SECRET – with attachments

DM Cyber

January 12, 2012
14:00 to 15:00

19th floor boardroom
269 Laurier Avenue West

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

For your meeting with:
Deputy Ministers Committee on Cyber Security
On: January 12, 2012

SECRET – with attachments

DATE: JAN 0 9 2012

cyber media

File No.: 384918
RDIMS No.: 537473

Seen by the DM
Vu par le SM

MEMORANDUM FOR THE DEPUTY MINISTER

DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY JAN 1 2 2012

(Information only)

ISSUE

You will be chairing the inaugural meeting of the Deputy Ministers Committee on Cyber Security (DM Cyber), which is scheduled to take place on January 12, 2012.

A briefing binder with necessary background information and proposed speaking points is enclosed for your convenience.

BACKGROUND

As you will recall, DMs and their representatives expressed a need for greater governance on cyber security at a November 8, 2011 meeting with the National Security Advisor (NSA) to the Prime Minister and officials from the Canadian Security Intelligence Service, the Communications Security Establishment Canada (CSEC), the Department of National Defence and Public Safety Canada.

It was agreed that the inaugural meeting of DM Cyber would take place in mid-December 2011; however, this meeting was postponed to January 12, 2012. The Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber) met on December 5, 2011, to review the draft DM Cyber agenda and prepare for the meeting.

CURRENT STATUS

At the inaugural DM Cyber meeting, it is proposed that DMs consider five main agenda items.

As this will be the first meeting of DM Cyber, and given that several participants were not at previous meetings with the NSA, the primary objective will be to seek agreement on the membership and terms of reference of the Committee. This item, the first on the agenda, is for decision.

Responding to requests made at the previous meeting of DMs, two items are on the agenda for information. The Treasury Board of Canada Secretariat will speak to network hygiene in the Government by describing the challenge in protecting Government systems, work undertaken in this area to date, and planned work going forward. I will then present on roles and responsibilities of departments with respect to cyber security.

Finally, there are two additional items for information.

Second, you could brief on the January 23, 2012 meeting of Federal/Provincial/Territorial Clerks, at which cyber will be discussed.

NEXT STEPS

Since DMs agreed to meet quarterly, the next DM Cyber will be scheduled in late March or early April 2012. ADM Cyber and the Directors General Committee on Cyber Security will meet monthly to support the efforts of DM Cyber.

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

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure: (1)

Prepared by: Melanie Mohammed

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

Deputy Ministers Committee on Cyber Security

January 12, 2012 – 14:00 to 15:00
19th floor boardroom, 269 Laurier Avenue West

AGENDA

	Time	Item	Associated Documentation
	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	
	14:40	[redacted]	
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

s.15(1) - Int'l

Page 345

is not relevant

est non pertinente

DM CYBER MEETING PARTICIPANTS
Thursday, January 12, from 2-3PM

PS (Chair)	William V. Baker	YES
PS	Graham Flack	YES
PS	Lynda Clairmont	YES
CSIS	Richard Fadden	YES
RCMP	Bob Paulson	YES
DND	Robert Fonberg	YES
CF	General Walt Natynczyk	YES
CSEC	John Adams	YES
IC	Richard Dicerni *Helen McDonald*	Delegate (Helen McDonald, Assistant Deputy Minister, SITT)
JUS	Myles Kirvan *Yves Coté*	Delegate (Yves Coté)
PCO	Stephen Rigby *Rennie Marcoux*	Delegate (Rennie Marcoux)
SSC	Lisanne Forand	YES
TBS	Michelle D'Auray *+1 – Pierre Boucher*	YES +1 Pierre Boucher
DFAIT	Morris Rosenberg *Gérald Cossette*	Delegate (Gérald Cossette)

TAB 1

1. OPENING REMARKS

- Bonjour tout le monde, et bienvenue à notre première réunion.
  - *Good afternoon everyone, and welcome to our first meeting.*

- Since this is our first meeting, and since several around the table were not at previous related meetings with the National Security Advisor, today's primary objective will be to set the stage for future work. Our first item of discussion will be to agree on the Committee's terms of reference and membership.

- Next, there are two information items intended to provide us with the necessary knowledge to help us contextualize future discussion. The first item today will be on network hygiene, which Michelle (D'Auray) will brief on given her responsibility for the Chief Information Officer Branch.

- For the second item, a higher-level overview of roles and responsibilities across the federal government, I've asked Lynda Clairmont to present, given her responsibility as lead Senior Assistant Deputy Minister for *Canada's Cyber Security Strategy*.

- I would invite each of you to identify future topics on which you would like to brief this Committee, or be briefed.

- Finally, there are two transactional items on which it is timely that we be briefed. [redacted] Last, I will speak to the January 23, 2012 meeting of the Federal-Provincial-Territorial Clerks, at which cyber will be discussed.

- A final note: a template has been circulated to your departments seeking input on the forward agenda for this Committee, so you'll have an opportunity to shape that by talking to your ADMs.

TAB 2

2. DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

PROPOSED TALKING POINTS

- I'd like to take a couple of minutes to outline the draft terms of reference and membership for this Committee, formally known as the Deputy Ministers Committee on Cyber Security (DM Cyber), and seek any comments that you may have with respect to what is proposed.

- DM Cyber will guide the overall policy direction and set priorities for forward work. We will also be monitoring progress on the implementation of *Canada's Cyber Security Strategy*, and our meetings will serve as a venue for considering emerging issues. We ~~would~~ will not be an operational committee – crisis management mechanisms already exist.

- The Directors General Committee on Cyber Security (DG Cyber) met in late November 2011 to discuss the membership of DM Cyber. That group recommended that the Department of Foreign Affairs and International Trade be added to the membership list for DM Cyber and we have done so.

- At the December 2011 meeting of the Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber), Public Works and Government Services Canada (PWGSC) also indicated potential interest given its roles to protect Government's sensitive information provided through contract to industries within Canada and abroad; however, it was agreed that they would postpone joining our meetings until a future date.

- In the interim, I believe it would be beneficial that Shared Services Canada keep PWGSC apprised of issues that may require their attention.

- I want to underscore that should issues touch on the roles, responsibilities and mandates of other departments, implicated Deputy Heads would be invited to attend our meetings.

- We are proposing that DM Cyber meet on a quarterly basis, with additional meetings, if necessary, to consider urgent issues.

- My Department is also developing a draft forward agenda. Input is being sought from DG and ADM Cyber member departments, and I hope to have a version ready for your review by our next meeting.

ISSUE

You will lead a discussion on the draft terms of reference and membership for the Deputy Ministers Committee on Cyber Security (DM Cyber). **You** will also speak to the development of a draft forward agenda that will be presented at a future meeting.

Draft terms of reference and membership for DM Cyber were distributed to participants in advance of the meeting, and are enclosed for your ease of reference.

CURRENT STATUS

Terms of reference

Public Safety Canada has developed draft terms of reference and a proposed membership for DM Cyber. The terms of reference indicate that the purpose of the Committee is to:

- establish policy direction;
- set priorities;
- monitor the implementation of *Canada's Cyber Security Strategy*; and
- consider emerging issues.

Membership

During the November 30, 2011 meeting of the Directors General Committee on Cyber Security (DG Cyber), the Department of Foreign Affairs and International Trade (DFAIT) indicated that their DM was interested in participating on DM Cyber.

DG Cyber supported this request given international focus, DFAIT's role, and broader policy linkages that would benefit from a greater awareness on the part of the DM of Foreign Affairs to cyber security concerns.

Public Works and Government Services Canada (PWGSC) also indicated that they were interested in having their Deputy participate on DM Cyber given the Department's mandate to protect Government's sensitive information provided through contracts to industries within Canada and abroad. At the December 5, 2011 meeting of ADM Cyber, however, it was agreed that PWGSC would consider joining DM Cyber at a future date. In the interim, it was deemed to be preferable that Shared Services Canada keep PWGSC apprised of issues that may require their attention.

It will be important to underscore that should issues touch on the roles, responsibilities and mandates of other departments, other Deputy Heads would of course be invited to attend.

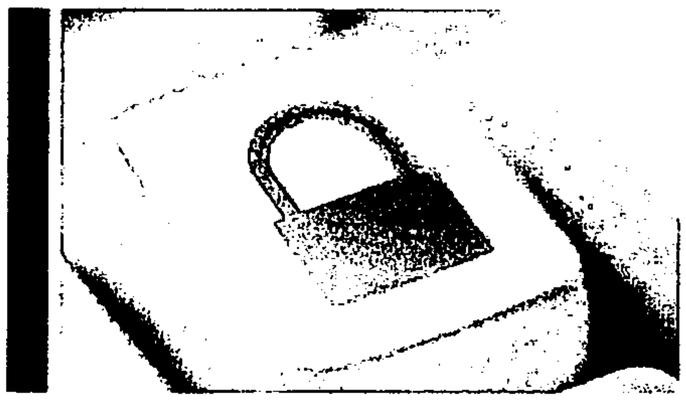
Forward agenda
Information presented in the forward agenda will show alignment of activities with domestic priorities, and will provide information regarding efforts underway to advance objectives.

A template was circulated during the week of December 16, 2011, to DG and ADM Cyber member departments. Input is expected in early 2012, and will be refined at the DG and ADM levels before being presented at the next DM Cyber meeting.

Prepared by: Melanie Mohammed
Approved by: Corey Dvorkin

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED
DRAFT



Deputy Ministers Committee on Cyber Security

Terms of Reference

Purpose

The purpose of the Deputy Ministers Committee on Cyber Security (DM Cyber) is to:

- establish policy direction;
- set priorities;
- monitor progress on the implementation of *Canada's Cyber Security Strategy*; and
- consider emerging issues.

Membership

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

- Core members:
  - Director, Canadian Security Intelligence Service
  - Commissioner, Royal Canadian Mounted Police
  - Deputy Minister, National Defence
  - Chief of Defence Staff, Canadian Forces
  - Chief, Communications Security Establishment Canada
  - Deputy Minister, Foreign Affairs
  - Deputy Minister, Industry Canada
  - Deputy Minister and Deputy Attorney General of Canada, Department of Justice Canada
  - National Security Advisor to the Prime Minister, Privy Council Office
  - President, Shared Services Canada
  - Secretary of the Treasury Board, Treasury Board of Canada Secretariat

Governance / Relationship to other working groups and committees

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

Meeting frequency

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

Page 355

is not relevant

est non pertinente

TAB 3

3. NETWORK HYGIENE

PROPOSED TALKING POINTS

- At the November 8, 2011 meeting, some of our colleagues expressed interest in learning more about network hygiene and how best to advance it in Government. This is a fundamental cyber security issue.

- The Treasury Board of Canada Secretariat has drafted a deck, and I invite them to walk us through it.

During discussion

- Given that this is a long-term goal, does our current approach respond directly enough to the evolving threat environment? If we had to move faster, could we?

- Is there more we need to do to manage our network hygiene while we undertake the consolidation of our systems? Can we provide a clearer framework to departments, or specific guidelines to Deputies?

- Can we work more collaboratively to expedite this process?

ISSUE

You will introduce this agenda item. Treasury Board of Canada Secretariat (TBS) will present for discussion a deck they have prepared with input from the Communications Security Establishment Canada (CSEC).

The deck was distributed to participants in advance of the meeting, and is enclosed for your ease of reference.

BACKGROUND

Network hygiene refers to regularly performing the "bread and butter" activities of network and information technology (IT) security, such as upgrades and patch maintenance. It is well recognized that disciplined network hygiene makes a significant

difference in security, but that it can also be onerous and time-consuming for IT staff given other operational priorities.

Shared Services Canada (SSC) will centralize the governance of Government IT, which should simplify the maintenance of uniform network hygiene. This transition will evolve over years, during which time discipline will still be required across the decentralized IT infrastructure.

CURRENT STATUS

TBS, CSEC and SSC are recommending the increased consolidation of Government networks to ensure that all departments are operating in the same environment.

s.15(1)(i)

This number has been reduced by one third since 2009.

The creation of SSC will continue to advance this endeavour; however, consolidation alone will not resolve all of Government's IT or cyber security issues, and other steps are also underway.

TBS is also assessing departmental IT security compliance via the Management Accountability Framework to hold each Deputy Head accountable for their department's level of compliance.

NEXT STEPS

Government departments implicated in *Canada's Cyber Security Strategy*, principally TBS, CSEC, SSC and Public Safety Canada (PS), will continue to promote awareness of IT security practices among Deputy Heads and in other fora within and outside Government.

TBS and SSC will continue to redesign the enterprise IT security model to ensure that IT security is built in to the architecture, rather than added as an afterthought.

Finally, TBS and SSC are working to establish a Government of Canada Incident Recovery Team (IRT). The IRT would provide IT incident recovery services to Government departments and agencies with a view to reducing recovery time and ensuring comprehensive and lasting solutions.

CONCLUSION

To ensure that network hygiene is effective, a simplified and more cohesive network infrastructure needs to be implemented across Government. TBS, CSEC and SSC are working to reduce complexity, increase IT homogeneity, and reduce the footprint of Government IT infrastructure.

