.

4. Member States shall provide that the controller documents any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

Article 29
Communication of a personal data breach to the data subject

1. Member States shall provide that when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 28(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the personal data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. The communication to the data subject may be delayed, restricted or omitted on the grounds referred to in Article 11(4).

SECTION 3
DATA PROTECTION OFFICER

Article 30
Designation of the data protection officer

1. Member States shall provide that the controller or the processor designates a data protection officer.

2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32.

3. The data protection officer may be designated for several entities, taking account of the organisational structure of the competent authority.

Article 31
Position of the data protection officer

1. Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or processor shall ensure that the data protection officer is provided with the means to perform duties and tasks referred to under Article 32 effectively and independently, and does not receive any instructions as regards the exercise of the function.

Article 32
Tasks of the data protection officer

Member States shall provide that the controller or the processor entrusts the data protection officer at least with the following tasks:

(a) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations and the related audits;

(c) to monitor the implementation and application of the provisions adopted pursuant to this Directive, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under the provisions adopted pursuant to this Directive;

(d) to ensure that the documentation referred to in Article 23 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 28 and 29;

(f) to monitor the application for prior consultation to the supervisory authority, if required pursuant to Article 26 ;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on his own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative.

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 33
General principles for transfers of personal data

Member States shall provide that any transfer of personal data by competent authorities that is undergoing processing or is intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:

(a) the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and

(b) the conditions laid down in this Chapter are complied with by the controller and processor.

Article 34
Transfers with an adequacy decision

1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) ..../2012 or in accordance with paragraph 3 of this Article that the third country or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.

2. Where no decision adopted in accordance with Article 41 of Regulation (EU) ..../2012 exists, the Commission shall assess the adequacy of the level of protection, giving consideration to the following elements:

(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law as well as the security measures which are complied with in that country or by that international organisation; as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subject in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation in question has entered into.

3. The Commission may decide, within the scope of this Directive, that a third country or a territory or a processing sector within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

5. The Commission may decide within the scope of this Directive that a third country or a territory or a processing sector within that third country or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 57(3).

6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, that any transfer of personal data to the third country or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, this decision shall be without prejudice to transfers under Article 35(1) or in accordance with Article 36. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country or an international organisation where it has decided that an adequate level of protection is or is not ensured.

8. The Commission shall monitor the application of the implementing acts referred to in paragraphs 3 and 5.

Article 35
Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 34, Member States shall provide that a transfer of personal data to a recipient in a third country or an international organisation may take place where:

(a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument; or

(b) the controller or processor has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data.

1. The decision for transfers under paragraph 1 (b) must be made by duly authorised staff. These transfers must be documented and the documentation must be made available to the supervisory authority on request.

Article 36
Derogations

By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:

(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or

(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or

(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or

(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or

(e) the transfer is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.

Article 37
Specific conditions for the transfer of personal data

Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met.

Article 38
International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 34(3).

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 39
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission.

2. Member States may provide that the supervisory authority established in Member States pursuant to Regulation (EU)..../2012 assumes responsibility for the tasks of the supervisory authority to be established pursuant to paragraph 1 of this Article.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board.

Article 40
Independence

1. Member States shall ensure that the supervisory authority acts with complete independence in exercising the duties and powers entrusted to it.

2. Each Member State shall provide that the members of the supervisory authority, in the performance of their duties, neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.

6 Each Member State shall ensure that the supervisory authority must have its own staff which shall be appointed by and subject to the direction of the head of the supervisory authority.

7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.

Article 41
General conditions for the members of the supervisory authority

1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties are demonstrated.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.

4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.

5. Where the term of office expires or the member resigns, the member shall continue to exercise their duties until a new member is appointed.

Article 42
Rules on the establishment of the supervisory authority

Each Member State shall provide by law:

(a) the establishment and status of the supervisory authority in accordance with Articles 39 and 40;

(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;

(c) the rules and procedures for the appointment of the members of the supervisory authority, as well as the rules on actions or occupations incompatible with the duties of the office;

(d) the duration of the term of the members of the supervisory authority, which shall be no less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period;

(e) whether the members of the supervisory authority shall be eligible for reappointment;

(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;

(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including where they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

Article 43
Professional secrecy

Member States shall provide that the members and the staff of the supervisory authority are subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

SECTION 2
DUTIES AND POWERS

Article 44
Competence

1. Member States shall provide that each supervisory authority exercises, on the territory of its own Member State, the powers conferred on it in accordance with this Directive.

2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of courts when acting in their judicial capacity.

Article 45
Duties

1. Member States shall provide that the supervisory authority:

(a) monitors and ensures the application of the provisions adopted pursuant to this Directive and its implementing measures;

(b) hears complaints lodged by any data subject, or by an association representing and duly mandated by that data subject in accordance with Article 50, investigates, to the extent appropriate, the matter and informs the data subject the association of the progress and the outcome of the complaint within a reasonable period, in particular where further investigation or coordination with another supervisory authority is necessary;

(c) checks the lawfulness of data processing pursuant to Article 14, and informs the data subject within a reasonable period on the outcome of the check or on the reasons why the check has not been carried out;

(d) provides mutual assistance to other supervisory authorities and ensures the consistency of application and enforcement of the provisions adopted pursuant to this Directive;

(e) conducts investigations either on its own initiative or on the basis of a complaint, or on request of another supervisory authority, and informs the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable period;

(f) monitors relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(g) is consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(h) is consulted on processing operations pursuant to Article 26;

(i) participates in the activities of the European Data Protection Board.

2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights laid down in provisions adopted pursuant to this Directive, and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.

5. Member States shall provide that the performance of the duties of the supervisory authority shall be free of charge for the data subject.

6. Where requests are vexatious, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action required by the data subject. The supervisory authority shall bear the burden of proving of the vexatious character of the request.

Article 46
Powers

Member States shall provide that each supervisory authority must in particular be endowed with:

(a) investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;

(b) effective powers of intervention, such as the delivering of opinions before processing is carried out, and ensuring appropriate publication of such opinions, ordering the restriction, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or admonishing the controller, or referring the matter to national parliaments or other political institutions ;

(c) the power to engage in legal proceedings where the provisions adopted pursuant to this Directive have been infringed or to bring this infringement to the attention of the judicial authorities.

Article 47
Activities report

Member States shall provide that each supervisory authority draws up an annual report on its activities. The report shall be made available to the Commission and the European Data Protection Board.

CHAPTER VII
CO-OPERATION

Article 48
Mutual assistance

1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions pursuant to this Directive in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior consultations, inspections and investigations.

2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority.

3. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.

Article 49

Tasks of the European Data Protection Board

1. The European Data Protection Board established by Regulation (EU)..../2012 shall exercise the following tasks in relation to processing within the scope of this Directive:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

(b) examine, on request of the Commission or on its own initiative or of one of its members, any question covering the application of the provisions adopted pursuant to this Directive and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of those provisions;

(c) review the practical application of guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;

(d) give the Commission an opinion on the level of protection in third countries or international organisations;

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) promote the exchange of knowledge and documentation with data protection supervisory authorities worldwide, including data protection legislation and practice.

2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 57(1) and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

CHAPTER VIII
REMEDIES, LIABILITY AND SANCTIONS

Article 50
Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for the right of every data subject to lodge a complaint with a supervisory authority in any Member State, if they consider that the processing of personal data relating to them does not comply with provisions adopted pursuant to this Directive.

2. Member States shall provide for the right of any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and is being properly constituted according to the law of a Member State to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects, if it considers that a data subject's rights under this Directive have been infringed as a result of the processing of personal data. The organisation or association must be duly mandated by the data subject(s).

3. Member States shall provide for the right of any body, organisation or association referred to in paragraph 2, independently of a data subject's complaint, to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

Article 51
Right to a judicial remedy against a supervisory authority

1. Member States shall provide for the right to a judicial remedy against decisions of a supervisory authority.

2. Each data subject shall have the right to a judicial remedy for obliging the supervisory authority to act on a complaint, in the absence of a decision which is necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 45(1).

3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

Article 52
Right to a judicial remedy against a controller or processor

Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority, Member States shall provide for the right of every natural person to a judicial remedy if they consider that that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.

Article 53
Common rules for court proceedings

1. Member States shall provide for the right of any body, organisation or association referred to in Article 50(2) to exercise the rights referred to in Articles 51 and 52 on behalf of one or more data subjects.

2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions adopted pursuant to this Directive or to ensure consistency of the protection of personal data within the Union.

3. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

Article 54
Liability and the right to compensation

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with the provisions adopted pursuant to this Directive shall have the right to receive compensation from the controller or the processor for the damage suffered.