Prepared by: Melanie Mohammed
Approved by: Adam Hatfield

Treasury Board of Canada Secretariat / Secrétariat du Conseil du Trésor du Canada

Better government with partners for Canadians

SECRET

Cyber Security

The Challenge In Protecting Government Systems

Canada

SECRET

Agenda

- Threat Landscape
- What we have done to date
- The Way Ahead
- Conclusions

2

1

SECRET

Cyber Threat Landscape

SOPHISTICATED

SIMPLE

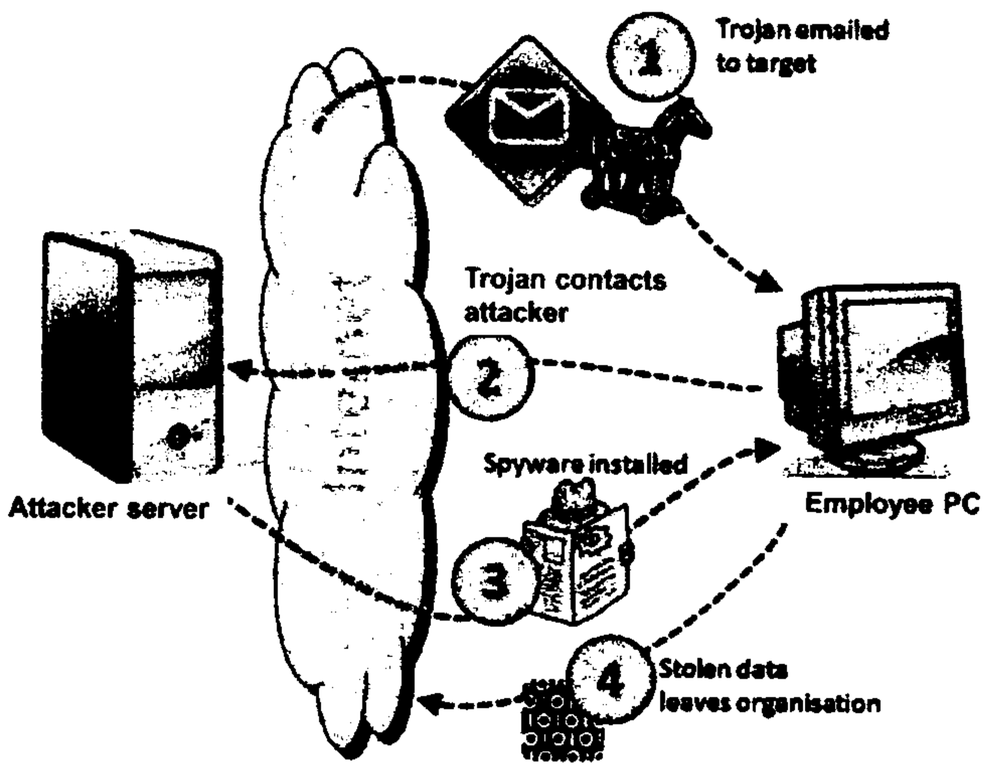
Planned

- Hackers and Hacktivists
  - Motivation: Social/political
  - Target: Organizations promoting political and/or societal positions
  - Methods: Website defacement, denial of service
  - Techniques: Exploitation of common software vulnerabilities
- Criminals
  - Motivation: Profit
  - Target: Canadian citizens, retailers, financial sector
  - Methods: Social engineering to send malicious emails to groups of people, exploitation of common software vulnerabilities, establishment of fake websites
- State Sponsored
  - Motivation: Political, military, economic advantage
  - Target: Government, academia, industry, critical infrastructure
  - Methods: Exploitation of non-public software vulnerabilities, targeted social engineering of individuals, tampering with products during manufacture to build in vulnerabilities or malicious code

3

SECRET

Typical Attack Scenario



4

SECRET

Cyber Defence is a Challenge

- IT security is not implemented in a systemic, coordinated fashion at the enterprise level – uncoordinated evolution, various level of services, disperse operation, multiple authorities and accountabilities
- People are also targets - it can be hard for a user to detect malicious emails
  - Adversaries use social engineering techniques to trick people into believing the malicious email or attachment is valid and important to them
- Sophisticated attackers constantly probe and persist until they succeed, exploiting any weaknesses in our defences, scaling from most common and well known vulnerability to the most complex methods and non-public vulnerability.
  - Constantly harvesting data (network and human behaviour) for future exploitation.
  - Successfully implementing top "x" mitigations is not enough

5

- need an organized network & implement some of the suggested solutions

SECRET

Government IT Systems Complexity and Diversity

- The GC IT infrastructure has been cobbled together over time without an overarching plan:
  - Networks of networks: over 3000 overlapping networks
    - Unique security requirements, in some cases accountable to other international partners
  - Data centers: over 300 data centers
  - Mid-range servers: over 25,000
    - Wide range of vendors, platforms (MS, Unix, Linux)
    - 30% simple, 40% web or mail, 30% complex apps & databases
  - Applications: over 16,000 business applications
    - Aging/legacy apps; some 45 years old
  - Desktops: wide range of OS currently in service; from Windows 95 on, Unix family, Linux, etc

s.15(1)(i)

[redacted]

s.21(1)

6

HR - over 800 applications
6 months ago
- 10 year old software
- windows 95/98

SECRET

What We Have Done To Date

- TBS Assessing IT Security compliance via MAF (2006)
  - Improvements in compliance
  - Awareness including basic network hygiene practices
- TBS leading the Consolidation of Internet Access Points
  - Reduced by one third since 2009
  - TBS has clearly defined acceptable / not acceptable configurations (2011 shows 80% acceptable)
  - Allows for cost-effective deployment of defence solutions

s.15(1)(i)

[redacted]

7

SECRET

Moving Forward

TBS continues to champion initiatives that support IT infrastructure consolidation and rationalization

- Creation of SSC
  - Game changer: significant impact on our consolidation effort
  - Consolidating and standardizing Enterprise IT Architecture
  - Increasing operational excellence at the enterprise level
  - Standing up a Gov-CIRT at SSC
- Enterprise-wide secret network
- Application Consolidation Strategy
- End User Device Strategy
  - Desktop rationalization Ex. HRSDC Cluster
    - HRSDC, DFO, AGAF/CFIA, IC (*SSC & HC as observers*)
    - 61,700 seats and over 100,000 devices
    - Moving to Windows 7, Internet Explorer 8, Office 2010
- Security awareness: changing behaviour

8

network
Late delete
email

partial rollout
in a domain
environment

SECRET

Consolidation is a Prerequisite for Sustainable Network Hygiene

- Government must defend against the full spectrum of cyber threats, including the most sophisticated
- GC IT infrastructure is complex, massive, heterogeneous, and still teeming with legacy systems
- Implementing the simplest security measure is an operational and technical challenge. A comprehensive security effort in such an environment is complex, risky and costly
- For network hygiene to be effective we need a simplified and more cohesive network infrastructure
- We are tackling the issue with initiatives that will reduce complexity, increase IT homogeneity, and reduce our infrastructure footprint
- Even with a simple, cohesive network, there must be ongoing efforts to ensure security-conscious behaviour by individuals and management

We will leverage current consolidation initiatives to build a cohesive, resilient and secure enterprise IT infrastructure

9

SECRET

ANNEX

10

SECRET

Network Hygiene – Top 10 Mitigating Actions*

1. Patch Operating systems in a timely manner
2. Patch applications (PDF viewer, browser, office applications)
3. Minimize use of administrator privileges
4. Application "whitelisting" to prevent malicious programs
5. Host-based intrusion detection/prevention system
6. Workstation inspection of Microsoft Office files
7. Whitelisted email content filtering to block malicious attachments
8. User education on Internet risks, social engineering
9. Ensure routing of internal traffic does not exit the network
10. Tools to help prevent malicious code from running

** Extracted from CSEC Top 35 Mitigation Actions*

11

Pages 366 to / à 372

are not relevant

sont non pertinentes

TAB 4

4. CYBER SECURITY ROLES AND RESPONSIBILITIES

PROPOSED TALKING POINTS

- It's obviously critical that we have a shared understanding of who does what on cyber security.

- Lynda Clairmont, Senior Assistant Deputy Minister of National Security at Public Safety Canada, will give us a high-level overview of the key roles of federal departments and agencies.

ISSUE

You will introduce this item. Lynda Clairmont, Senior Assistant Deputy Minister of National Security at Public Safety Canada, will speak to the distribution of cyber security efforts across Government, with a view to informing Deputies on the roles and responsibilities of cyber security lead departments.

A roles and responsibilities dashboard was distributed to participants at the beginning of the meeting, and is enclosed for your ease of reference.

BACKGROUND

In November 2010, members of the Directors General Committee on Cyber Security (DG Cyber) provided Public Safety Canada with a slide that described their department's mandate as it relates to cyber security. In November 2011, departments were asked to update or validate their response. This information was categorized so as to be able to be presented visually.

Comments received at the late November and early December 2011 meetings of DG Cyber and the Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber) indicated a need to better describe the roles of departments in terms of cyber security, primarily with regard to the role of defence departments, and with regard to critical infrastructure protection. It was suggested that a dashboard may be more representative and accurate means of doing this.

CONSIDERATIONS

The roles and responsibilities of Government departments and agencies as presented in the *Government of Canada Information Technology Incident Management Plan* (GC IT IMP) are somewhat defined in terms of responding to a cyber incident affecting a Government network; however, owing to the launch of Shared Services Canada, this

mechanism needs to be revised. In the case of a cyber incident affecting a province or territory, critical infrastructure sector or private sector entity, however, roles, responsibilities and capabilities are more ambiguous.

A series of tabletop exercises beginning January 13, 2012, will help to provide the necessary clarity, and identify policy and operational barriers to information sharing. Additionally, these exercises will contribute to Public Safety Canada's initiative to establish a national cyber incident response framework. This framework would clarify the roles and responsibilities of Government, provincial and territorial partners, and private sector entities.

s.15(1) - Int'l

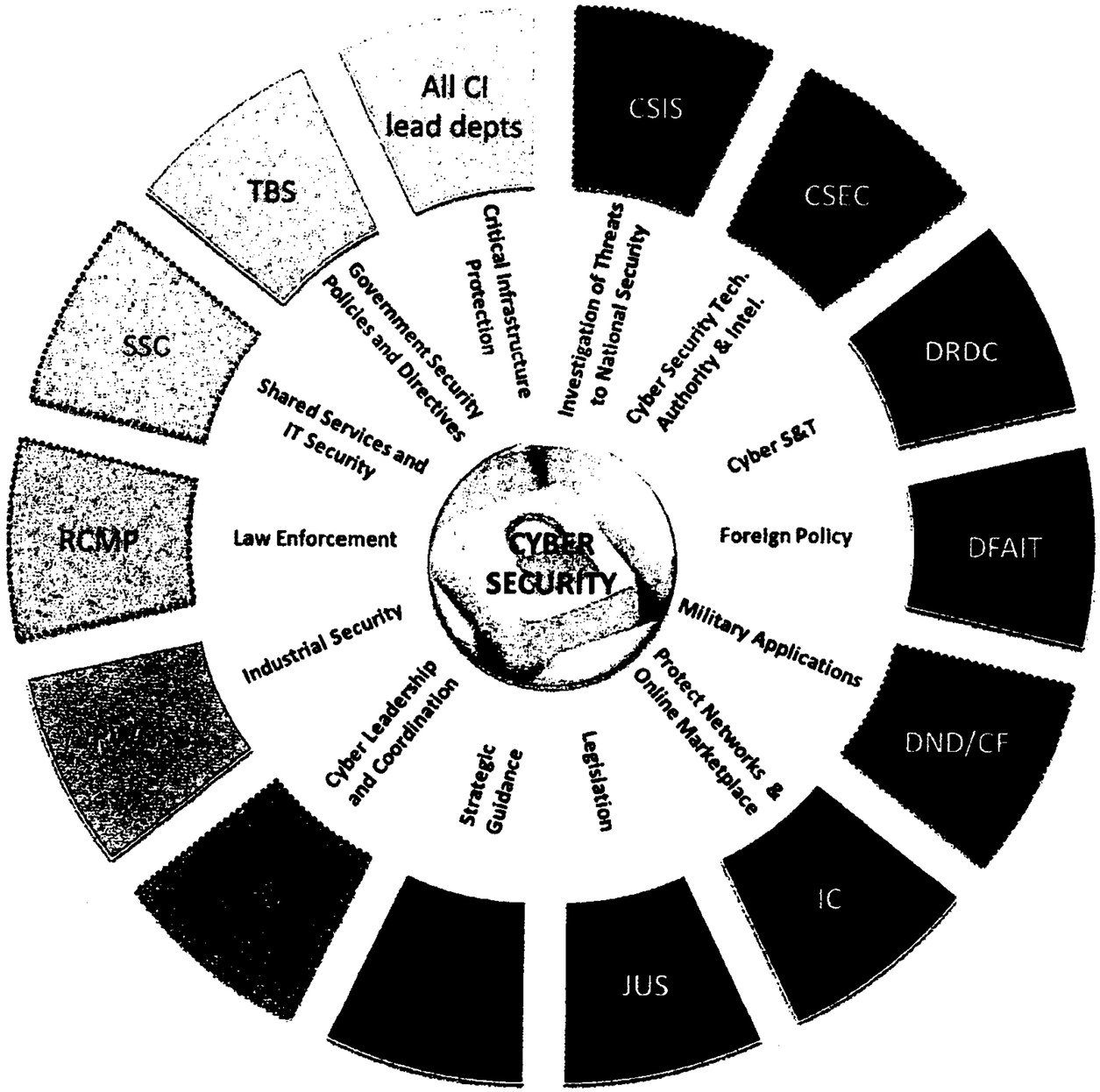
CONCLUSION

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 [redacted]
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

TAB 5

Pages 379 to / à 382

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

Pages 383 to / à 391

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Page 392

is withheld pursuant to sections

est retenue en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

TAB 6

6. FEDERAL-PROVINCIAL-TERRITORIAL CLERKS MEETING

PROPOSED TALKING POINTS

- Federal-Provincial-Territorial (FPT) Clerks are meeting on January 23, 2012, and they will be discussing cyber security, among other things.

- We have a one-hour time slot that will allow us to deliver a comprehensive threat briefing, including a focus on cyber. In many ways, it will mirror the brief given to FPT Justice Ministers last year. The Canadian Security Intelligence Service and the Communications Security Establishment Canada have offered to give these presentations.

- I think it is important that the briefing focus on areas of concern for PTs, and should pay particular attention to areas where we want to invite them to get in partnership with us, such as energy, resources and risks to officials travelling abroad. There are also threats to the PTs' own systems and the sensitive economic information they hold, such as corporate financial, land use and exploration data.

- There is a keen appetite in the PT community for information on which to base decisions and priority-setting for practical outcomes on cyber security. [redacted]

s.14(a)

ISSUE

You will provide an overview of the plans for the January 23, 2012 meeting of Federal-Provincial-Territorial (FPT) Clerks, at which cyber security will be a topic of discussion.

A deck was distributed in advance of the meeting, and is enclosed for your ease of reference.

BACKGROUND

s.14(a)

[redacted]

The Privy Council Office has invited the Director of the Canadian Security Intelligence Service to provide an overall threat briefing, while the Chief of the Communications Security Establishment Canada will present on the cyber-specific threat environment.

The one-hour time commitment may also allow for general discussion on emerging threats and provide the opportunity to discuss broader FPT engagement on cyber security.

CONCLUSION

The meeting of Clerks is expected to be very positive, and should generate some momentum to further FPT collaboration on cyber security. This will be a great opportunity to arrive at some key deliverables with PTs to partner in the implementation of *Canada's Cyber Security Strategy*.