2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.

3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or processor proves that they are not responsible for the event giving rise to the damage.

Article 55
Penalties

Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

CHAPTER IX
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 56
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 28(5) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Directive.

3. The delegation of power referred to in Article 28(5) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 28(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or the Council.

Article 57
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER X
FINAL PROVISIONS

Article 58
Repeals

1. Council Framework Decision 2008/977/JHA is repealed.

2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.

Article 59
Relation with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation

The specific provisions for the protection of personal data with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected.

Article 60
Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation

International agreements concluded by Member States prior to the entry force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.

Article 61
Evaluation

1. The Commission shall evaluate the application of this Directive.

2. The Commission shall review within three years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in particular those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive.

3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry

into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Directive and aligning other legal instruments. The report shall be made public.

Article 62
Implementation

1. Member States shall adopt and publish, by [date/ two years after entry into force] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions.

   They shall apply those provisions from xx.xx.201x [date/ two years after entry into force].

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 63
Entry into force and application

This Directive shall enter into force on the first day following that of its publication in the *Official Journal of the European Union.*

Article 64
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 25.1.2012

For the European Parliament
The President

For the Council
The President

Public Safety Canada | Sécurité publique Canada

An Intro to Cyber Security and NCSD

From Policy to Protection In 60 Minutes Or Less

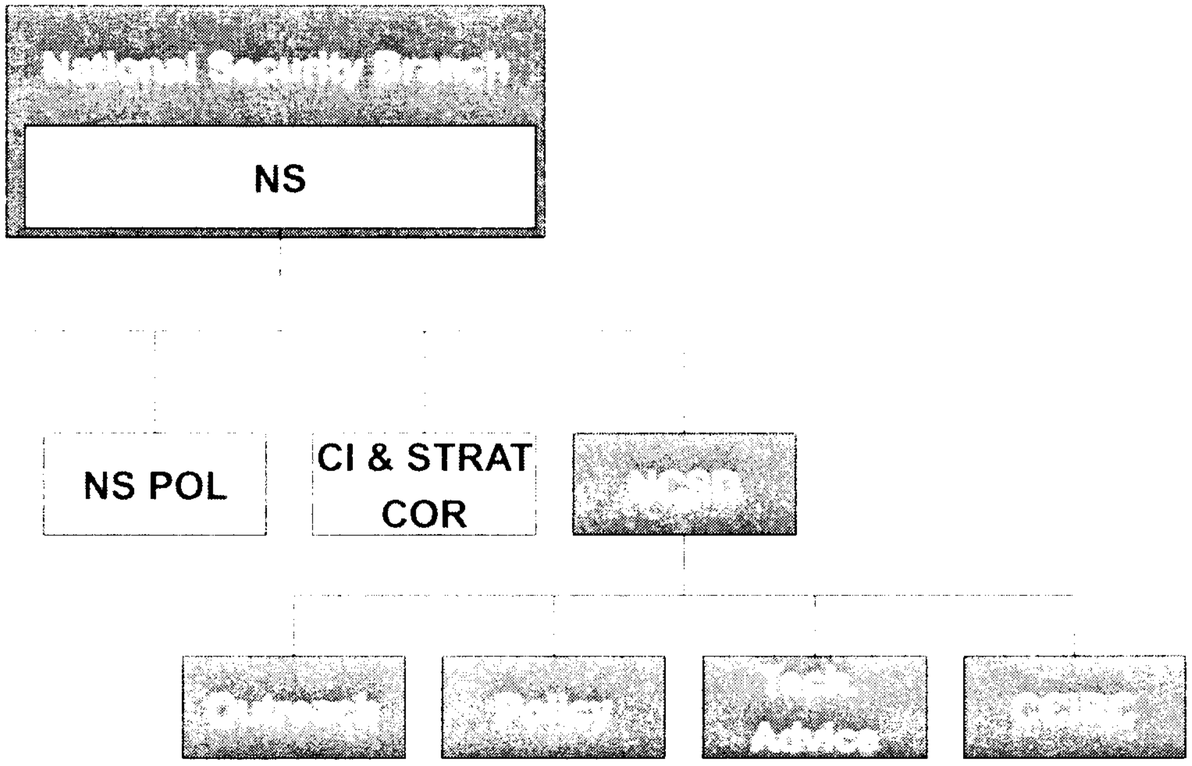
Generic Deck

Canada

An Intro To Cyber Security

- Who we are, what we do
- High level overview of the strategy
- Roles and responsibilities within Government for Cyber
- The threat landscape – incidents related initiatives and other challenges
- Basic Advice
- Q&A

National Cyber Security Directorate (NCSD)



- DG – Robert Dick
- Head of Cyber Strategy – Bob Gordon
- ~ 40 in total (with casuals, contractors, and indeterminate staff)
- AS', ECs, CS', and PMs

What we do? (1/2)

- Outreach
  - Responsible for engaging with partners outside of the Federal Government (P/Ts, Industry etc.)
- Policy
  - Responsible for developing leading edge policy and high level briefings on all things related to cyber

What we do? (2/2)

- Technical Advice
  - Responsible for providing leading technical advice and briefings to Outreach, Policy and the Departments senior executives
- CCIRC
  - Canada's Computer Emergency Readiness Team
    - Incident response (P/T/ CI & Industry)
    - Technical analysis
    - Information sharing and product generation (SA)

Canada's Cyber Security Strategy

- Signals cyber security as a priority for the Government of Canada.

- Commits investment by the Government in resources.

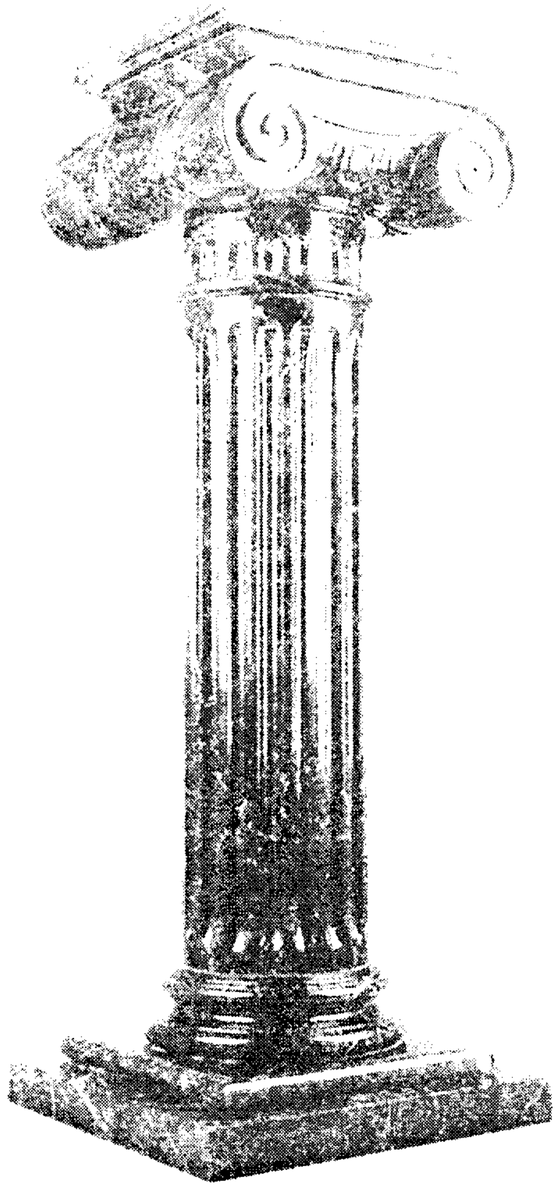
- Coordinates and unifies domestic and international action.

Canada's Cyber Security Strategy

- Launched in October 2010
- Built on three pillars:

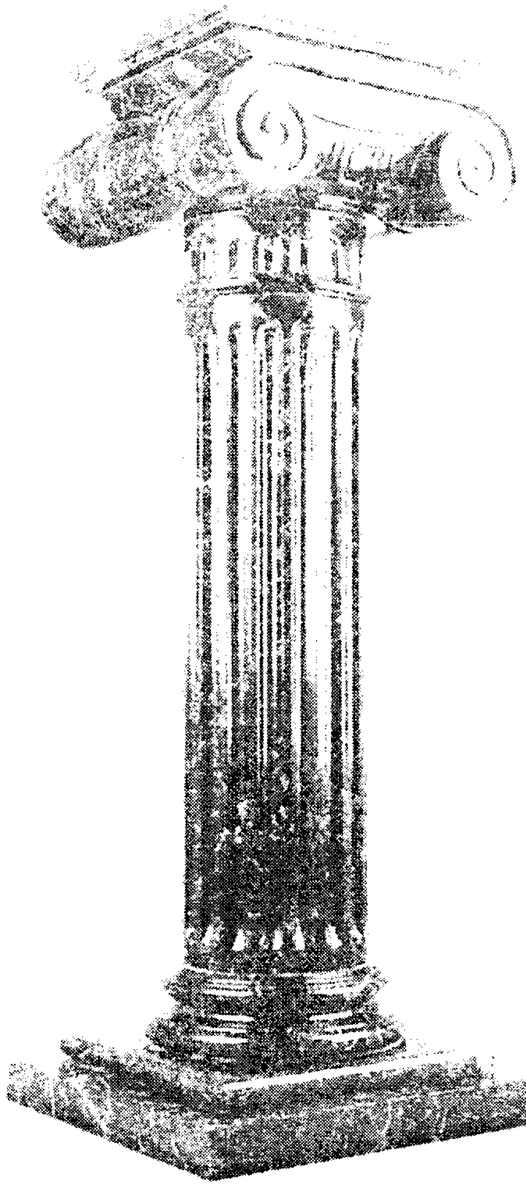
1. Secure Government systems
2. Partner to secure systems outside the Government of Canada
3. Help Canadians to be secure online

Pillar 1: Secure Government systems



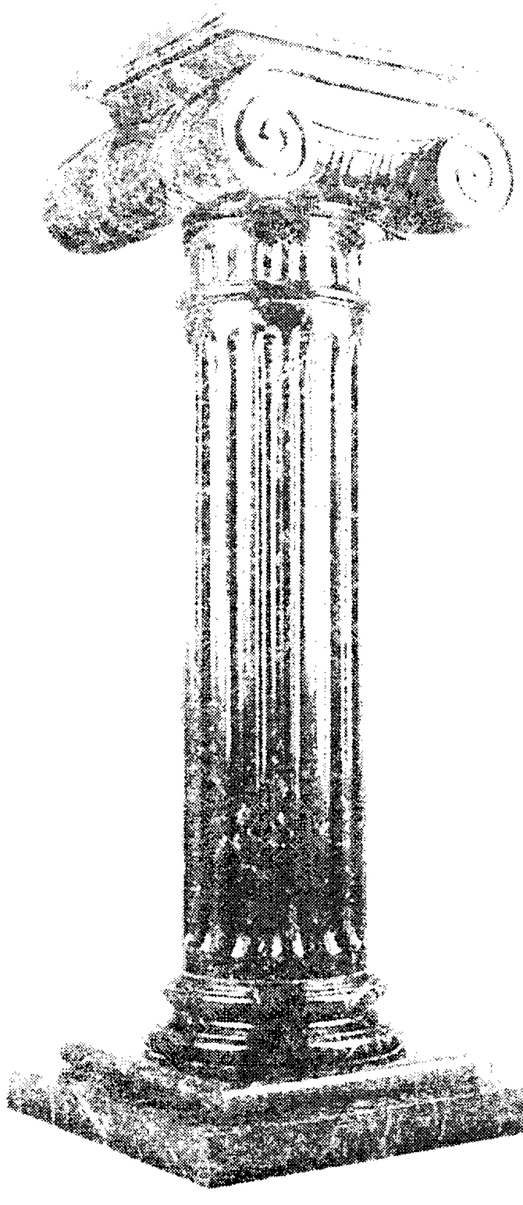
- Establish clear federal roles and responsibilities.
- Strengthen the security of federal cyber systems.
- Enhance cyber security awareness throughout Government.

Pillar 2: Partner to secure systems outside the Government of Canada



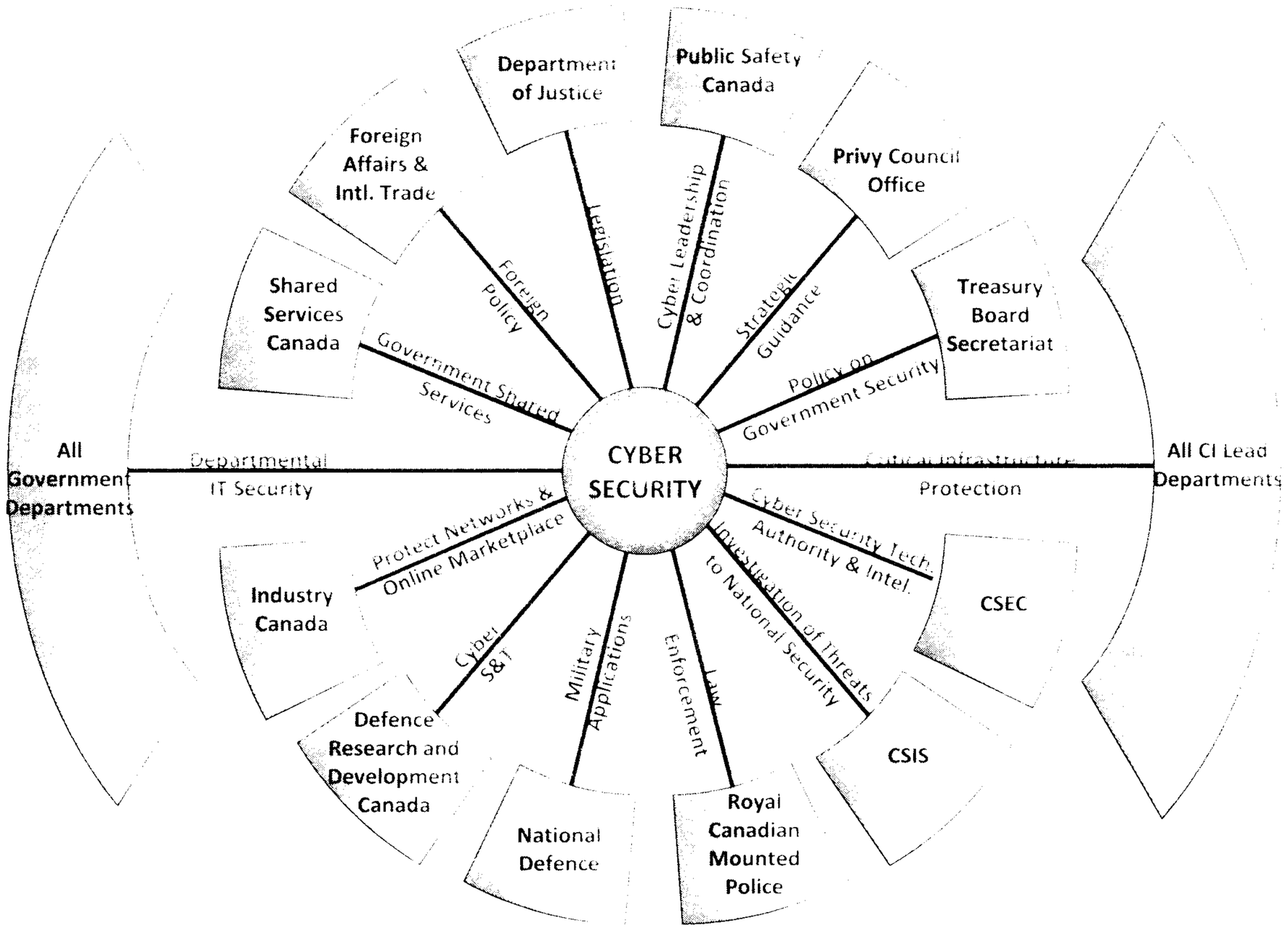
- Partner with the provinces and territories, the private and academic sectors, and international partners.
- Develop leading-edge cyber security science and technology, and innovative research and development.
- Leverage and build upon public-private partnerships to secure critical infrastructure and promote awareness.

Pillar 3: Help Canadians to be secure online



- Canadians need three things to be secure online:
  - Awareness of the need to act
  - Information about how to act
  - Protection from those that act criminally

Key Players At The Federal Level



Canadian Cyber Incident Response Centre (CCIRC)

- Pre June 20, 2011 were the place to call for government cyber security incidents
- This role is now taken on by CSEC
- Now CCIRC is transitioning to be a national CERT for Canada where they will support other levels of government as well as the private and public sectors.