Prepared and approved by: Sébastien Labelle

UNCLASSIFIED

BUILDING A SAFE AND RESILIENT CANADA

Discussion of Cyber Security at the FPT Clerks Meeting

Presentation to DM Cyber
January 12, 2011

Background

- The Clerk of the Privy Council meets with his provincial and territorial counterparts twice per year
- Co-chaired by a PT clerk: British Columbia is co-chairing this year
- Meetings are informal in nature and typically focus on common challenges of public service management rather than serving as a forum to discuss substantive policy files
- FPT Clerks will be meeting for a full day on January 23, 2012, to address:
  - innovation in times of fiscal restraint
  - open government
  - the governance of horizontal government
  - streamlining intergovernmental business
  - security and cyber security

Page 397

is withheld pursuant to section

est retenue en vertu de l'article

14(a)

of the Access to Information

de la Loi sur l'accès à l'information

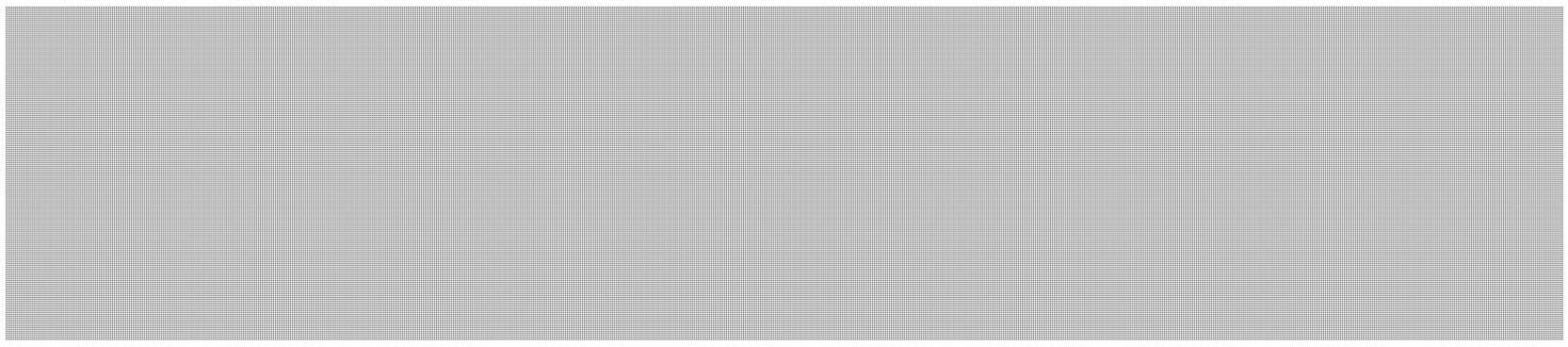
Strategic framework for PT engagement

UNCLASSIFIED

BUILDING A SAFE AND RESILIENT CANADA

- Strategic objectives for engagement are to have PTs:
  - take steps to ensure resiliency and security of their cyber systems
  - engage as active partners in areas of shared interest (e.g., critical infrastructure sectors) in line with jurisdictional roles
- The proposed FPT approach is to:
  - build trust, by systematically delivering on commitments

s.14(a)



  - establish a rhythm of working together, through regular outreach, meetings, collaboration on projects at various levels
  - seek their commitment of resources at the operational and policy levels

Current status

UNCLASSIFIED

BUILDING A SAFE AND RESILIENT CANADA

- Progress is being made:
  - initial consultations have been positive, and have informed the development of a federal engagement strategy
  - senior level FPT committee established, chaired by ADM – PS; working towards defining the elements of a shared action plan
    - a gap analysis, informed by table top exercises, is among next steps
  - PS is working with FPT Chief Information Security Officers on early deliverables
    - portal for information exchange, protocols for incident reporting, baseline assessment of PT cyber security, sharing sensitive information
  - FPT communications working group established, focusing on public awareness and incident communications coordination
  - B.C., Alberta, Manitoba, Ontario and New Brunswick have indicated a high willingness to engage, and are leaders in capability

Next steps

UNCLASSIFIED

BUILDING A SAFE AND RESILIENT CANADA

- A teleconference on December 15 with the ADM level FPT cyber security committee was held to discuss the proposed elements of a joint action plan
- Develop a regular approach for information exchange and threat briefings
- Increase the pace of collaboration with willing PTs, and show responsiveness to their priorities
- Work federally to improve the gap analysis, and to operationalize the strategic framework for PT engagement
- Invite working level PT officials to participate in shaping CCIRC products, services, tools (e.g., on the design and functionality of the Cyber Community Portale)
- Use Public Safety Canada regional offices to bring together PT emergency management and cyber security

Objectives for the Clerks meeting

UNCLASSIFIED

BUILDING A SAFE AND RESILIENT CANADA

- The Clerks' meeting is an excellent opportunity to:
  - secure support for intergovernmental collaboration on cyber security
  - reinforce our commitment to sharing more information through action
  - secure support for a multi layered approach (strategic, operational and communications)
  - recommend the review of existing emergency response protocols to asses their applicability for cyber incidents

TAB 7

7. ROUNDTABLE

During the roundtable, it is not expected that you will have any items to add.

Future

-

- situational awareness products

- SSC

- IC - agenda on cyber

UNCLASSIFIED

DATE: January 12, 2012

RDIMS No.: 532838
File No.: 384639

MEMORANDUM FOR THE DIRECTOR GENERAL

INFORMATION SHARING MEMORANDUM OF UNDERSTANDING WITH THE CANADIAN ELECTRICITY ASSOCIATION

(For approval)

ISSUE

To seek your approval of a Memorandum of Understanding (MOU) between the Canadian Cyber Incident Response Centre (CCIRC) and the Canadian Electricity Association (CEA). The MOU has received approval from Public Safety's Legal Services, and is attached at **TAB 1**.

BACKGROUND

As part of its role as Canada's National Computer Emergency Response Team (CERT), CCIRC sought to deepen existing relationships with various critical infrastructure partners. As a means to achieve this, CCIRC began exploring mechanisms to improve the two-way flow of information with industry partners at the operational level.

The initial proposal was to develop a non-disclosure agreement (NDA) with the CEA as a pilot. However, further examination by NCSD and Public Safety Legal Services concluded that the structure and language of an NDA prevented the agreement from being deployed with other critical infrastructure sectors without considerable amendments.

An MOU has been developed that will allow for sufficient flexibility to be annexed in the *Critical Infrastructure Information Sharing Framework*, a document developed in partnership with Francis Bradley, Vice President of the CEA and current Information Sharing Champion for the National Cross Sector Forum. The Framework is attached for reference at **TAB 2**.

CONSIDERATIONS

An MOU was selected as it would allow for sufficient flexibility to facilitate the two-way flow of information, without creating undue liability or risk for the signatories.

.../2

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

[redacted] Section 13 of the SOAS states:

"*Departments must ensure, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations. The agreement should represent an undertaking to safeguard information appropriately, to limit use, to control release to third parties and to inform authorized users of their responsibilities under the agreement.*"

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

[redacted]

NEXT STEPS

Francis Bradley of the CEA has approved the notion of an MOU in principle.

Provided you approve the attached agreement, NCSD will ensure concurrence with Public Safety's Critical Infrastructure and Strategic Coordination Directorate before sending it to the CEA for signature. It will then return to NCSD for your final signature and will come into force.

In the interim, the MOU will be sent for translation.

I approve_____

I do not approve_____

Sébastien Labelle
Director of Cyber Engagement and Partnerships

Prepared by: Dorian Panchyson

MEMORANDUM of UNDERSTANDING

BETWEEN

Public Safety Canada

AND

The Canadian Electricity Association

("the participants")

Concerning

The sharing and protection of information

Participants to this agreement include Public Safety Canada and the Canadian Electricity Association (the CEA), including all member companies which comprise the association.

The Participants acknowledge the following principles:

As part of Public Safety Canada, the Canadian Cyber Incident Response Centre (CCIRC) provides a federal focal point for Canada's cyber threat and vulnerability warning, analysis and response.

Information that may be exchanged by any participant to this MOU supports the development of cyber mitigation strategies for participants to enhance the overall resilience of critical infrastructure.

Information sharing and information protection pertaining to cyber security must be based on collaborative efforts between industry and government to strengthen the resiliency of critical infrastructure.

Information sharing and information protection must respect federal legislation and policies, or provincial law as the case may be.

The potential or actual inappropriate or unauthorized disclosure of information may result in harm to any participant and that risk be mitigated by the use of the "Best Practices" further described in this MOU.

1. Purpose

The purpose of this memorandum of understanding (MOU) is:

- to support the objectives of the information sharing and protection processes related to cyber security and mechanisms identified under the National Strategy and Action Plan for Critical Infrastructure and the Critical Infrastructure Information Sharing Framework; and

- to advance collaborative efforts to facilitate cyber security related information sharing among critical infrastructure partners.

2. Participants

This MOU is between Public Safety Canada, acting through the Canadian Cyber Incident Response Centre (CCIRC), and the CEA.

The CEA will sign this agreement on behalf of its thirty-four members, including:

Alberta Electric System Operator
AltaLink Management Ltd.
ATCO Electric
ATCO Power
BC Hydro and Power Authority
Capital Power Corporation
City of Medicine Hat, Electric Utility
Columbia Power Corporation
Énergie renouvelable Brookfield
ENMAX Corporation
EPCOR
FortisAlberta
FortisBC
Horizon Utilities Corporation
Hydro One Inc.
Hydro Ottawa Holding Inc.
Hydro Quebec
Independent Electricity System Operator
Manitoba Hydro
Maritime Electric Power Company
New Brunswick Power Holding Corporation
Newfoundland and Labrador Hydro (Naclor)
Newfoundland Power. Inc.
Northwest Territories Power Corporation
Nova Scotia Power Inc.
Oakville Hydro Corporation
Ontario Power Generation
Saint John Energy
Saskatoon Light & Power
SaskPower
Toronto Hydro Corporation
TransAlta
TransCanada
Yukon Energy Corporation

3. Object

The object of this MOU is to set out common principle which will surround the treatment of information shared amongst the participants of this MOU.

4. Framework

CCIRC receives sensitive information from CEA and its members on the understanding that:

- the dissemination of the information by CCIRC within or to other elements of the federal government may be restricted to those who need to know;
- the use of information received by CCIRC will be for furthering CCIRC's mandate;
- the treatment of the information by CCIRC will be consistent with all applicable law, regulations and policies published by the Treasury Board of Canada and Public Safety Canada.

The CEA and its member organizations provide sensitive information to CCIRC on the understanding that:

- federal legislation and polices provide mandatory rules, subject to certain exemptions, for the retention, disclosure and destruction of information in the custody and control of a government institution;
- adherence to best practices for the marking and transmittal of protected critical infrastructure/emergency management information facilitates the proper handling of information by CCIRC.

5. Transmittal

The accepted method of information transmittal deemed to be non-sensitive by the sending party shall be via email or via an online information sharing portal. If, however, material is deemed as sensitive, the sending party may choose to either encrypt or password protect the information. If required, the sender should confirm with the recipient when encrypted or password protected information is being sent.

For instances where the sender determines that the information is too sensitive to be sent via electronic means, information exchange can be achieved by alternative secure, traceable methods such as express, certified or registered mail or a commercial courier service. The material should be double enveloped, sealed with an inner envelope marked accordingly. When sending materials via this method, confirmation should be obtained from the recipient on their availability to receive the materials.

6. Information Management

Marking:
If the information being received by the Government is being provided in confidence, the provider of the information may wish to appropriately mark each page of the document prior to transmittal.

If a document is identified as containing critical infrastructure information provided in confidence to a government department or agency, it may be marked according to the following:

CRITICAL INFRASTRUCTURE / EMERGENCY MANAGEMENT INFORMATION PROVIDED IN CONFIDENCE TO
[*name of recipient*]

The marking should be located either at the top or bottom of each page consistently throughout the document. The marking should also appear on the outside of any front or back cover, any binder cover or folder (front and back) and any title page.

Handling and Storage of Information:
Information received under this agreement will be assessed and marked in accordance with the Security Organization and Administration Standard (SOAS) to a PROTECTED B level. Information provided will be marked as such as it is received and re-assessed with the passage of time or as new events occur. The department security officer will determine storage requirements outside a security, or high security zone on a case by case basis.

SOAS Protected information refers to specific provisions of the Access to Information Act and the Privacy Act and applies to sensitive personal, private, and business information. For internal purpose, Protected B is defined as any information that could result in grave injury, such as loss of reputation or competitive advantage.

7. Use of Information

CCIRC, in its role as Canada's National Computer Emergency Response Team (CERT), may wish to anonymize information received under this agreement into an un-attributable, aggregate state, for distribution to CCIRC partners, unless the originator of the information states otherwise.

CCIRC may wish to contact the originator of information marked SENSITIVE, should the information be deemed valuable or useful to share with partners outside of this MOU. This will be dealt with on a case-by-case basis.

8. Exclusion of confidentiality

The above responsibilities on the treatment of information will not apply to information that can be proved to be:

- in the public domain at the time of its disclosure or that later becomes publicly available without breach of this understanding;
- independently developed without reference to any Confidential Information disclosed or communicated threw this understanding;
- received from a third party without breach of any obligation of confidentiality; or
- disclosed as required by law or judicial decree.

9. Access to Information

Public Safety Canada is subject to the Access to Information Act. In the event that Public Safety Canada receives an Access to Information request for Confidential Information shared under this MOU, CCIRC will seek to enact disclosure exemptions, according to the relevant provisions contained within the Act. However, the final determination regarding the disclosure of Confidential Information remains with the Federal Court.

In all cases, Public Safety Canada will notify relevant parties and they will be given opportunity to make representations to protect its Confidential Information in the Federal Court, if necessary.

10. No legal effect

The participants, including Public Safety Canada, the CEA and its members, understand that this MOU is of no binding legal effect and no legal rights, express or implied, are created by this MOU. Nothing in this MOU supersedes or relieves the responsibility of a participant from protecting against the unauthorized or inappropriate disclosure of information.

11. Settlement of Dispute

Disputes regarding the interpretation or implementation of this MOU will be resolved by consultation between the participants and will not be referred to any other third party for settlement.

12. Amendment

This MOU may be amended only with the mutual written consent of the Participants. Further, the MOU may be subject to an annual review cycle, to ensure the agreement continues to meet the needs of the participants.

13. Duration and withdrawal

This MOU will remain in effect unless amended or terminated by the participants. This MOU may be terminated through a 30-days notice to the other participants. The participants understand that, unless otherwise indicated by the provider of the confidential information, withdrawal from this MOU in no way affects the confidential nature of any information provided to CCIRC.

14. Contacts

(1) in the case of Public Safety Canada:
Robert Dick, Director General, National Cyber Security Directorate
Public Safety Canada
340 Laurier Avenue West
Ottawa, ON
Tel: (613) 990-2661
Fax: (613) 990-3287
E-Mail: robert.dick@ps.gc.ca

(2) in the case of the Canadian Electricity Association:
Francis Bradley, Vice President, Policy Development
The Canadian Electricity Association
350 Sparks Street, Suite 1100
Ottawa, ON
Tel: (613) 230-5027
Fax: (613) 230-9326
E-Mail: bradley@electricity.ca

Robert Dick, Director General
National Cyber Security Directorate
Public Safety Canada

March 6/12
Date:

Francis Bradley
Vice President, Policy Development
The Canadian Electricity Association

Date: 21 Feb 2012

Pages 818 to / à 819

are not relevant

sont non pertinentes

Public Safety Canada
Sécurité publique Canada

Senior Assistant Deputy Minister
Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

For your meeting with: Stephen Rigby,
National Security Advisor
Date: April 19, 2012
Time: 4:30pm
Location: Boardroom 307-PSB, 59 Sparks Street

UNCLASSIFIED

DATE:

File No.: 387125
RDIMS No.: 601692

MEMORANDUM FOR THE DEPUTY MINISTER

MEETING WITH THE NATIONAL SECURITY ADVISOR ON THE AUDIT OF CYBER SECURITY AND CRITICAL INFRASTRUCTURE

(For Information)

ISSUE

You are scheduled to meet with the National Security Advisor, the Secretary of the Treasury Board of Canada, and the Chief of Communications Security Establishment Canada (CSEC) on April 19, 2012, to discuss the Office of the Auditor General's (OAG) audit of protecting Canada's critical infrastructure against cyber threats. A deck (**TAB A**) is enclosed to frame the discussion.

You will be accompanied by Graham Flack, Associate Deputy Minister, and Lynda Clairmont, Senior Assistant Deputy Minister, National Security Branch.

BACKGROUND

On August 31, 2011, the OAG sent you a letter providing notice of intent to audit the implementation of *Canada's Cyber Security Strategy* (the Cyber Strategy).
On December 22, 2011, the OAG sent you an Audit Plan Summary for review, noting that the focus of the audit will be on the protection of critical infrastructure against cyber threats. Specific lines of inquiry included:

- to determine whether departments/agencies are leading activities to secure critical infrastructure from cyber threats, in partnership with provinces, territories, the private sector and international allies;

- to determine whether roles and responsibilities for securing the Government's critical infrastructure against cyber threats are being exercised as defined; and

- to determine whether Public Safety Canada is helping to increase the awareness of Canadians against cyber threats.

s.21(1)(b)

[redacted]

- announce the *National Strategy and Action Plan for Critical Infrastructure* (which was announced on May 28, 2010); and

- provide guidance to departments/agencies for identifying critical infrastructure (development of a methodology is still underway).

In April 2012, the OAG met with the Privy Council Office to discuss their preliminary findings, including:

s.21(1)(b)

- [redacted]

- [redacted]

[redacted]

NEXT STEPS

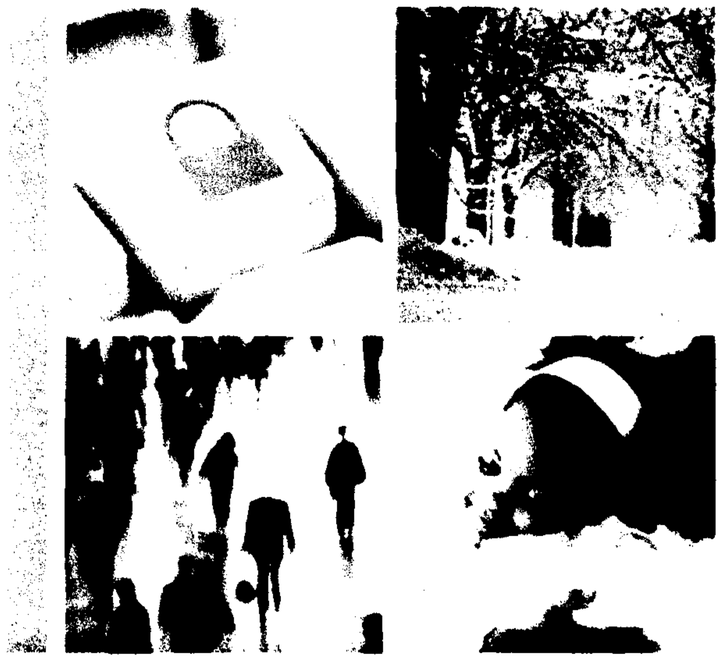
You are scheduled to meet with the OAG in April 2012 (date still to be determined), which provides an opportunity [redacted]

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Suki Wong, Director General, Critical Infrastructure and Strategic Coordination at 613-991-3583.

for Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Enclosure: (1)

Public Safety Canada | Sécurité publique Canada



Audit of Protecting Canada's Critical Infrastructure Against Cyber Threats

Canada

Context

- On August 31, 2011, the Office of the Auditor General (OAG) sent a letter to the Deputy Minister of Public Safety (PS), providing notice of intent to audit the implementation of *Canada's Cyber Security Strategy* (the Strategy)

- On December 22, 2011, the OAG sent an Audit Plan Summary to the Deputy Minister of PS for review, noting that the focus of the audit is on the protection of critical infrastructure from cyber threats
  - *Line of enquiry #1*: To determine whether departments/agencies are leading and coordinating activities to secure critical infrastructure, in partnership with provinces/territories, the private sector and international allies
  - *Line of enquiry #2*: To determine whether roles and responsibilities for securing the Government's critical infrastructure against cyber threats are being exercised as defined
  - *Line of enquiry #3*: To determine whether PS is helping to increase the awareness of Canadians against cyber threats

Pages 1250 to / à 1255

are withheld pursuant to section

sont retenues en vertu de l'article

21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Page 1256

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

Next Steps

s.21(1)(b)

- The Deputy Minister of PS is scheduled to meet with the OAG in April 2012, which provides an opportunity

[redacted]

Office of the Auditor General of Canada
Bureau du vérificateur général du Canada

6 December 2011

Ms. Rosemary Stephenson
Chief Audit Executive
Internal Audit Directorate
Department of Public Safety and Emergency Preparedness
269 Laurier Avenue West, Suite 11D5000
Ottawa, Ontario K1A 0P8

Dear Ms. Stephenson:

As part of our performance audit of the protection of Canada's critical infrastructure from cyber threats to be reported in the Fall 2012 Report of the Auditor General, we have developed, in draft, audit objectives and a set of audit criteria for the audit. Prior to issuing a final version of the Audit Summary Plan for your department's formal response, we would like to provide you with an opportunity to comment on these objectives and criteria. We would appreciate receiving comments prior to the end of day on 13 December 2011.

Please note that the attached excerpt is in English only. As it is labelled <NOT TO BE COPIED>, we have provided you with five copies of the Audit Plan Summary numbered 08-4001 to 08-4005. As agreed in your response to our letter of 29 August 2011, please respect the confidentiality of the information in this document.

If you have any questions or would like to meet, please do not hesitate to call Jean Goulet or me at 613-995-3708.

Yours sincerely,

Edward Wood, P. Eng.
Principal

Encl., Excerpt of the Audit Plan Summary, dated 6 December 2011, copies 08-4001 to 08-4005.

240 rue Sparks Street, Ottawa, Ontario K1A 0G6

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

December 16, 2011

Mr. Edward Wood, Principal
Auditor General of Canada
240 Sparks Street
Ottawa, Ontario
K1A 0G6

Dear Mr. Wood,

Thank you for providing us with the opportunity to review the content of the draft version of the Audit Plan Summary of the performance audit of the protection of Canada's critical infrastructure from cyber threats.

s.21(1)(b)

The responsible Public Safety Canada officials have reviewed the document for accuracy of the facts, as well as any omissions, new information, or context changes.

Canada

s.21(1)(b)

[redacted]

Please consider these comments in the preparation of your final Audit Plan Summary.

Should you have any questions, please do not hesitate to contact me at (613) 949-0472.

Sincerely,

Rosemary Stephenson, CIA, CISA
Chief Audit Executive
Public Safety Canada

Enclosure: Excerpt of the Audit Plan Summary, dated December 2011, copies 08-4001 to 08-4005.

Office of the Auditor General of Canada
Bureau du vérificateur général du Canada

22 December 2011

Mr. William V. Baker
Deputy Minister
Deputy Minister's Office
Department of Public Safety and Emergency Preparedness
269 Laurier Avenue West, Suite 19B-1900
Ottawa, Ontario K1A 0P8

Dear Mr. Baker:

In my letter dated 31 August 2011, I notified you that we were beginning a performance audit of Cyber Security Strategy to be reported in the Fall 2012 Report of the Auditor General.

We have now developed the objectives and criteria for this audit, presented in the attached Audit Plan Summary. The standards for assurance engagements set by the Canadian Institute of Chartered Accountants require that you acknowledge, in writing, your organization's responsibility for the protection of Canada Critical Infrastructure from Cyber Threats, as described in the *Entity Management Responsibility* section of the Audit Plan Summary and whether you agree with the audit objectives and criteria as stated. A suggested letter of acknowledgement is attached for your convenience.

Please review the Audit Plan Summary with your management team and reply **no later than 13 January 2012.**

We are providing you with 5 copies of the Audit Plan Summary numbered 08-4059 to 08-4063. These are labelled "NOT TO BE COPIED, Draft Document for the purposes of fact verification and comment only, Property of the Office of the Auditor General of Canada, Protected A". As acknowledged in your response to my notification letter, the information in the Audit Plan Summary is to be kept confidential. If you require additional copies, we will be pleased to provide them. We remind you that all controlled documents must be returned to us no later than one week after tabling of the relevant report in the House of Commons.

.../2

240 rue Sparks Street

We would be pleased to meet with you and/or departmental managers to discuss the Audit Plan Summary. Please do not hesitate to call Edward Wood, Audit Principal, Jean Goulet, Audit Director or me at 613-995-3708.

Yours sincerely,

Wendy Loschiuk
Assistant Auditor General

Encl. Audit Plan summary of Cyber Security Strategy, dated 21 December 2011, copies numbered 08-4059 to 08-4063

c.c.: Rosemary Stephenson, Chief Audit Executive, PS
Edward Wood, Principal, OAG

Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

PROTECTED A

JAN 16 2012

Ms. Wendy Loschiuk
Assistant Auditor General
Office of the Auditor General of Canada
240 Sparks Street
Ottawa, Ontario K1A 0G6

Dear Ms. Loschiuk:

This is to respond to your letter dated December 22, 2011 regarding your performance audit of the *Protection of Canada's Critical Infrastructure from Cyber Threats* to be reported in the Fall 2012 Report of the Auditor General.

I would like to thank the Office of the Auditor General (OAG) for sharing the Audit Plan Summary. The extensive details included in this document will help ensure that we are prepared to work effectively with the audit team and contribute to a successful report.

As Deputy Minister of Public Safety Canada, I acknowledge responsibility as set out in the Audit Plan Summary under the sections "Management's Responsibility" and "Audit Objectives." I agree that the criteria set out in the document are suitable as a basis for assessing whether the audit objectives have been met.

Based on the notice of intent letter dated August 31, 2011,

s.21(1)(b)

The CI Strategy commits the Department to strengthening the resilience of critical infrastructure from all hazards, such as natural disasters, terrorist attacks, pandemics and cyber threats.

.../2

Canada

s.21(1)(b)

[redacted]

While I appreciate that the audit plan has been structured to show the potential impact of cyber threats to Canadians, [redacted]

s.14(a)

[redacted] and helps shape the implementation of Canada's Cyber Security Strategy.

Concerning the third line of enquiry, it would be worthwhile to obtain some additional information or clarification about how the OAG intends to conduct its examination of its third line of enquiry: *"To determine whether Public Safety Canada is helping to increase the awareness of Canadians against cyber threats."* In the Audit Scope and Approach section, the Summary only states that "we will examine Public Safety Canada's role in increasing Canadians' awareness of keeping safe online." [redacted]

s.21(1)(b)

We look forward to working with the audit team and receiving further clarification, as noted above.

Sincerely,

William V. Baker

c.c. Ms. Lynda Clairmont
Assistant Deputy Minister
National Security

Ms. Stéphanie Durand
Director General
Communications

Pages 1372 to / à 1378

are not relevant

sont non pertinentes

Pages 1393 to / à 1396

are withheld pursuant to section

sont retenues en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1)(a)

[redacted]

- the development of a cyber foreign policy, led by the Department of Foreign Affairs and International Trade;

- the Government's cyber defence initiative, led by the Treasury Board of Canada Secretariat; and

- the development of a national framework for responding to a cyber incident, led by Public Safety Canada.

- Deputies also expressed an interest in being debriefed on:

  - the mechanisms in place for information sharing inside and outside government; and

  - the progress in establishing Shared Services Canada. [redacted]

s.15(1)(i)

[redacted]

- These items will be brought forward to the notional June 2012 DM Cyber meeting.

Gallagher,Stephanie

From: Gallagher,Stephanie on behalf of Gorman, Denis
Sent: May-14-12 11:49 AM
To: Gallagher,Stephanie
Subject: FW: post-session note (Preliminary discussion of 31 Jan 2012 - Horizontal Evaluation of "Cyber Security Strategy")
Attachments: PS-SP-#544886-1-CEE HOE 28 Jan 2011 Evaluating Policy - FIN presentation - EN .PDF; PS-SP-#544889-1-CEE HOE 28 Jan 2011 Evaluating Policy - FIN presentation - FR.PDF; PS-SP-#556894-1-DEC - SP Protocole pour les évaluations horizontales menées par... - fév 2010.PPT; PS-SP-#556891-1-DEC - PS Protocol for OGD-led Horizontal Evaluations - Feb 2010.PPT

Stephanie Gallagher
Office Manager | Gestionnaire de Bureau
Evaluation | Évaluation
Public Safety Canada | Sécurité publique Canada
Tel: 613-993-9558
Fax: 613-949-3189

From: Kelland, Stephen
Sent: March-27-12 11:17 AM
To: Sandrock, Sharla
Cc: Gorman, Denis
Subject: FW: post-session note (Preliminary discussion of 31 Jan 2012 - Horizontal Evaluation of "Cyber Security Strategy")

Per my email of moments ago – this is a ***reference*** email, for a sense of what occurred and who was in attendance.

Sharla – key message from the meeting as conveyed by Denis was…

> Public Safety Canada, in consultation with the heads of Evaluation from the partner departments/agencies has proposed that the evaluation occur in 2015-2016. PS will integrate this evaluation into its 2012 Departmental Evaluation Plan. Funding for this initiative has been adequately provided for so long as participating organizations agree to carry-out their own field work.

The above was also communicated to FIN and Cyber POCs at PS. The funding issue/point is critical.

From: Kelland, Stephen
Sent: February-01-12 16:02
To: [redacted] Ramona.Helm@tbs-sct.gc.ca; Petrus, Elena (Elena.Petrus@tbs-sct.gc.ca); Brigitte Hébert (Brigitte.Hebert@tpsgc-pwgsc.gc.ca)
Cc: Gorman, Denis; [redacted] Mike.Milito@tbs-sct.gc.ca; graham.barr@tpsgc-pwgsc.gc.ca; Kelland, Stephen
Subject: post-session note (Preliminary discussion of 31 Jan 2012 - Horizontal Evaluation of "Cyber Security Strategy")

Good day, ***Colleagues*** – to follow up from our meeting yesterday, thanks for taking the time to attend on short notice. Below and attached is some additional documentation for your reference, which we hope you can access and that you will find helpful/useful for retention purposes. It is, as follows:

s.15(1) - Subv

1) **Protocol** – EN & FR versions of the PS 'Protocol' for how we engage and participate in evaluations led by other government departments and agencies; and,
2) **Evaluating Policy** – EN & FR versions of a FIN presentation at a TBS-CEE Heads of Evaluation forum on how that department is facing the challenges of evaluating policy.

(For initial invitees that could not attend, you are cc'd on this email for your awareness.)

Per Denis' comments on the way forward in the coming months, we are in liaison with our primary PS program representative (Sébastien Labelle – Director, Engagement and Partnership - National Cyber Security) to determine the appropriate contacts from all Cyber partner departments/agencies.

Thank you.
Stephen

From: Kelland, Stephen
Sent: January-26-12 10:10
To: 'Mike.Milito@tbs-sct.gc.ca'; 'graham.barr@tpsgc-pwgsc.gc.ca'; Jimenez, Rosanne (Rosanne.Jimenez@tbs-sct.gc.ca)
Cc: Gorman, Denis; 'debbie.konecny@tpsgc-pwgsc.gc.ca'; Gallagher,Stephanie
Subject: Meeting request (preliminary discussion) - Horizontal Evaluation of "Cyber Security Strategy"

Good day, ***Evaluation Colleagues*** –

We request a meeting with you next Monday, 30 January (10:00) or Tuesday, 31 January (14:00 or 2 pm) to hold a preliminary discussion on the evaluation approach for a horizontal file on which your respective organizations are all included in the latest "ask" document, which will very soon be under ministerial review and consideration. The idea is to engage you as the principals on the Cyber Security Strategy file, in terms of evaluation, i.e. TBS, SSC, and CSEC.