Understanding Cyber Threats

- Basic Hackers and Script Kiddies
  - High frequency, low threat
  - Usually for fame, protest or attention
  - Typically not that sophisticated
- Criminal for Profit Actors
  - Fairly frequent and more sophisticated
  - More common than you may think
  - Highly profitable
- Insider Threat
  - Where to begin…
- Advanced Persistent Threats
  - The most sophisticated
  - Low frequency, high potential impact

Recent Incidents for Fame / Protest

PBS: Hacked. Tupac Shakur: Still Dead (Update: PBS Issues Statement)

HBGary Federal Hacked by Anonymous

239

Stratfor Hack: Anonymous Affiliated Hackers Publish Thousands Of Credit Card Numbers

BUSINESS CENTER

Sony Hacked Again: How Not to Do Network Security

guardian

LulzSec Hacks Arizona Police in Retaliation for Racial Profiling

News Technology Hacking

Hacking of Fox News claimed by group with links to Anonymous

IMF Hacked: No End in Sight to Security Horror Shows

LulzSec leaks 62,000 emails and passwords, also targets CIA

Hacker Exposes Perils of Remote Voting Machines

For Profit: Breaches / Hacks / SPAM

- The underground market for stolen information and illicit goods is booming
- Here are some examples:
  - Carders Gone Wild: Gonzalez and Max Vision
  - Search Poisoning
  - Rogue Pharmacy
  - Fake Antivirus Scams

Criminal for Profit Actors: Carders Gone Wild

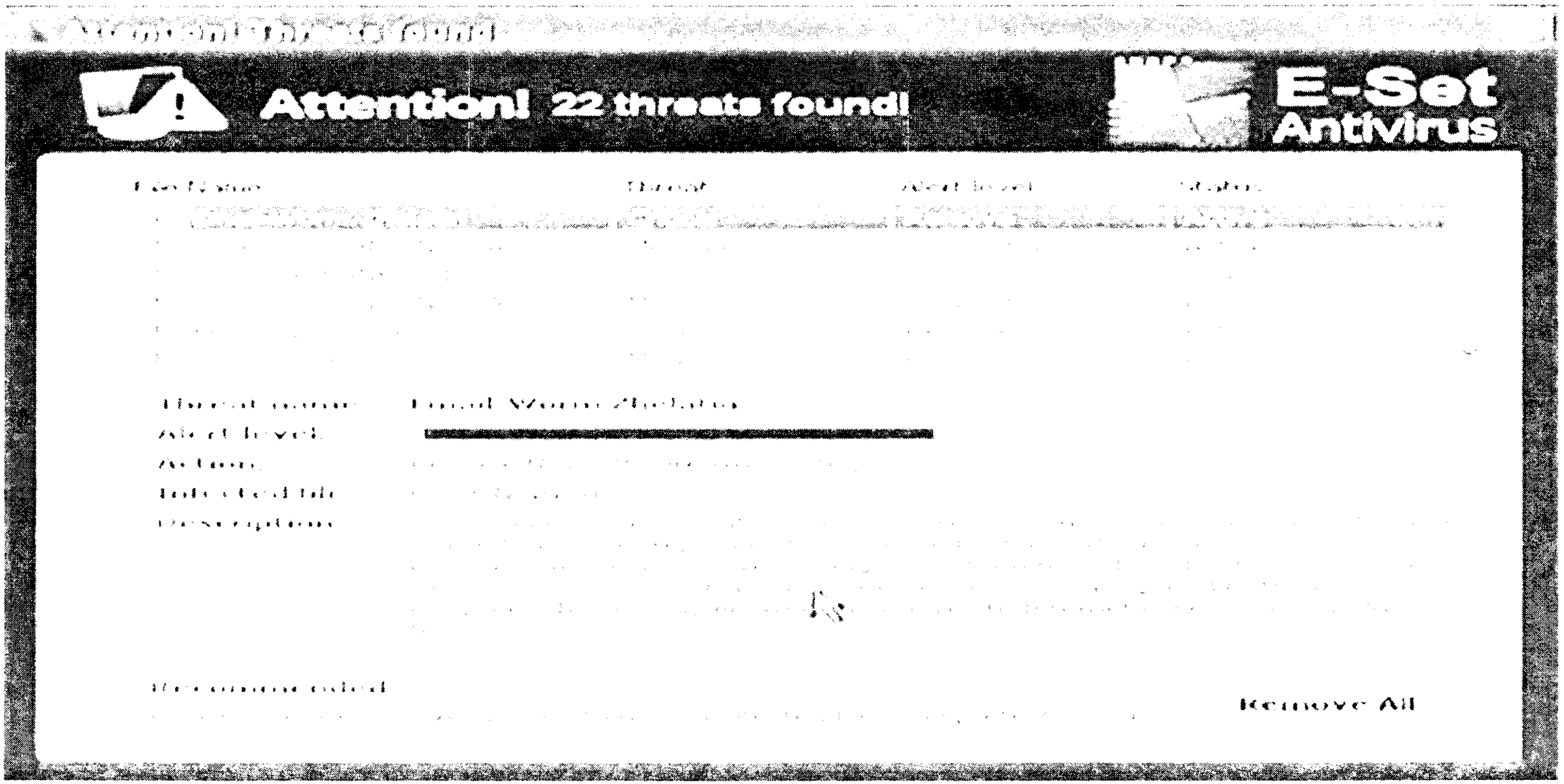
THREAT LEVEL

Record 13-Year Sentence for Hacker Max Vision

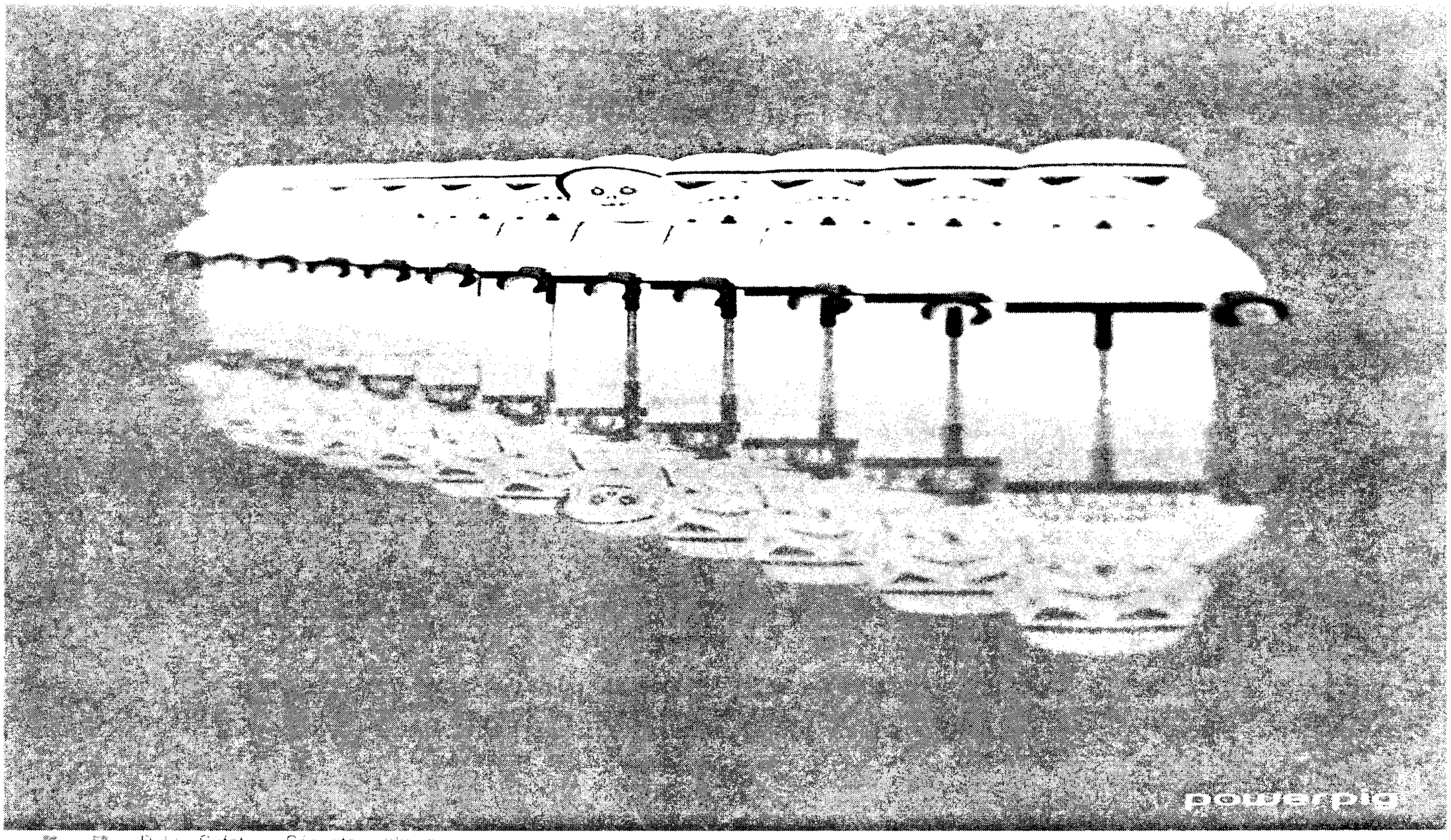
Criminal for Profit Actors: Search Poisoning