With apology for the short fuse on this request, we are subject to the "ask" document process, which we understand is proceeding quickly. Pending your response, we will send an invitation to our offices located at 257 Slater Street. Please advise of your availability, by return email.

For CSEC, we have consulted the Centre of Excellence for Evaluation to assist in contacting you in a timely fashion. Ms. Jimenez, further to our telephone conversation, please pass to the Head of Evaluation.

Thank you.

Stephen

Stephen Kelland
Director - Evaluation / Directeur - Évaluation
Public Safety Canada / Sécurité publique Canada
T: (613) 990-6693 F: (613) 949-3189
Stephen.Kelland@ps-sp.gc.ca

Department of Finance Canada | Ministère des Finances Canada

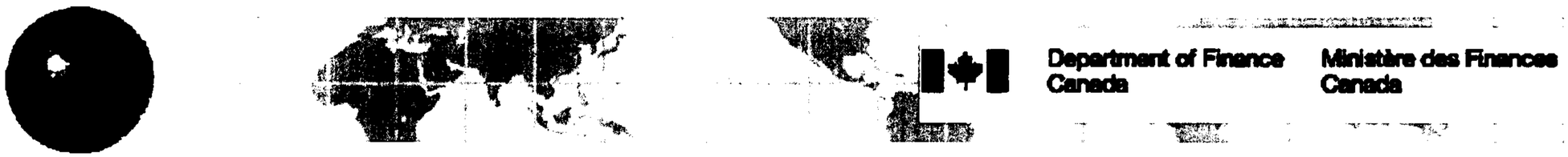
Finance Canada Evaluation Study of the Economic Studies and Policy Analysis Division (ESPAD)

Presented to: Heads of Evaluation Meeting, January 28, 2011

(Prepared January 26, 2011)

Presentation Outline

- Overview of the Evaluation Project
- Evaluation Study Objectives and Scope
- Evaluation Issues and Challenges
- Evaluation Approach
- Evaluation Study Methodology
- Evaluation Progress to Date
- Appendices
  - Appendix A: Evaluation Questions
  - Appendix B: The Balanced Scorecard Approach
  - Appendix C: Schacter's Quality Criteria

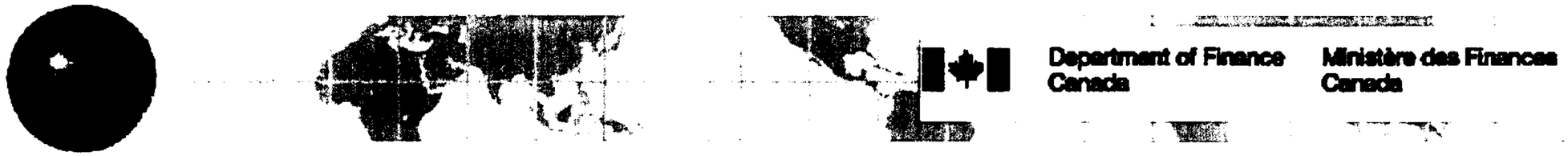


Overview of the Evaluation Project

- The purpose of today's presentation is to share our pilot approach to evaluating a policy program: the Economic Studies and Policy Analysis Division (ESPAD).
- ESPAD is one of three divisions in the Economic and Fiscal Policy Branch, one of the six policy branches at Finance.
- ESPAD is the largest policy research group within Finance, and one of the largest in the Government.
- ESPAD has two fundamental objectives:
  - Excellence in conducting policy-relevant research; and
  - Excellence in communicating policy relevant research.

Evaluation Objectives and Scope

- The evaluation study assesses the relevance and performance of the Division through examining client services, internal processes, financial and human resources management.
- Taking into consideration, but not limited to:
  - Extent to which key objectives and results are being achieved, such as the provision of timely and high-quality policy-relevant research;
  - Extent to which resource utilization relates to the production of outputs and progress toward expected outcomes;
  - Extent to which current and anticipated needs of clients drive the organization and its research programs; and
  - Lessons learned and best practices.



Evaluation Issues & Challenges

- Extensive research was undertaken on the "evaluability" of the policy advice and research function.
- No clear-cut causal link between policy advice and policy decisions; therefore cannot use implementation of policy advice as an outcome.
  - Example: Steel tariffs
- Nevertheless, there are inputs required to develop policy advice, and there are outputs and immediate outcomes, such as access to quality advice, that are expected as a result. So the input, process, output and to some extent, outcomes, can all be evaluated.

Evaluation Issues & Challenges cont'd

- Example: Tariffs on imported steel
  - Classic economic argument against tariffs: distort free trade
    - Domestic producers produce and sell more at the higher domestic price, as they are protected from foreign competitors who may be more efficient producers.
    - Tariffs benefit domestic producers and the government (tariff revenue) at the expense of consumers (who pay a higher price for the same good); the net economic effects on the importing country are negative.
  - However, say a government is elected on a platform that includes protecting the steel industry from foreign competition.
  - Despite sound economic policy advice, the government may choose to impose tariffs on foreign steel because of its prior commitment.

Evaluation Approach

- Finance invested a considerable amount of resources into planning the evaluation:
  - Researched and adapted leading practices from evaluations, performance management and other related fields.
  - Recognized the distinct nature of this evaluation which focuses more on the process, outputs and immediate outcomes of an organization, and includes some analysis of intermediate outcomes.
- Conclusion – Focus on the quality of the policy-advice and its development process:
  - Examine to what extent the policy analysis and advice function is relevant and of high quality, timely, and efficiently produced.
  - To the extent possible, assess the usefulness of policy advice for senior management.

Evaluation Approach *cont'd*

- Our evaluation approach combines and integrates traditional evaluation methods with innovative tools:
  - Treasury Board Policy on Evaluation as the guiding framework for evaluation issues to be addressed.
  - The Balanced Scorecard approach as a goal setting and performance measurement tool, which focuses on four key dimensions for monitoring and improving results: clients, internal processes, financial resources and people.
  - Quality management principles to assess the importance and the level of satisfaction with key outputs.
  - Schacter's criteria for quality of policy advice: timely, based on adequate consultations, clearly articulated purpose, sound logical basis, sound evidence base, balanced, presents a range of viable options for actions, relevant, well presented and pragmatic.

Evaluation Study Methodology

- Multiple Lines of Evidence and Collection Methods Used
- Review of Literature and Documents/Files
- Key Informant Interviews: with ESPAD staff, clients, senior management and external stakeholders.
- Service Survey: rates the importance and level of satisfaction with the outputs of the Division from both researcher and client perspectives.
- Case Studies: in-depth examination of selected research outputs better understand the research development process and the extent to which the outputs met quality criteria.

Evaluation Progress to Date

- Planning the evaluation
  - Evaluation Team worked with experienced consultants who assisted the team to research best practices and develop an effective and pragmatic approach to the evaluation of the policy advice function and policy research function (June 2009- March 2010).
  - Developed a program profile, including performance measurement information (February- June 2010).
  - Developed and finalized the Terms of Reference (April-July 2010), taking into consideration comments provided by senior management, while maintaining impartial perspective

Evaluation Progress to Date *cont'd*

- Conducting the evaluation (July 2010 to Present)
  - Completed extensive literature and document review.
  - Developed interview guides for ESPAD staff, clients and external stakeholders.
  - Developed survey tool.
  - Selected case studies, which are underway.
- Next steps?
  - Finalize data collection and analysis.
  - Prepare evaluation report, including management response.
  - Present final report to Audit and Evaluation Committee.
  - Draw and share lessons, best practices from this pilot study.

Appendices

Appendix A: Evaluation Questions

- **Relevance**
  - Are the Divisional mission, objectives and activities still relevant and consistent with the strategic objectives of Finance Canada and government priorities?
  - Is there still need for the Federal Government to be involved and are there effective alternatives?

- **Performance: Design and Implementation**
  - Does the organizational structure support the effective execution of the Division's mandate?
  - Are the structures, mechanisms and processes in place for monitoring the quality of activities and outputs and the satisfaction of clients, adequate and appropriate?
  - Are adequate processes and mechanisms in place to liaise and cooperate with the policy research community both inside and outside the country?

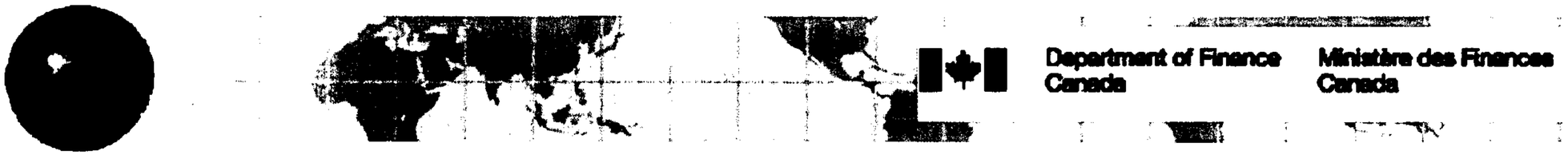
Appendix A: Evaluation Questions *cont'd*

- **Performance: Achievement of Expected Outcomes**
  - Has the Division been able to meet its objectives in terms of quality/quantity of research and other outputs?
  - Has the Division been able to influence/inform the development and understanding of fiscal/budgetary and other policies?

- **Performance: Efficiency and Economy**
  - Has the level of demand for services/products changed over time, and has there been a corresponding change in level of resources?
  - Is organizational knowledge captured and integrated into work tools and the decision making process in a timely manner?
  - Are there alternative approaches that could improve efficiency and results?

Appendix A:Evaluation Questions cont'd

- **Human Resources**
  - Are the management practices, working environment and culture conducive to producing quality research?
  - Are HR practices for the recruitment, training, development and retention of highly skilled staff working effectively?
- **Financial Resources**
  - In recent years how has the level of funding (FTEs and $) evolved?
  - What are the key linkages between inputs and outputs?



Appendix B: The Balanced Scorecard Approach

- The Balanced Scorecard Approach focuses on four dimensions for improving results: clients, internal processes, financial resources and people (staff learning and growth).

- This framework recognizes that achieving results depends on having the right products and services to satisfy client needs, which in turn requires having the right processes in place to produce the products and services needed by clients. Furthermore, to be effective, the processes should be operated by employees with the right knowledge and training.

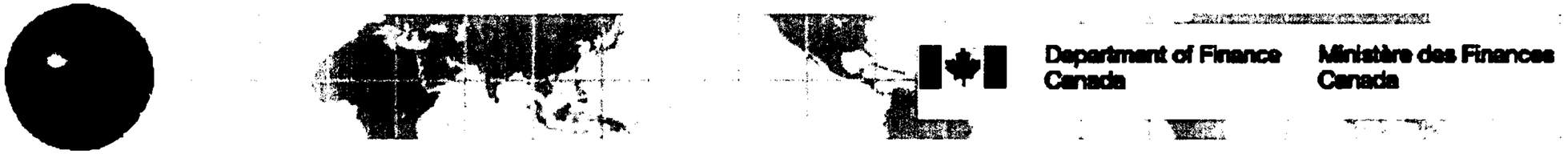
- It also takes into consideration the level of financial resources available e.g., more dollars translate into higher expectation of performance.

Robert S. Kaplan and David P. Norton. The Balanced Scorecard - Measures that Drive Performance", Harvard Business Review, Feb. 1992

Appendix C: Schacter's Quality Criteria

- Timeliness – Was it ready when the Minister and other decision-makers needed it;
- Was it based on adequate consultation with stakeholders inside and outside government;
- Did it clearly articulate the purpose for which it was prepared;
- Did it have a sound logical basis – there was a clear description and articulation of the links between fact and assumptions on the one hand, and conclusions and recommendations on the other;
- Was it based on sound evidentiary basis – the underlying evidence was accurate and complete;
- Was the advice balanced – it presented a representative range of viewpoints;
- Did it present an adequate range of viable options for action;
- Was it relevant to the situation faced by decision-makers – did it take into account the realities (including political realities) and did it anticipate related developments;
- Was it well-presented to the reader – the prose was concise; the text was well organized, the presentation was clear; and
- Was it pragmatic – it kept in mind implementation issues.

Mark Schacter, *The Worth of a Garden – Performance Measurement and Policy Advice in the Public Service – A discussion paper,* March 7, 2006.



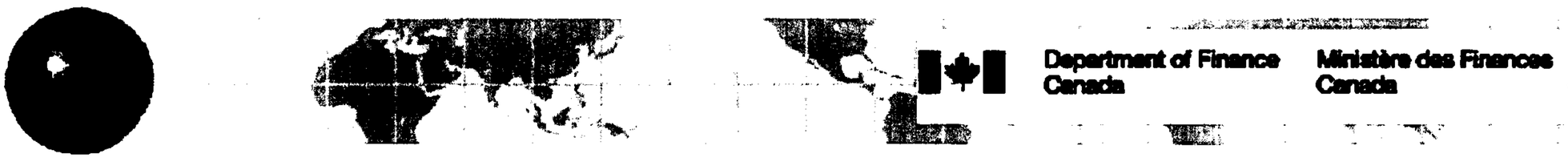
Étude d'évaluation de la Division des études économiques et de l'analyse des politiques (DEEAP) de Finances Canada

Présentée à la réunion du 28 janvier 2011 des chefs de l'évaluation

(Préparée le 26 janvier, 2011)

Aperçu de la présentation

- Aperçu du projet d'évaluation
- Objectifs et portée de l'étude d'évaluation
- Enjeux et défis de l'évaluation
- Approche de l'évaluation
- Méthodes de l'étude d'évaluation
- Progrès de l'évaluation à ce jour
- Appendices
  - Appendice A: Questions d'évaluation
  - Appendice B: L'approche du tableau de bord équilibré
  - Appendice C: Critères de qualité de Schacter

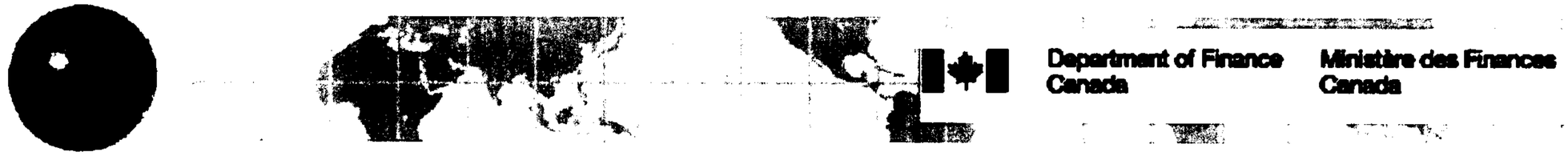


Aperçu du projet d'évaluation

- Le but de la présentation d'aujourd'hui est de partager notre approche pilote à l'évaluation d'un programme de politiques : la Division des études économiques et de l'analyse de la politique (DEEAP).
- La DEEAP est l'une des trois divisions de la Direction de la politique économique et fiscale, une des six directions de politiques des Finances.
- La DEEAP est le plus important groupe de recherche sur les politiques au sein des Finances, et l'un des plus importants au gouvernement.
- La DEEAP a deux objectifs fondamentaux :
  - Excellence dans la réalisation de recherches stratégiques;
  - Excellence dans la communication de recherches stratégiques.