Image from http://www.infowat.com/blog/wp-content/uploads/2010/12/koobface.jpg

Criminal for Profit Actors
Fake AV



Insider Threat

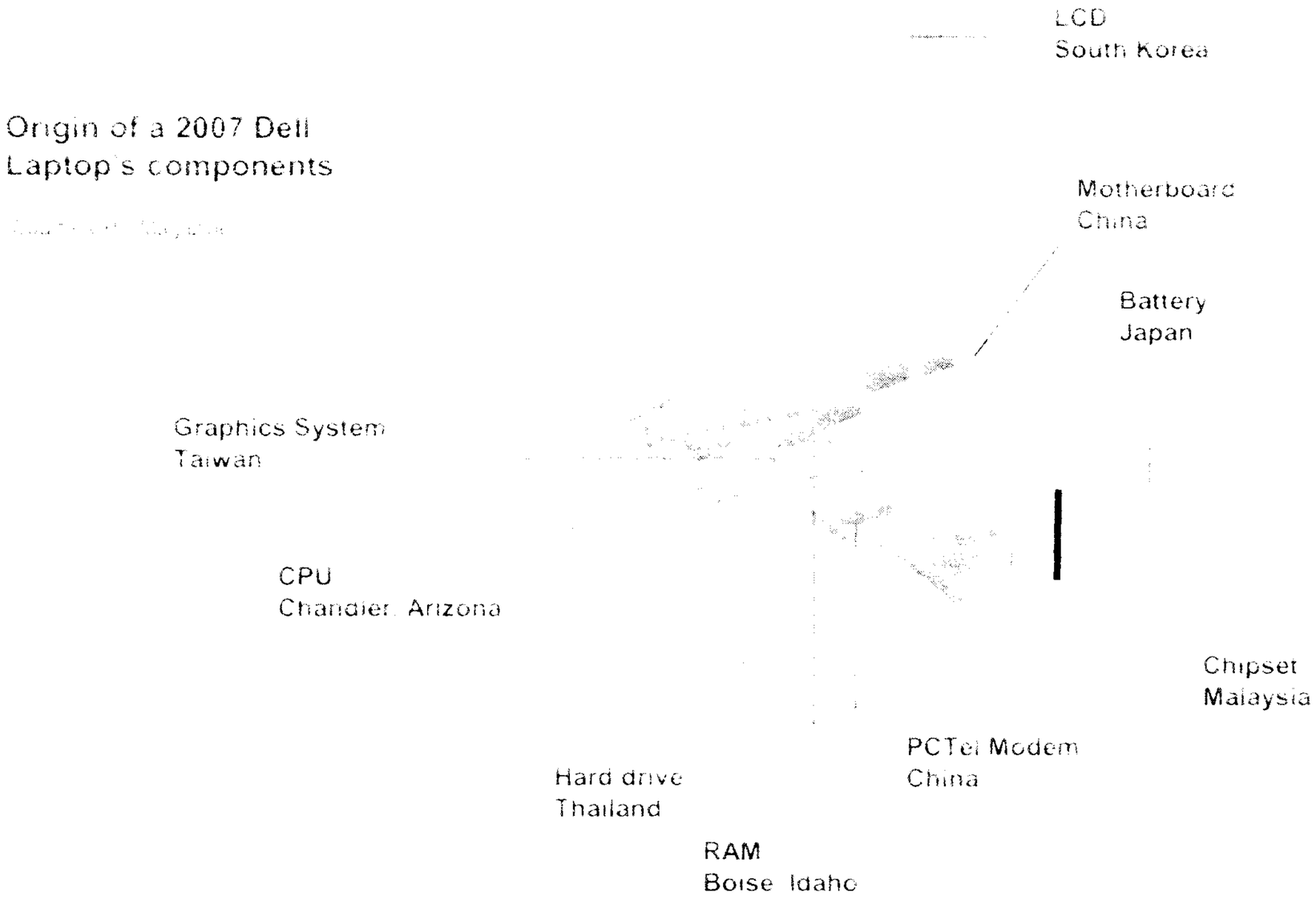


Advanced Threats

- Attacks undertaken by sophisticated actors
- Examples:
- Supply Chain Issues
- Attacks against control systems
- Stealing sensitive information (secrets, intellectual property etc...)

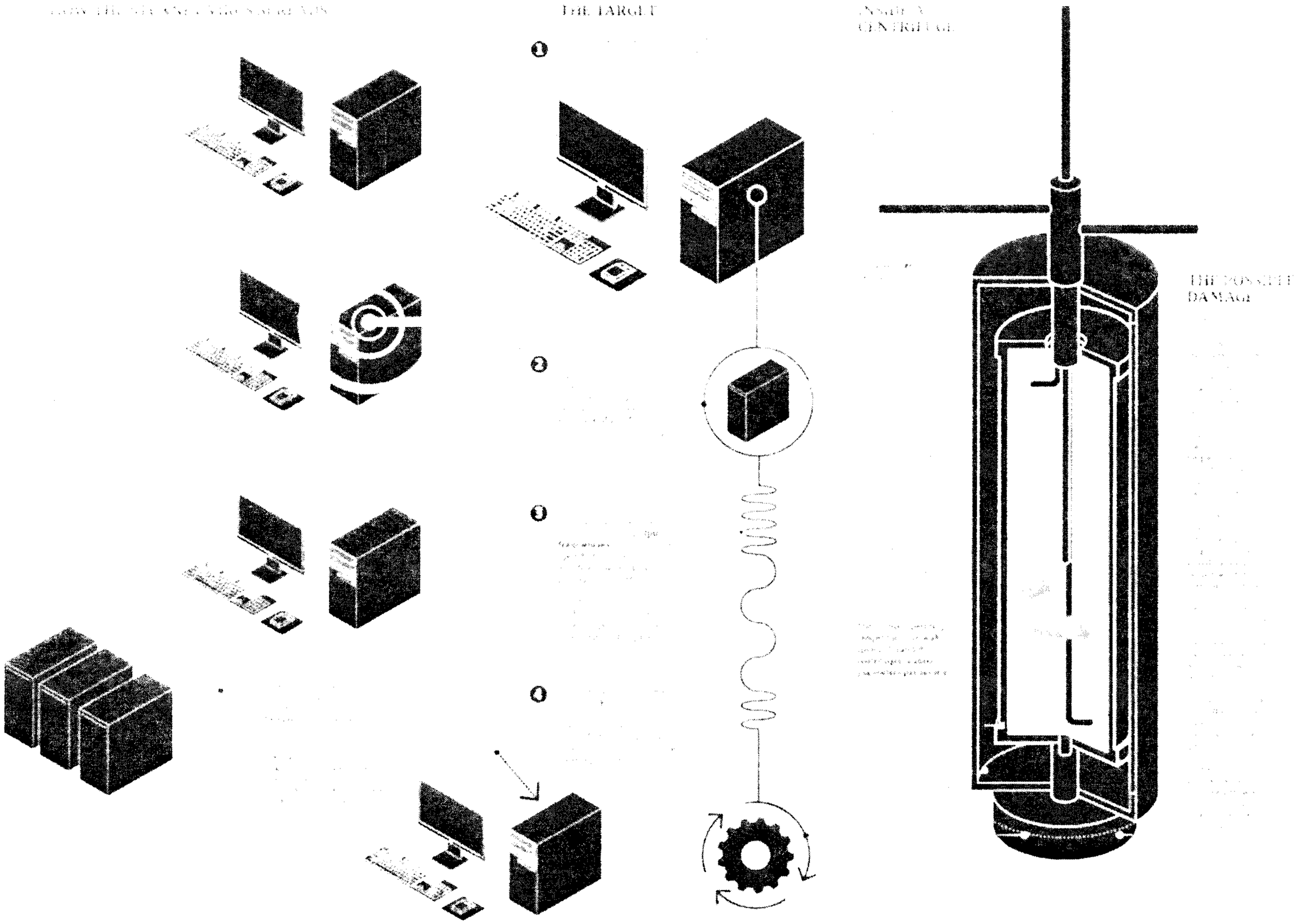
Supply Chain Issues

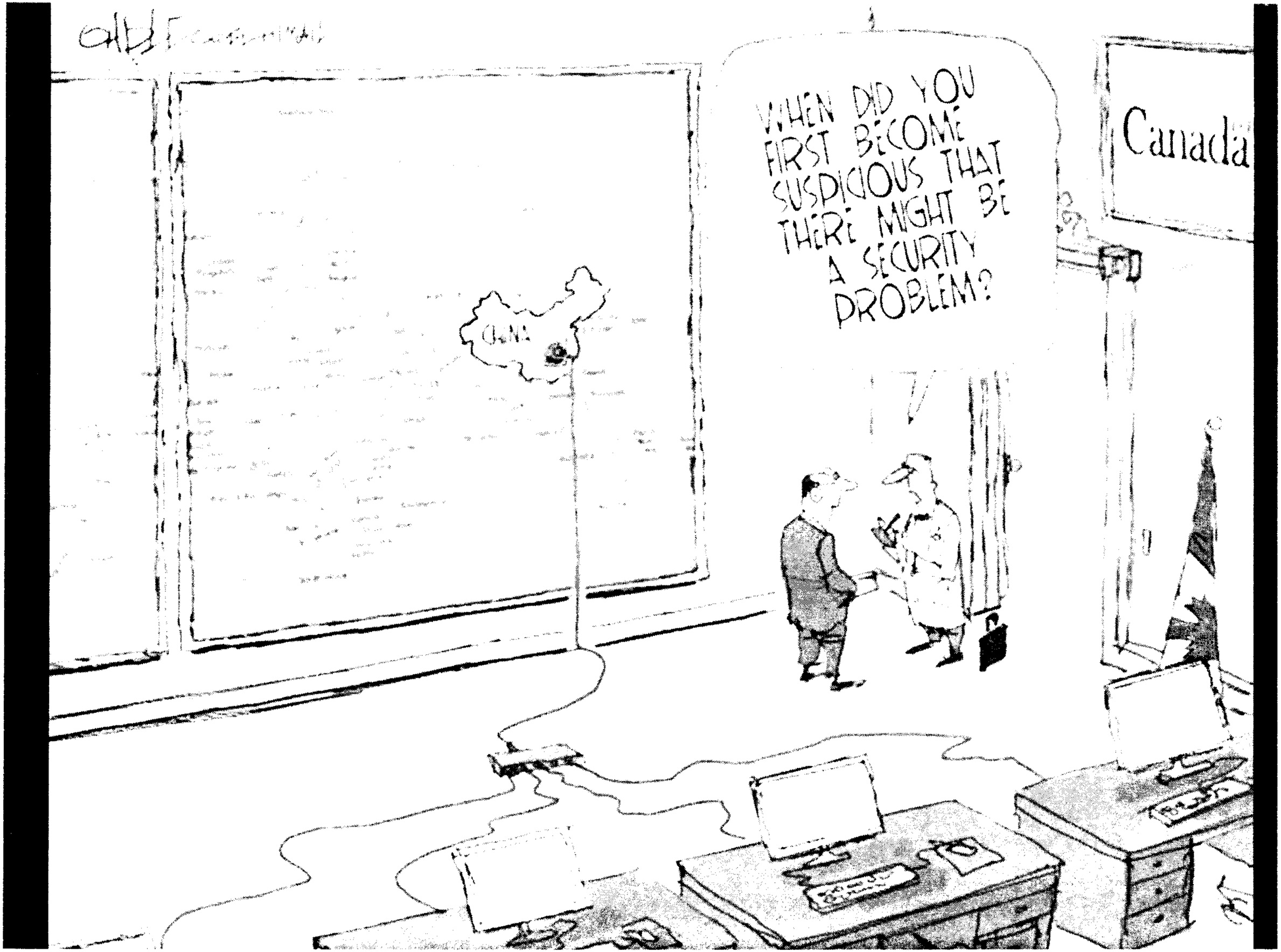
Origin of a 2007 Dell Laptop's components

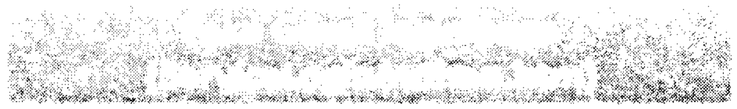


Attacks Against Control Systems

- STUXNET – a sophisticated attack against the Iranian nuclear program
- Likely the most complex cyber attack ever discovered
- Many questions about its origin







Account

Some ... are en_KR (Google in English for Korea)

Wrong password alert (JS pop up)

Wrong password alert (editext)

Account

RSA BREACH

- RSA (named for Rivest, Shamir and Adleman)
- Provider of RSA SecurID a two factor authentication system
- March 2011 – RSA announces that it has been victim of an advanced attack that "may" have compromised the SecurID technology
- June 2011 – First news of compromises released from US Defence contractors where a compromised SecurID was part of the attack

Examples of Emerging Areas of Concern

- Move towards Cloud computing
- Mobile device security
- Social Networking
- Commercialization (personal devices at the office)
- Weaponization of Cyberspace

NCSD Current Work and Long Term Priority Areas

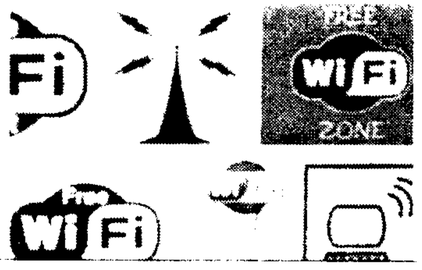
- Norms / Principles Governing Behaviour in Cyberspace
- Increasing cross border and international cooperation
- Working to increase information sharing across Government
- Supply chain management issues
- Control systems issues
- National response plan
- Public awareness and education

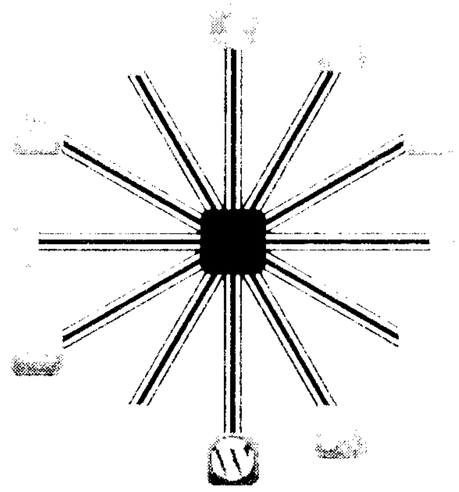
Am I aware of my cyber vulnerabilities?

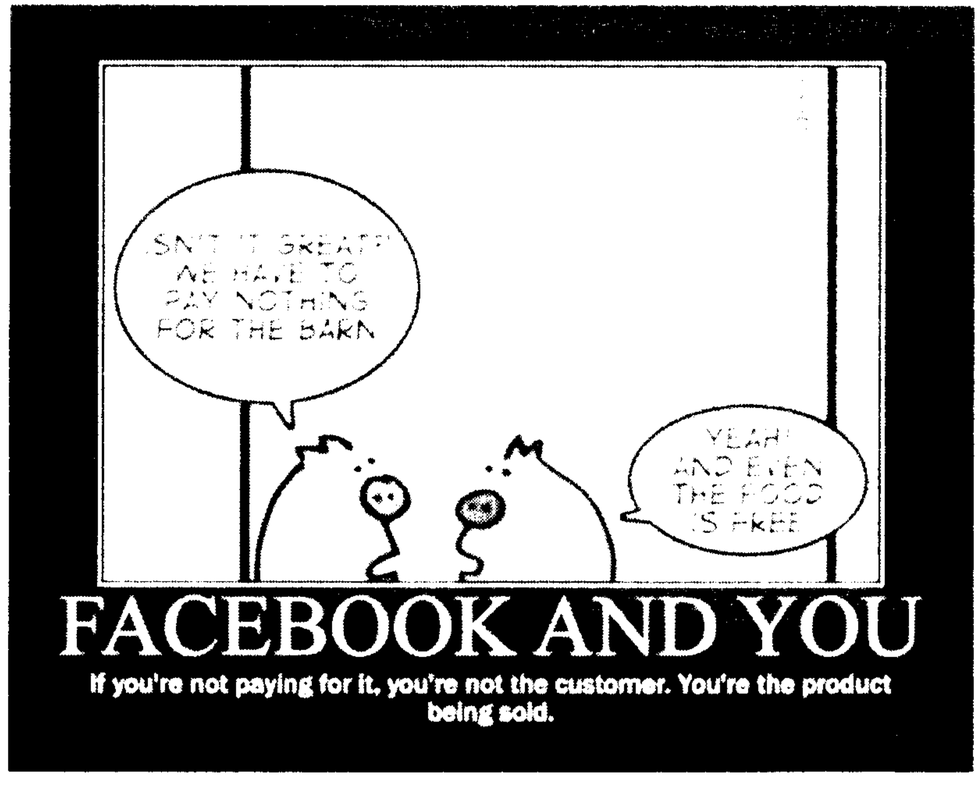
How to Hijack Facebook Using Firesheep

I hijacked a Facebook account with Firesheep. It was easy, and here's what you should do to avoid falling victim.