Objectifs et portée de l'évaluation

- L'étude d'évaluation portera sur la pertinence et le rendement de la Division, évalués selon le service à la clientèle, les processus internes et la gestion des ressources financières et humaines.
- Elle prendra entre autres en considération :
  - la mesure dans laquelle les principaux objectifs et résultats sont atteints, par exemple de fournir des recherches stratégiques pertinentes, opportunes et de qualité;
  - la mesure dans laquelle l'utilisation des ressources se rattache à la production d'extrants et aux progrès réalisés dans l'atteinte des résultats escomptés;
  - la mesure dans laquelle les besoins actuels et prévus des clients orientent l'organisation et ses programmes de recherche;
  - les leçons retenues et pratiques exemplaires.



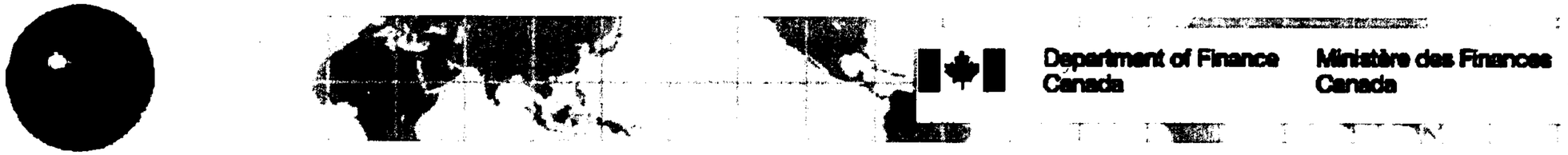
Department of Finance Canada | Ministère des Finances Canada

Enjeux et défis de l'évaluation

- Des recherches approfondies ont été entreprises quant à « l'évaluabilité » de la fonction de conseil stratégique et recherche.
- Il n'y a pas de lien net entre les conseils stratégiques et les décisions stratégiques; il n'est donc pas possible d'utiliser la mise en œuvre des conseils stratégiques comme résultat.
  - Exemple : mesures tarifaires imposées à l'acier
- Néanmoins, des intrants sont requis pour l'élaboration de conseils stratégiques, et des extrants et résultats immédiats, comme l'accès à des conseils de qualité, sont attendus en tant que résultat. Ainsi, les intrants, le processus, les extrants et, dans une certaine mesure, les résultats peuvent tous être évalués.

Enjeux et défis de l'évaluation *suite*

- Exemple : mesures tarifaires imposées à l'acier importé
  - Argument économique classique à l'encontre des mesures tarifaires : distorsion du libre-échange
    - Les producteurs nationaux produisent et vendent davantage au prix intérieur plus élevé puisqu'ils sont protégés contre des concurrents étrangers qui pourraient être des producteurs plus efficaces.
    - Les mesures tarifaires profitent aux producteurs nationaux et au gouvernement (recettes tarifaires) aux dépens des consommateurs (qui paient un prix plus élevé pour le même produit); l'incidence économique nette sur le pays importateur est négative.
  - Cependant, disons qu'un gouvernement est élu grâce à un programme qui prévoit la protection de l'industrie sidérurgique contre la concurrence étrangère.
  - Malgré des conseils éclairés en matière de politique économique, le gouvernement pourrait choisir d'imposer des mesures tarifaires à l'acier étranger en raison de son engagement antérieur.



Approche de l'évaluation

- Les Finances ont investi une quantité considérable de ressources dans la planification de l'évaluation :
  - Ont fait des recherches et adapté les principales pratiques tirées des évaluations, de la gestion du rendement et d'autres domaines liés.
  - Ont reconnu la nature distincte de cette évaluation, qui met davantage l'accent sur le processus, les extrants et les résultats immédiats d'une organisation, y compris l'analyse de certains résultats intermédiaires.
- Conclusion – Mettre l'accent sur la qualité des conseils stratégiques et leur processus d'élaboration :
  - Voir dans quelle mesure la fonction de conseil et d'analyse stratégique est pertinente et de qualité, opportune et efficace.
  - Dans la mesure du possible, évaluer l'utilité des conseils stratégiques pour la haute gestion.

Approche de l'évaluation *suite*

- Notre approche de l'évaluation combine et intègre des méthodes d'évaluation traditionnelles et des outils novateurs :
  - La Politique sur l'évaluation du Conseil du Trésor en tant que cadre directeur pour les questions d'évaluation devant être réglées.
  - L'approche du tableau de bord équilibré en tant qu'outil de détermination des objectifs et de mesure du rendement, qui met l'accent sur quatre dimensions pour le contrôle et l'amélioration des résultats : clients, processus internes, ressources financières et personnes.
  - Les principes de gestion de la qualité pour évaluer l'importance et le degré de satisfaction à l'égard des principaux extrants.
  - Les critères de Schacter concernant la qualité des conseils stratégiques : opportuns, fondés sur des consultations adéquates, but clairement articulé, fondement logique solide, source de données valables, équilibré, comportant un éventail de possibilités d'action viables, pertinent, bien présenté et pragmatique.

Méthodes de l'étude d'évaluation

- De multiples sources de données et méthodes de collecte sont utilisées

  - Examen de la littérature et des documents et dossiers

  - Entrevues avec les principaux informateurs : avec le personnel de la DEEAP, les clients, la haute direction et les intervenants externes.

  - Sondage sur le service : quantifie l'importance et le degré de satisfaction à l'égard des extrants de la Division, du point de vue tant des chercheurs que des clients.

  - Études de cas : examen approfondi d'extrants de recherche choisis pour mieux comprendre le processus d'élaboration de la recherche et la mesure dans laquelle les extrants ont satisfait aux critères de qualité.

Progrès de l'évaluation à ce jour

- Planification de l'évaluation
  - Travail avec des consultants d'expérience qui ont aidé l'équipe à rechercher les pratiques exemplaires et à élaborer une approche efficace et pragmatique à l'évaluation de la fonction de conseil stratégique et de la recherche stratégique (juin 2009 à mars 2010).
  - Élaboration d'un profil de programme, y compris des renseignements sur la mesure du rendement (février à juin 2010).
  - Élaboration et finalisation du mandat (avril à juillet 2010), en considération des commentaires fournis par la haute gestion, cependant gardant une perspective objective.

Progrès de l'évaluation à ce jour

suite

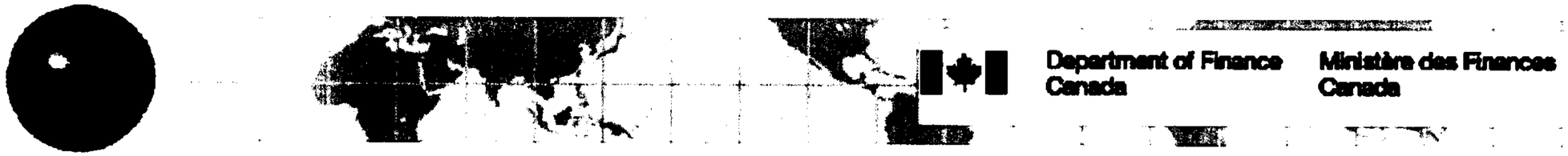
- Tenue de l'évaluation (juillet 2010 jusqu'à maintenant)
  - Examen exhaustif de la littérature et des documents achevé.
  - Guides d'entrevue pour le personnel de la DEEAP, les clients et les intervenants externes élaborés.
  - Outil de sondage élaboré.
  - Études de cas choisies et en cours.
- Prochaines étapes?
  - Achever la collecte et l'analyse des données.
  - Préparer le rapport d'évaluation, y compris la réponse de la direction.
  - Présenter le rapport final au Comité de vérification et d'évaluation.
  - Définir les leçons et les pratiques exemplaires de l'étude pilote et les communiquer.

Appendices

Appendice A: Questions d'évaluation

- **Pertinence**
  - La mission, les objectifs et les activités de la Division sont-ils toujours pertinents et conformes aux objectifs stratégiques de Finances Canada et aux priorités du gouvernement?
  - La participation du gouvernement fédéral est-elle toujours nécessaire et y a-t-il des solutions de rechange efficaces?

- **Rendement : Conception et mise en œuvre**
  - La structure organisationnelle appuie-t-elle l'exécution efficace du mandat de la Division?
  - Est-ce que les structures, mécanismes et processus qui sont en place pour contrôler la qualité des activités et des extrants ainsi que la satisfaction des clients sont adéquats et appropriés?
  - Est-ce que des processus et mécanismes adéquats sont en place pour communiquer et collaborer avec la collectivité de la recherche stratégique tant au pays qu'à l'étranger?



Appendice A: Questions d'évaluation

suite

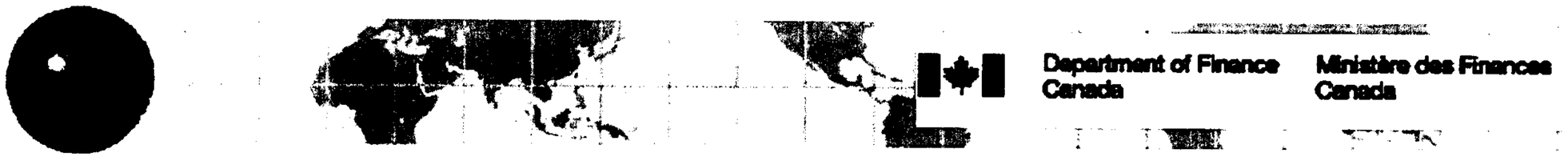
- **Rendement : Atteinte des résultats escomptés**
  - La Division a-t-elle pu atteindre ses objectifs en termes de qualité et de quantité de recherche et d'autres extrants?
  - La Division a-t-elle pu fournir une orientation ou des renseignements aux fins du développement et de la compréhension de la politique budgétaire et d'autres politiques?

- **Rendement : Efficacité et économie**
  - Le niveau de la demande de services et de produits a-t-il changé avec le temps, et y a-t-il eu un changement correspondant du niveau des ressources?
  - Le savoir organisationnel est-il saisi et intégré en temps opportun dans les outils de travail et le processus de prise de décision?
  - Y a-t-il d'autres approches qui permettraient d'améliorer l'efficacité et les résultats?

Appendice A: Questions d'évaluation

suite

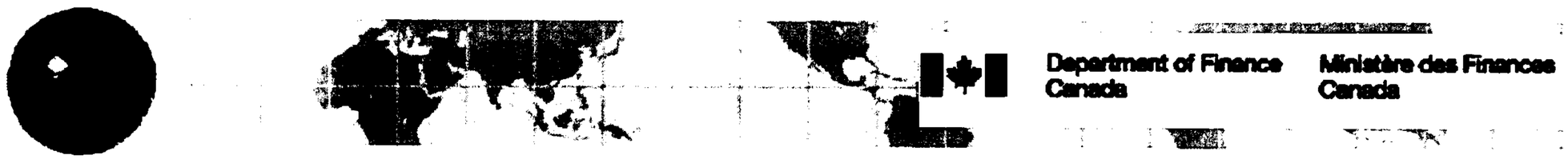
- **Ressources humaines**
  - Les pratiques de gestion, le milieu de travail et la culture sont-ils propices à la réalisation de travaux de recherche de qualité?
  - Les pratiques des RH en matière de recrutement, de formation, de perfectionnement et de maintien en poste des employés hautement qualifiés fonctionnent-elles efficacement?
- **Ressources financières**
  - Au cours des dernières années, comment le niveau de financement (ETP et $) a-t-il évolué?
  - Quels sont les principaux liens entre les intrants et les extrants?



Appendice B: L'approche du tableau de bord équilibré

- L'approche du tableau de bord équilibré met l'accent sur quatre dimensions pour améliorer les résultats : les clients, les processus internes, les ressources financières et les personnes (apprentissage et croissance du personnel).
- Ce cadre reconnaît que l'atteinte de résultats dépend du fait de disposer des bons produits et services pour répondre aux besoins des clients, ce qui exige que les bons processus soient en place pour produire les produits et services dont ont besoin les clients. De plus, pour que les processus soient efficaces, ils doivent êtres effectués par des employés ayant les bonnes connaissances et la bonne formation.
- Il tient également compte du niveau des ressources financières disponibles, p. ex. des ressources financières plus élevées se traduisent par des attentes plus élevées en matière de rendement.

Robert S. Kaplan et David P. Norton, The Balanced Scorecard - Measures that Drive Performance", Harvard Business Review, février 1992



Appendice C: Critères de qualité de Schacter

- Opportunité – Est-ce que le produit était prêt lorsque le ministre et d'autres décideurs en avaient besoin?
- Est-ce que le produit était fondé sur une consultation adéquate des intervenants de l'intérieur et de l'extérieur du gouvernement?
- Est-ce que le produit énonçait clairement le but pour lequel il a été préparé?
- Le produit avait-il un fondement logique solide? – il y avait une description et un énoncé clairs des liens entre les faits et hypothèses d'un côté, et les conclusions et recommandations de l'autre côté;
- Le produit était-il fondé sur une source de données valables? – les données sous-jacentes étaient exactes et complètes;
- Les conseils étaient-ils équilibrés? – ils constituaient un éventail représentatif de points de vue;
- Le produit présentait-il un éventail adéquat de possibilités d'action viables?
- Le produit était-il pertinent eu égard à la situation à laquelle faisaient face les décideurs? – tenait-il compte de la réalité (y compris en matière de politiques) et prévoyait-il les développements connexes?
- Le produit a-t-il été bien présenté au lecteur? – le libellé était concis; le texte était bien organisé; la présentation était claire;
- Le produit était-il pragmatique? – il tenait compte des questions liées à la mise en œuvre.

Mark Schacter, *The Worth of a Garden – Performance Measurement and Policy Advice in the Public Service – A discussion paper,* le 7 mars 2006.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT**

Protocole pour les évaluations horizontales – menées par d'autres ministères/organismes fédéraux

Approuvé par :
Le Comité d'évaluation ministériel

EN VIGUEUR LE 24 FÉVRIER 2010
SGDDI #: 556894

Canada

001434

Enjeux

- Besoin d'adopter un protocole concernant les évaluations horizontales menées par d'autres ministères ou organismes fédéraux.
- Besoin d'adopter une approche coordonnée tout au long des évaluations.
- Besoin de clarifier les rôles et les responsabilités.
- Besoin de pouvoir compter sur la participation de la haute gestion : essentielle pour faire en sorte que la participation de SP soit rapide et efficace.
- Besoin d'adopter un processus d'acceptation et d'approbation uniforme qui permettra au Ministère de se conformer aux exigences de la *Politique sur l'évaluation*.

Processus

- La Direction générale de l'évaluation (DGE) assigne un agent d'évaluation à chaque évaluation horizontale. Le rôle de l'agent est de :
  - représenter SP et assurer la liaison avec le groupe ou la fonction d'évaluation de l'organisation responsable de mener l'évaluation horizontale;
  - assurer l'engagement complet des secteurs de programmes de SP au cours de la phase de recherche ainsi que lors de l'élaboration de la réponse et du plan d'action de la gestion de SP;
  - coordonner l'examen ministériel des ébauches du rapport d'évaluation, et coordonner l'acceptation et l'approbation du rapport par le Ministère.