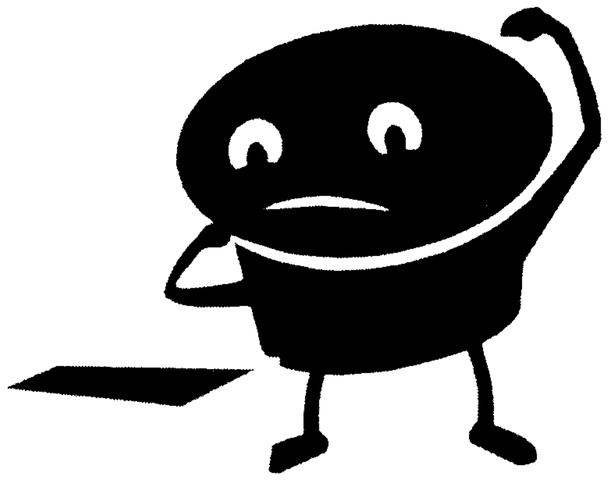
Unprotected Wi-Fi getting owners in trouble







Questions?



s.15(1) - Subv

Ap 26 2012

SECRET

s.13(1)(a)

DATE:

File No.: 387423

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

(Decision sought)

ISSUE

BACKGROUND

CONSIDERATIONS

.../2

SECRET

Prior to the London International Cyber Conference, Public Safety Canada led an interdepartmental consultative process to prepare several papers articulating the Government of Canada's position on various cyber issues.

[redacted]

RECOMMENDATION

[redacted]

Should you require additional information, please do not hesitate to contact me at 613-990-2661 or Mark Matz, Director of Policy and Issues Management at 613-993-9635.

Robert Dick
Director General
National Cyber Security

Enclosures: (1) [redacted]
(2)

I approve:

_____
Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Kees Bradley

Pages 1298 to / à 1370

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1) - Subv

SECRET [redacted]

25 April 2012

[redacted]

s.13(1)(a)

Dear [redacted]

[redacted]

s.13(1)(a)

Should you have any questions, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security at 613-990-2661.

Sincerely,

Lynda Clairmont
Senior Assistant Deputy Minister, National Security

Public Safety Canada / Sécurité publique Canada

SAFE RESILIENT CANADA

Canada's Cyber Security Strategy – One Year Later

May 2, 2012

Public Safety Canada - Regional Directors' NHQ Briefing

Canada

SAFE RESILIENT CANADA

Strengthen security of federal information and systems

- Division of cyber security roles
  - Communications Security Establishment Canada established the Cyber Threat Evaluation Centre as the Government of Canada computer emergency response team
  - The Canadian Cyber Incident Response Centre (CCIRC) is now the national computer emergency response team for provinces, territories and critical infrastructure sectors

UNCLASSIFIED

Progress on Pillar 1: Secure Government systems – cont'd

Shared Services Canada

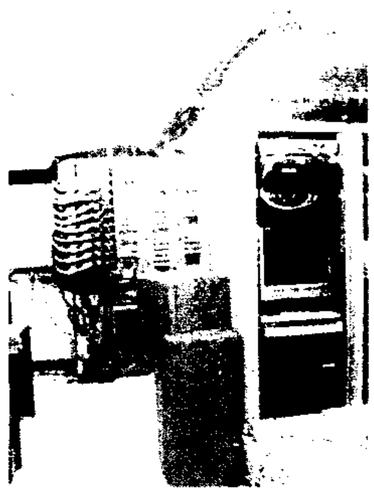
- Effective August 4, 2011, the Government streamlined and consolidated its information technology (IT) architecture in the areas of email, data centres and networks
- Will produce savings and reduce the Government's footprint; strengthen security and the safety of Government data to ensure Canadians are protected; and realize economies of scale and make it more cost-effective to modernize these IT services

UNCLASSIFIED

CCIRC

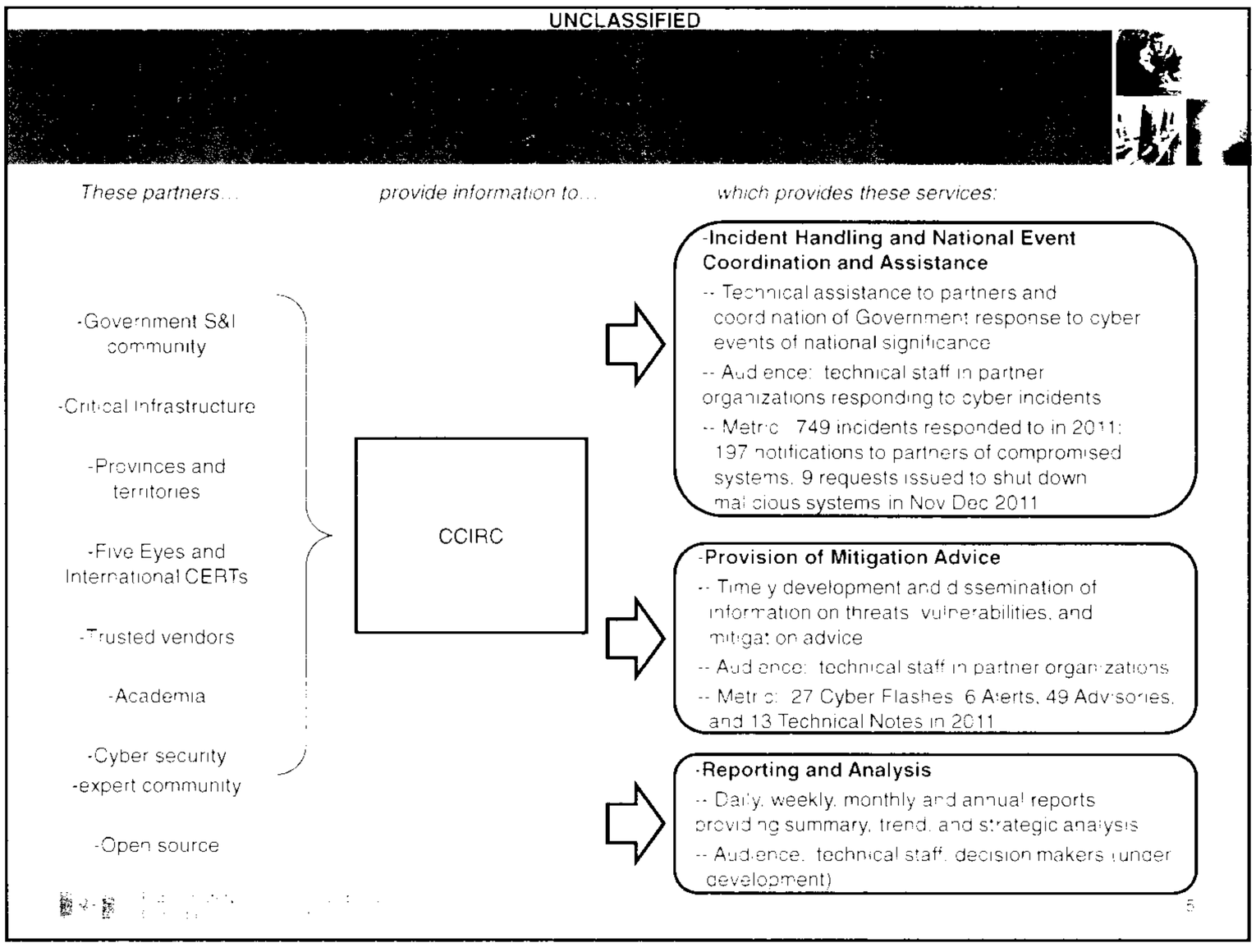
- Incident response centre
  - primary contact point into Government for domestic and international partners
  - CCIRC subject matter experts respond 9-5, 5 days a week
  - after hours coverage by Government Operations Centre

- Computer lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors



Progress on Pillar 2: Partnership, Security and Resilience [illegible]

- 22 Full time staff (once fully staffed)
  - highly specialized computer specialists with knowledge of IT security, computer forensics, and incident handling
  - analysis of multi-source intelligence and technical data and writing strategic assessments
- Organized into three functions:
  - Incident Handling – assists partners in identifying, mitigating, and managing incidents
  - Technical Support – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis
  - Strategic Initiatives and Situational Awareness – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers



UNCLASSIFIED

Projects on Pillar 2: Partnering to secure Critical Cyber Systems outside of the Government of Canada

Provinces and Territories (PTs) are a key partner

- Own systems with sensitive information
- Operate/regulate big critical infrastructure sectors (e.g.. energy)
- Have a role to play in managing the impacts of an event
- Can be instrumental in building a cyber-savvy workforce and changing behaviour through the education system