Acceptation et approbation

- Dans le cas des rapports comportant des recommandations adressées à SP :
  - La DGE travaille auprès du secteur concerné en vue d'obtenir l'acceptation du rapport par le sous-ministre adjoint responsable ainsi que la réponse et le plan d'action de la gestion.
  - Les constations et les recommandations contenues dans le rapport ainsi que la réponse et le plan d'action de la gestion de SP sont soumis au Comité d'évaluation ministériel afin que les membres puissent en recommander l'approbation au SM. La soumission se fait :
    - soit lors d'une réunion régulière, si les échéances fixées par l'organisation responsable le permettent;
    - soit par courriel aux membres du Comité d'évaluation ministériel sous réserve de l'approbation finale du sous-ministre.
  - La DGE prépare un document d'information pour le cabinet du ministre, conformément aux procédures normalisées.
- Le suivi de la mise en œuvre du plan d'action de la gestion se fera selon les processus courants.
- Si aucune recommandation ne s'adresse à SP, la DGE obtiendra l'acceptation des rapports d'évaluation de la part du SMA responsable et l'approbation du SM par le biais d'une note d'information. Les rapports d'évaluation seront alors présentées au Comité d'évaluation ministériel à des fins d'information seulement lors de la réunion subséquente.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT**

Protocol for Horizontal Evaluations - led by other government departments/agencies

Approved by:

Departmental Evaluation Committee

EFFECTIVE FEBRUARY 24, 2010
RDIMS#: 556891

Canada

001438

Issues

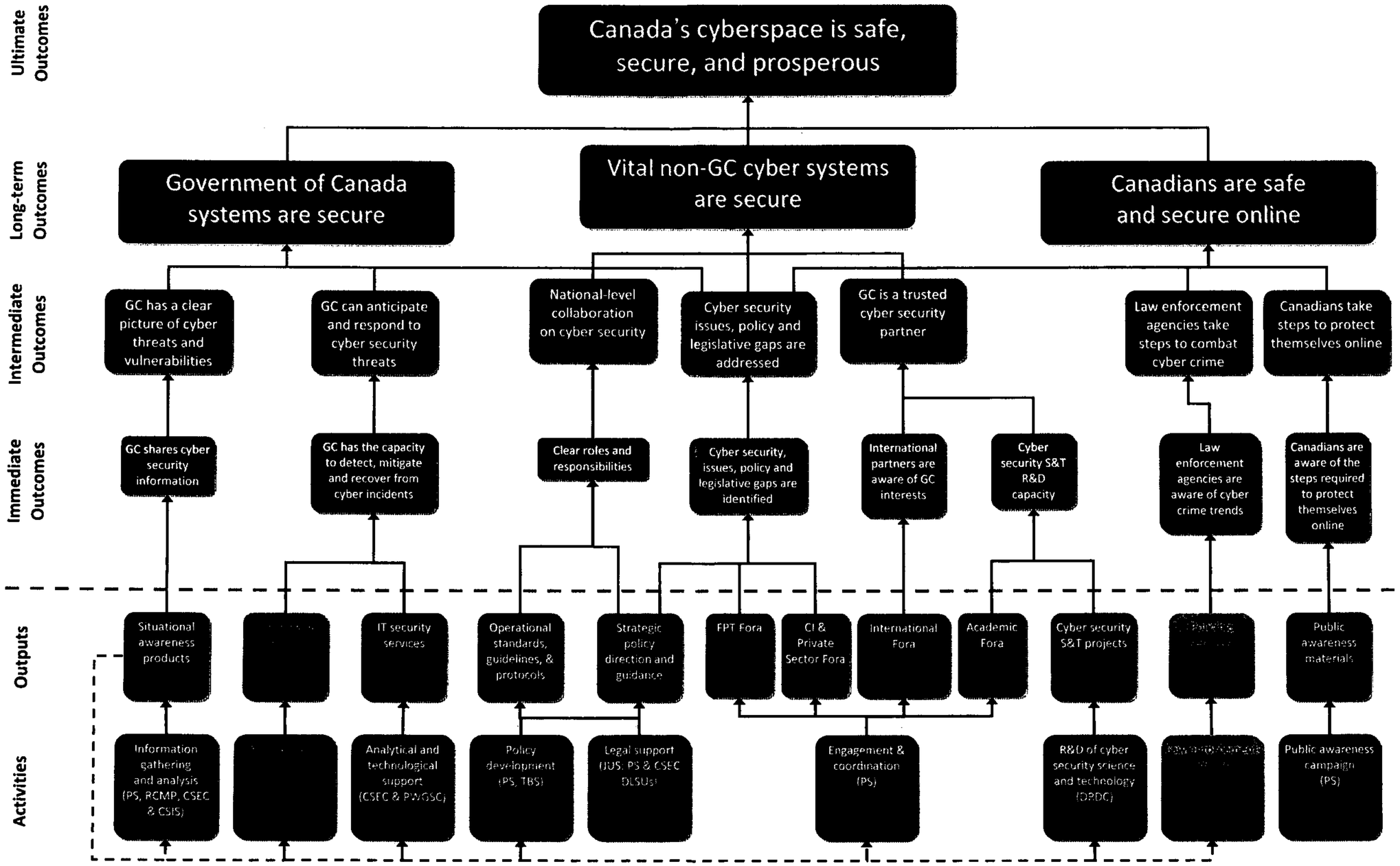
- Need for a formal protocol for horizontal evaluations led by other government departments/agencies.
- Need for a coordinated approach through all phases of the evaluation.
- Need for clarified roles and responsibilities.
- Need for senior management participation: critical to ensure PS' participation is relevant, effective and timely.
- Need for a uniformed acceptance and approvals process to ensure departmental compliance with the requirements of the *Policy on Evaluation*.

Process

- The Evaluation Directorate (ED) assigns an officer to each horizontal evaluation. ED officer's role is to:
  - Represent PS on horizontal evaluations and act as the departmental liaison with the lead organization's evaluation group/function.
  - Ensure the full collaboration of PS program areas in the research phase and in development of PS' management responses and action plans.
  - Coordinate PS' review of draft versions of evaluation reports and coordinate the Department's acceptance and approval.

Acceptance and Approval

- For reports with PS-specific recommendations:
  - ED works with Branch(es) and seeks acceptance from responsible ADMs as well as a management response and action plan.
  - Reports' findings, recommendations and the PS management response are presented to DEC for recommendation to the DM, either:
    - During a regular meeting, if the lead organization's timelines permit; or,
    - By e-mail to DEC members with final approval by the Deputy Minister.
  - ED would prepare the briefing package for the MO, as a standard procedure.
- Monitoring of MAP implementation conducted as a standard process.
- If there were no recommendations directed to PS, ED would seek acceptance of evaluation reports by responsible ADMs and seek DM approval through a briefing note. Reports would be provided to DEC as an information item at the next meeting.



Public Safety Canada | Sécurité publique Canada

Public Safety Canada's 2012-13 Performance Measurement Framework

1.1 National Security

Expected Result 1 - Canada is prepared to intervene and can respond to National Security threats
- Number of measures taken to address gaps in Canada's national security framework (Target: ≥ 15)

Expected Result 2 - Canada's critical infrastructure is resilient
- Critical Infrastructure Resilience Score (Target: TBD)

[illegible]

Expected Result 1 - Individuals and entities who pose National Security threats are prevented from operating in Canada
- Percentage of statutory obligations, including requests from PS Portfolio agencies, that are completed within given timelines (Target: 100%)

Expected Result 2 - National security policies and programs consider and/or are informed by input from Canadians
- Percentage of engagement sessions in which program/policy areas utilize gathered advice and perspectives to inform policies and programs (Target: ≥ 60%)

Output Indicator
- *Number of policies, initiatives and strategies developed or implemented as per workplan (Target: TBD)*

[illegible]

Expected Result 1 - Owners/operators of critical infrastructure and the Government of Canada take risk management action
- Percentage of sectors that have up-to-date sector overviews featuring modern risk management practices (Target: 100%)

Expected Result 2 - Partnerships are established with and among critical infrastructure sectors
- Percentage of sectors represented at the National Cross Sector Forum (Target: 100%)

Expected Result 3 - CI information is trusted and protected
- Number of inappropriate disclosures (Target: 0)

Output Indicator
- *Percentage of National Strategy and Action Plan deliverables completed on time (Target: 100%)*

[illegible]

Expected Result 1 - Canada is prepared for and can respond to cyber security threats
- Number of substantive engagements with Government of Canada departments responsible for cyber security to enhance the security of Government systems (Target: ≥ 4)
- Percentage of cyber incidents reviewed affecting stakeholders outside the Government of Canada that indicate a response was coordinated (Target: TBD)
- Percentage of Canadians that undertake cyber security measures (Target: TBD)

Output Indicators
- *Percentage of initiatives identified within Canada's Cyber Security Strategy that are underway or implemented (Target: ≥ 85%)*
- *Number of provincial, territorial and critical infrastructure entities engaged with the Canadian Cyber Incident Response Centre (Target: TBD)*
- *Number of substantive engagements with partners of importance, including international and domestic partners, to help promote awareness among the Canadian public (Target: TBD)*

Public Safety Canada's Strategic Outcome

"A safe and resilient Canada"

- Proportion of incidents where there was a timely response to events affecting the national interest (Target: 100%)
- Number of hours that any border service point is closed due to a security concern (Target: 0)
- Percent of the Canadian population satisfied with their personal safety from crime (Target: ≥ 93% by 2013)

1.2 Border Strategies

Expected Result 1 - Secure borders that facilitate legitimate trade and travel
- Percentage of border wait times standards that are achieved (Target: ≥ 95%)
- Percentage of people examined who are inadmissible and/or arrested (Benchmark: 0.5%)
- Percentage of goods examined that are seized (Benchmark: 0.5%)

Output Indicators
- *Percentage of key deliverables achieved as per annual workplan (Target: ≥80%)*
- *Number of Senior bilateral meetings / bilateral announcements (Target: 6)*

[illegible]

Expected Result 1 - The Minister is provided independent assurance as to whether CSIS operational activities are in compliance with legislation, ministerial direction and operational policy
- Percent of examinations requested by the Minister that were completed (Target: 100%)
- Percent of review work that is completed as per the annual plan (Target: 100%)

Expected Result 2 - CSIS takes action in accordance with the findings of the Inspector General of CSIS
- Extent to which CSIS takes action in accordance with the findings of IGCSIS (Target: ≥ 75%)

Output Indicator
- *Percent of core CSIS operational activities that are reviewed annually and completed (Target: 100%)*

1.3 Countering Crime

Expected Result 1 - Canadian communities are safe
- Percent of Canadians that think that crime in their neighborhood remained unchanged or decreased over the previous five years (Target: ≥ previous period (68%; 2009))

Expected Result 2 - Safe and effective reintegration of eligible offenders into Canadian communities
- Percentage of successfully completed day paroles (Target: ≥ 80%)
- Percentage of successfully completed full paroles (Target: ≥ 70%)

[illegible]

Expected Result 1 - Reduced offending among targeted populations (youth at-risk, Aboriginal communities, and high risk repeat offenders)
- Percentage of direct intervention projects with impact evaluations reporting a decrease in charges among targeted populations as a result of program participation (Target: ≥ 75%)

Expected Result 2 - Increase in the Canadian body of knowledge related to crime prevention
- Number of crime prevention knowledge-oriented resources (research reports, practice-oriented tools, communities of practice and learning events, presentations, etc.) that are produced by NCPC (Target: 10-20 per year)

Expected Result 3 - Reduced incidence of hate-motivated crime
- Percentage of projects that report a decrease in the number of hate-motivated crimes against buildings that received security infrastructure upgrades in communities that receive Security Infrastructure Program funding (Target: ≥30%)

Output Indicators
- *Percentage of projects funded through the NCPC that are evidence-based (Target: ≥ 80%)*
- *Number of Security Infrastructure Program project applications funded by type (Target: 15-20 projects in year one, and 30-40 projects ongoing)*

[illegible]

Expected Result 1 - Crime in Canada is attenuated
- Police-reported Crime Rate (Target: ≤ previous year (6145 incidents per 100,000 population; 2010))
- Police-reported Crime Severity Index (Target: ≤ previous year (82.7; 2010))

1.3.2.1 Serious and Organized Crime

Expected Result 1 - Law Enforcement is able to combat serious and organized crime
- Rate of firearms related serious crimes per 100,000 population (Target: ≤ previous year – TBC by StatCan)
- Police-reported drug offence rate (Target: ≤ previous year (318 drug offences per 100,000 population))

Expected Result 2 - Capital market fraud is detected and investigated
- Percentage of referrals by Integrated Market Enforcement Teams which were analyzed and actioned for investigation, or referred to other law enforcement or securities' authorities (Target 100%)

Output Indicator
- *Percentage of key deliverables achieved to combat serious and organized crime as per annual workplan (Target: ≥ 80%)*

1.3.2.2 RCMP and Policing

Expected Result 1 - Relations through the policing agreements between the Royal Canadian Mounted Police and provincial, territorial and municipal contracting jurisdictions are positive
- Level of satisfaction with the governance body and its objectives (Target: TBD when governance body is created in 2012-13)

Expected Result 2 - Canadians are confident with the national police service
- Percent of Canadians who have trust and confidence in the RCMP (Target: ≥ previous year (84%; 2010))

Output Indicators
- *Number of Policing Agreements renewed before expiration (Target: 100%)*
- *Percentage of key deliverables achieved to address trust and confidence in the RCMP as per annual workplan (Target: ≥ 80%)*

RDIMS: 440406

Public Safety Canada / Sécurité publique Canada

Public Safety Canada's 2012-13 Performance Measurement Framework

1.3 Countering Crime (Cont'd)

1.3.2.3 Aboriginal Policing

Expected Result 1 - First Nations and Inuit communities have access to dedicated and responsive police services
- Number of First Nations and Inuit communities that have access to the First Nations Policing Program (Target: ≥ 397)
- Population covered by police agreements (Target: ≥ 334,000)

Output Indicators
- *Number of agreements (Target: ≥ 168)*
- *Number of negotiated officers (Target: ≥ 1240)*

[redacted]

Expected Result 1 - Victims of crime are aware of the services available to them and are making use of those services, as needed
- Number of victims who register for information sharing with CSC and PBC (Target: ≥ 6105)

Expected Result 2 - Offenders successfully complete their period of conditional release
- Percentage of full paroles successfully completed (Target: ≥ 70%)

Expected Result 3 - First Nations, Métis, Inuit or urban Aboriginal communities have the knowledge and ability to improve community safety and to assume responsibility for corrections and healing
- Number of First Nations, Métis, Inuit or urban Aboriginal communities that have gained capacity and training to improve community safety and assume responsibility for corrections and healing (Target: ≥ 4)

Output Indicators
- *Number of phone calls at the National Office for Victims (Target: TBD)*
- *Number of Aboriginal communities which have implemented a community safety plan (Target: 3)*

1.4 Emergency Management

Expected Result 1 - Canadians are prepared and can respond to major disasters, accidents and intentional acts.
- Number of individuals impacted by major disasters, accidents and intentional acts
- Cost incurred by Canadians from major disasters, accidents and intentional acts

[redacted]

Expected Result 1 – Governments and key stakeholders have taken mitigative and preventative actions to address risks to Canadians
- Percentage of federal institutions that have assessed risks related to their area of responsibility in their strategic emergency management plan (Target: ≥ 20%)
- Percentage of federal institutions that have received a passing grade in the analysis and evaluation of their strategic emergency management plan (Target: ≥ 30%)
- Percentage of government and key stakeholders who participate in Canada's Platform for Disaster Risk Reduction (Target: ≥ 20%)