[redacted]

6

s.14(a)

UNCLASSIFIED

Strategic objectives for engagement are to have PTs

- Take steps to ensure security of their cyber systems
- Engage as active partners in areas of shared interest (e.g., securing economically sensitive information, critical infrastructure sectors) in line with jurisdictional roles

[redacted]

Progress on Pillar 2: Partnering to secure vital cyber systems outside the Government of Canada (cont'd)

Progress is being made

- Senior level FPT committee established, chaired by ADM – PS; working towards defining the elements of a shared action plan
- PS is working with FPT Chief Information Security Officers on early deliverables
- FPT communications working group established, focusing on public awareness and incident communications coordination

Proposal for a Cyber Incident Management Framework

- Establish criteria, protocols and mechanisms for sharing information and collaborating on resolution when necessary
- Ensure smooth national coordination and response to significant cyber events
- Clarify roles, responsibilities and expectations of all stakeholders
- Clarify linkages to national security and law enforcement activities
- Prevention of serious incidents
- Mitigate less serious incidents through information sharing and advice
- Integrate with the National Emergency Response System (NERS) to ensure seamless integration and consequence management for those events that cascade out of the cyber domain

UNCLASSIFIED

Proposed Components of the Framework

- Scope
- Concept of Operations
- Roles and Responsibilities
- Components:
  - Mitigation/Prevention
  - Preparedness
  - Response
  - Recovery
- Mechanisms:
  - CCIRC
  - MOU & Portal
  - Security clearances

UNCLASSIFIED

Proposed Initial Stakeholders

- Federal Government
  - Key security and intelligence partners (RCMP, DND/CF, CSEC, CSIS, TBS, SSC)
- Provincial and Territorial Governments
  - Assistant Deputy Minister level committee of cyber security
  - National CIO Sub-Committee for Information Protection

s.20(1)(d)

UNCLASSIFIED

Progress on Pillar 2: Partner to achieve [illegible] system [illegible] the Government of Canada [illegible]

Approach to Development and Approval

- Will not seek a specific body to approve final document

Next 12 months

- Framework Ver 1.0 promulgated as a working document to which parties can sign on
- Initial set of stakeholders will collectively sign on and publicize
  - Present Framework at conference/events
- Considered an open document
  - All can link with access to CCIRC portal and MOU

Years 1-2

- Broader process after one year to revise and find new signatories
- In future, would consider appending voluntary codes of conduct, security standards, etc

12

UNCLASSIFIED

Next Steps

- Increase the pace of collaboration with willing PTs, and show responsiveness to their priorities
  - MOU on Information Sharing
  - Incident Management Framework
- Reach out to Public Safety Canada regional offices to bring together PT emergency management and cyber security officials to discuss development of a national cyber incident response framework
  - Vancouver, May 29
  - Edmonton, May 30
  - Winnipeg, May 31
  - Regina, June 1

13

s.14(a)

UNCLASSIFIED

[redacted]

[redacted]

UNCLASSIFIED

Promote public awareness, education and engagement

- Public awareness campaign launched by Public Safety Canada
- Government-wide incident communications protocol being developed
- Communications working groups established with international partners and at the federal, provincial, and territorial level

Cyber Crime

- The Royal Canadian Mounted Police has established Cyber Fusion Centre to improve statistics on cyber crime

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

Briefing on Cyber Security

Minister Toews' Possible Visit to the United Kingdom (UK), May 10-15, 2012

ISSUES

- Global cyber security threats and trends
- Clearer understanding of public-private information sharing
- Canada-UK cooperation and common narrative on cyber security

STRATEGIC OBJECTIVES

Issue 1

- Convey the message that Canada and the UK face the same cyber threats and are pursuing compatible strategies.

Issue 2

- Obtain a clearer understanding of how the UK provides intelligence to private sector organizations, particularly in light of the UK's November 2011 update to its *National Cyber Security Strategy*.

s.15(1) - Int'l

s.15(1) - Subv

Issue 3

[redacted]

BACKGROUND

Issue 1: Global cyber security threats and trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. The ease of use of modern hacking tools makes it simple for activists to temporarily disrupt websites or cause other damage to networks. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. The hackers then craft emails or other messages that have been fabricated to trick the victim into downloading viruses or divulging details that would allow access to valuable information, such as intellectual

property or credit card information. Intelligence services and militaries are also capitalising on states' dependence on networked infrastructure to conduct espionage activities or to support military operations.

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

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

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

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

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the Royal Canadian Mountain Police's Integrated Cyber Crime Fusion Centre which was established per *Canada's Cyber Security Strategy*.
- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks.
- Canada's GetCyberSafe.ca website was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing

s.13(1)(a)

s.15(1) - Int'l

s.15(1) - Subv

the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.

Issue 2: Clearer understanding of public-private information sharing

United Kingdom: [redacted] The CPNI is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage. The advice under which these threats are addressed covers physical, personnel and information security, and includes cyber security.

Canada: [redacted] As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to identify any gaps and modernize Canada's frameworks for information sharing accordingly. In this matter, it may be useful to learn more about the UK's new national security hub to facilitate public-private information sharing.

[redacted]

Cyber security is gaining sustained and high-level attention globally. [redacted]

The Internet has historically been managed through a public-private model that is coordinated by a non-profit corporation based in the United States, namely the Internet Corporation for Assigned Names and Numbers (ICANN). [redacted]

United Kingdom: The UK [redacted] launched a counter-narrative with the London Conference on Cyberspace on November 1–2, 2011. This narrative emphasizes that:

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

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

The London Conference on Cyberspace represented a major initiative: it was hosted by the UK Foreign Minister William Hague, featured high-level participation (including from U.S. Vice President Joseph Biden), and brought together representatives from over 60 countries, the private sector and civil society. Hungary will host the next Conference in Budapest in October 2012, and will likely feature similar prominent political engagement.

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

Canada is a signatory to, and has committed publicly to ratifying, the Council of Europe Convention on Cybercrime, also known as the "Budapest Convention". Key allies, including the UK and the United States, view this as a key international agreement and are eager for Canada to complete its ratification process. The recently tabled Bill C-30 contains measures, including provision for data preservation orders, which would enable Canada to ratify the Budapest Convention.

STRATEGIC CONSIDERATIONS

Issue 1: Global cyber security threats and trends

None in particular.

Issue 2: Clearer understanding of public-private information sharing

UK intelligence agencies have the unique ability to provide intelligence information to private sector entities under their enabling legislation which states that a function of the UK's Secret Intelligence Service is to safeguard the economic wellbeing of the UK against threats posed by actions or intentions of persons outside of the British Islands.

s.15(1) - Int'l
s.15(1) - Subv
s.16(2)(c)

[redacted]

clear understanding how the UK shares intelligence information with the private sector, whether through CPNI or through other means.

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

[redacted]

Canada and the United Kingdom cooperate extensively on cyber issues both at an operational and policy level.

s.16(1)(b)

At the operational level, the Canadian Cyber Incident Response Centre (CCIRC) and its UK counterpart, the CPNI, have an excellent working relationship [redacted] They also collaborate in the Usual 5, a grouping of representatives from the computer emergency response teams from each of the Five Eyes allies.

s.15(1) - Int'l

s.15(1) - Subv

[redacted]

TALKING POINTS

Issue 1: Global cyber security threats and trends

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

- I was interested to note that your recently updated national cyber security strategy is very compatible with our own.

- In terms of our strategy, you may be interested in an initiative we are undertaking to bring a large portion of our government departmental networks under the management of a single new organization called Shared Services Canada. This will reduce the contact points of our network to the internet, allow for better monitoring of what goes in and out, and improve security measures to protect Government of Canada systems.

Issue 2: Clearer understanding of public-private information sharing

- The recent update to your cyber security strategy talked about the creation of a "hub" for government and private sector information sharing. What are the objectives for this hub and how would it work?

- As my staff and I work to address challenges associated with sharing information in Canada, it would be informative to hear about the kinds of challenges you face in sharing information to enhance the security of networks and systems in the UK.

Issue 3: Canada-UK cooperation and common narrative on cyber security

- Canada appreciates the international leadership and resolve shown by the United Kingdom in advancing a position on norms and principles of behaviour for all stakeholders in cyberspace.

- Canada strongly supports the United Kingdom in promoting common interests and policy positions on cyber security. The October conference in Budapest, as the follow on from the London Conference on Cyberspace, will be another key opportunity to influence the international discussion on cyber security and cyberspace generally.

- Canada has valued the collaboration with the UK and we look forward to continuing to work together with you.