1.4.1.1 Joint Emergency Preparedness Program

Expected Result 1 – Provinces and territories are prepared to respond to all types of emergencies
- Percent of provincial demand for capital investment in relation to emergency preparedness that is committed by the JEPP program (Target: ≥ 75%)

Output Indicator
- *Percentage of projects approved (Target: ≥ 75%)*

1.4.1.2 Emergency Management Training and Exercises

Expected Result 1 - Government of Canada's all hazards emergency management plans, procedures and protocols are evaluated, validated and/or improved through exercises
- Percentage of recommendations that have been monitored for completeness following assignment to responsible departments (Target: 100%)

Expected Result 2 - Federal/provincial/territorial and municipal governments are provided cross disciplinary training in emergency management
- Percentage of course evaluations that demonstrate improved knowledge as a result of training and other learning events (Target: 20% increase)

Output Indicators
- *Number of government officials and emergency first responders trained at the Emergency Management College (Target: ≥ 1000)*
- *Percentage of national exercises delivered as outlined in the National Exercise Calendar (Target: ≥ 80%)*

1.4.1.3 Emergency Management Planning

Expected Result 1 - Critical services continue to be delivered to Canadians and operations of federal government institutions are recovered in the event of an emergency and/or interruption
- Percentage of Continuity of Constitutional Government (CCG) institutions that meet all objectives of CCG Emergency Response and Recovery Plan exercises (Target: ≥ 100%)
- Percentage of federal institutions that have identified critical services that have been reviewed based on the criteria set for the Federal Registry of Critical Services (Target: ≥ 80%)
- Percentage of federal institutions that have demonstrated readiness based on assessment criteria (Target: ≥ 20%)

Output Indicators
- *Number of federal institutions that attend emergency management planning workshops (Target: ≥ 50%)*
- *Number of visits to the business continuity planning SharePoint website (Target: ≥ 1000)*
- *Number of business continuity planning information sessions (Target: 2)*

[redacted]

Expected Result 1 - Canada can respond to and recover from events affecting the national interest
- Percentage of incidents for which a national coordination response was required and provided (Target: 100%)

1.4.2.1 Emergency Management Coordination

Expected Result 1 - Canada's response to incidents affecting the national interest is coordinated
- Percentage of incident reviews that indicate that the response was coordinated, as required (Target: 100%)

Expected Result 2 - Canada has a comprehensive approach to emergency management planning that supports coordinated response to emergencies
- Percentage of responses to incidents for which plans were in place and utilized (Target: 100%)

Output Indicators - Events coordinated
- *Number of incidents for which information products were distributed in a timely manner (Target: 100%)*
- *Quantity of numbered incidents* coordinated by the GOC*

** The Government Operations Centre assigns a number to an incident that affects the national interest and/or meets specific incident reporting criteria*

1.4.2.2 Disaster Financial Assistance Arrangements

Expected Result 1 - Provinces and territories receive funding to assist with response and recovery from major natural disasters
- Percentage of events meeting DFAA criteria that receive funding (Target: 100%)

Output Indicators - Payments made under the DFAA
- *Number of events for which the federal government has agreed to reimburse*
- *Number of payments made*
- *Dollar value of payments made*

1.4.2.3 Interoperability

Expected Result 1 - Operational information regarding public safety and security is shared in an effective and timely manner
- Percentage of provinces/territories/regions/municipalities within targeted deployment area, linked to the newly deployed national interoperable communications infrastructure using the 700 MHz spectrum (Target: ≥ 20% by end of 2012 and ≥ 50% by end of 2013 of the 4G LTE deployed network)
- Level of satisfaction from respondent Canadian Emergency Operation Centres regarding the accuracy and reliability of the information being displayed on the Multi-Agency Situational Awareness System (Target: ≥ 80% satisfied by end of 2013)
- Percentage of provincial and territorial participation in federally coordinated activities targeted toward objectives set out in the Canadian Communication Interoperability Continuum (Target: ≥ 76%)

Output Indicators
- *Percentage of action items in the Communications Interoperability Action Plan for Canada delivered within respective timelines (Target: ≥80% by 2012)*
- *Number of public safety secure applications deployed on 700 MHz broadband network (Target: 5 by end of 2012 and 8 by end of 2013)*

RDIMS: 440406

UPDATE ON CYBER SECURITY

ISSUE

Recent cyber security policy developments in the U.S. and an update on Canadian activities.

U.S. DEVELOPMENTS

In the past six months, there have been three noteworthy developments in the United States (U.S.) policy landscape.

First, the White House released an *International Strategy for Cyberspace*, highlighting the commitment of the U.S. Government to work with allies and other states to promote the development of international cyberspace policy respecting fundamental freedoms, privacy, and the free flow of information. This document aligns with and supports efforts being coordinated among Canada's close allies.

Second, the Department of Defense released its *Strategy for Operating in Cyberspace*, outlining how it will mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy, civil liberties, and free expression.

Third, a suite of legislative changes was proposed by the Obama Administration, in May 2011, aimed at expanding the powers and authorities of the Department of Homeland Security (DHS) to monitor and secure cyber systems domestically. In November 2011, the President's Cybersecurity Coordinator, Mr. Howard Schmidt, indicated that a meeting with Senate leadership showed a political commitment to moving these amendments through the legislative process.

UPDATE ON CANADIAN CYBER SECURITY ACTIVITIES

Progress is being made in implementing *Canada's Cyber Security Strategy* (the Strategy).

- **Information sharing.** Awareness sessions have been completed with most of Canada's ten critical infrastructure sectors, and leaders representing all sectors have been briefed twice on cyber security at the National Cross Sector Forum. A controlled access online portal for trusted critical infrastructure partners, with cyber security content, was launched on December 1, 2011. In addition, a portal is being developed for cyber security operators to allow specific cyber threat and vulnerability information to be shared in near real time. This will be administered by the Canadian Cyber Incident Response Centre (CCIRC), Canada's Computer Emergency Response Team (CERT) housed at Public Safety Canada (PS).

.../2

Non-disclosure agreements are being established with the private sector: the first are likely to be signed with key telecommunications companies and the Canadian Electricity Association.

Canada is prioritizing collaboration with those critical infrastructure sectors that underpin others: sub-national governments, the telecommunications, financial and energy transmission sectors. Classified threat briefings are being provided to the telecommunications and energy sectors. Actionable technical information has been shared and is yielding information for follow up investigation by the Canadian Security and Intelligence Service. This information sharing will enhance our understanding of threats faced by systems outside Government.

- **Operational collaboration.** PS is exploring opportunities with DHS to better align incident management and reporting protocols. Investments are planned for CCIRC's classified communications abilities to enable greater and faster information exchange with the U.S. CERT and the U.S. National Cybersecurity and Communications Integration Centre (NCCIC, pronounced N kick). NCCIC is a real time operations centre that integrates cyber and communications information and staff from federal, state, and local governments as well as the intelligence and law enforcement communities and private sector partners.

- **International collaboration**. Collaboration on cyber security policy advancement is extensive and facilitated through Canada's close allies. In the near term, Canada will continue to advance the international dialogue on norms and standards for behaviour in cyberspace, as discussed at the London International Cyber Conference. This will ensure that Canada's values are reflected in international policy discourses on cyber security and reinforce that existing international laws apply in cyberspace as they would in the real world.

s.15(1) - Int'l

[redacted]

Bilateral collaboration is also regularly occurring between PS, DHS, and the White House on policy, operations and communications. [redacted]

[redacted]The Emergency Management Consultative Group and Permanent Joint Board on Defence are also driving progress on cyber.

Two cyber security initiatives are included in the Action Plan for the Shared Vision for Perimeter Security and Economic Competitiveness. The first focuses on enhanced Canada-U.S. cooperation internationally and the second on bilateral measures to share information and better coordinate operations.

RDIMS 528374

1) The first focuses on international cooperation: the U.S. was looking for increased Canadian diplomatic efforts and for Canada to ratify its 2001 signature to the Council of Europe Convention on Cybercrime.

2) The second initiative focuses on bilateral measures to share information and better coordinate operations during cross border cyber events. In support of this initiative, PS is seeking resources to extend CCIRC's operations to 15 hours per day, 7 days per week to enable national coverage during business hours. At the time of writing, the announcement of the Joint Action Plan for the Shared Vision for Perimeter Security and Economic Competitiveness was scheduled for early December 2011.

s.15(1) - Int'l

KEY MESSAGES

s.21(1)(a)

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

BRIEFING NOTE FOR THE DEPUTY MINISTER

CYBER SECURITY

Canada's Cyber Security Efforts

The Government of Canada has taken action to address threats emanating from cyberspace, announcing *Canada's Cyber Security Strategy* (the Strategy) on October 3, 2010. The Strategy assigns the primary coordinating lead for cyber security to Public Safety Canada and encompasses a whole-of-government effort with specific roles and responsibilities assigned among 11 involved departments and agencies.

The Strategy is built on three pillars:

1. **security government systems** to protect the information entrusted to it by Canadians, and to secure national security activities;
2. **partnering to secure vital cyber systems outside the federal government**, including the systems that control critical infrastructure and those that contain the personal information of Canadians and the intellectual property of Canadian businesses; and
3. **helping Canadians to be secure online** through improved awareness, education, and access to the information they need to protect themselves online.

Canada has been active in ensuring its laws keep pace with technology. The Government of Canada signed the Budapest Convention in 2001, but has not yet ratified it, as changes to Canada's own legislation are required to fully meet the Convention's obligations. However, Bill C-51 "*Investigative Powers for the 21st Century Act*" was not part of the recent omnibus crime and justice bill introduced in Parliament (Fall 2011), and no timing has been determined for its introduction. Ratifying the Convention would contribute to Canada's credibility in the ongoing efforts to prevent, deter and punish cyber facilitated criminal actions.

Associated with *Canada's Cyber Security Strategy*, Canada recently passed several important pieces of cyber related legislation, including bills to combat child pornography and fight the most damaging forms of spam. Furthermore, the RCMP is establishing the integrated Cyber Crime Fusion Centre which will provide a more comprehensive understanding of the national threat and risk environment.

Current Status

Efforts to strengthen the electronic security of federal cyber systems are ongoing, including the consolidation of Internet access points on Government of Canada networks, and the addition of analytical systems to increase awareness of what is occurring on the Government's networks.

Work towards engaging the private sector and other levels of government in Canada is underway with initial efforts focused on the energy, financial, and telecommunications sectors and provincial and territorial governments.

PS is also engaging internationally with traditional allies like the UK and the U.S., as well as nations that have been identified as foreign policy priorities (such as those in the Americas).

PS is currently reviewing existing legal and policy regimes; building trusted relationships with the private sector to overcome industry reluctance to discuss cyber vulnerabilities with the Government; and developing a joint action plan with Canada's provinces and territories.

London International Cyber Conference

To launch an international discussion on the value of norms for cyberspace, the UK is hosting the London International Cyber Conference on November 1-2, 2011. Canada has been invited along with approximately 65 other states including, Australia, Brazil, Chile, China, India, Japan, Mexico, the Republic of Korea, the Russian Federation, Singapore, South Africa, Turkey, and most states of the European Union. International organisations, such as the United Nations, regional organisations, such as the Association of South Eastern Nations, prominent technology companies, and civil society organisations are also expected to attend. UK officials have indicated that while Conference attendees are expected to discuss the value of norms for cyberspace in thematic areas (safe and reliable access, international security, social benefits, economic growth and development and cybercrime), they are not expected to establish a specific set of cyber norms by the end of the Conference.

International Norms and Principles

UK's Perspective

The UK has recently begun promoting the establishment of international norms and principles for behaviour in cyberspace. This push is largely in response to increasing international momentum for a globally binding treaty which would set out precise roles and responsibilities for state activities in cyberspace. The UK, along with a number of other countries, believes that existing international agreements already apply to cyberspace and that additional legal instruments in this area are currently unnecessary. Furthermore, an international treaty specifically tailored to cyberspace would only bind states, and not the myriad of businesses, civil society groups and individuals that are active in cyberspace, making it of limited value. In light of these difficulties, the UK believes it best to pursue a norms-based approach to cyber security, where states, businesses and civil society would agree to and comply with mutually agreed-upon norms. These norms would create societal pressures for compliance without the need for long and arduous treaty negotiations.

s.15(1) - Int'l

Canada's Perspective

Canada, through Public Safety Canada, has actively supported the UK in its efforts to promote cyber norms. [redacted]

Council of Europe Convention on Cybercrime

In late 2010, the EU unveiled two proposals to enhance the security of networks and information within the EU. The first was a renewal of the mandate of the European Network and Information Security Agency (ENISA), which is mandated to enhance network security within the EU for all member states. The second was a Directive to deal with cybercrime. The proposed Directive is in the European Parliamentary process and would introduce higher criminal sanctions for criminals, enhance cooperation between the judiciary and police of member states, and provide for the establishment of a system to record and trace cyber attacks.

CANADA-COLOMBIA SECURITY CONSULTATIONS
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

COLOMBIAN POSITION

- Colombia has recently announced a cyber security strategy and welcomes the opportunity to share it with the Canadian delegation at the security consultations.

BACKGROUND

Cyber systems – computers and the Internet – are fundamental for the effective operations of Government, the private sector, 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, through 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 in the Americas

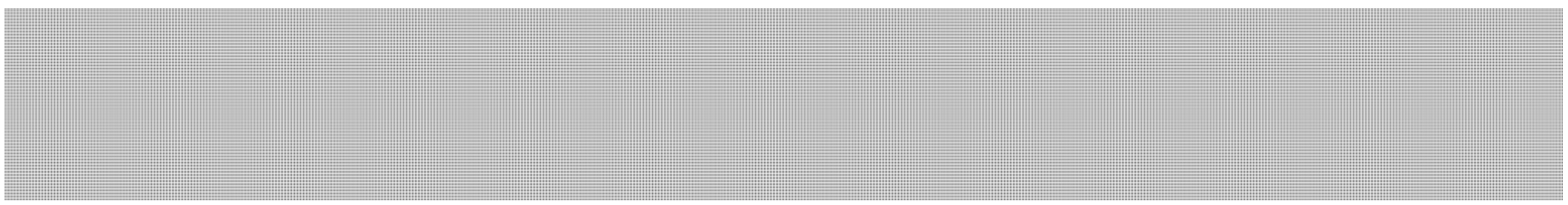
Outside of bilateral work with the United States, Canada has had little engagement on cyber security issues within the hemisphere. Regionally, only the United States and Canada have released formal cyber security strategies, although the issue is gaining in visibility following high profile cyber incidents in Brazil, Mexico, Venezuela and Chile over the last year.

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 within 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.

s.15(1) - Int'l



CICTE will be meeting in Washington, DC on March 7, 2012. Its focus will be on finalizing a draft declaration on "Strengthening Cyber Security in the Americas." It is possible that an official from Public Safety will be on the delegation.

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.

RESPONSIVE ONLY **– If Asked for Resources**

- Canada has not made capacity building and development assistance a formal part of our Cyber Security Strategy.

- We may be able to share our experiences and expertise during expert visits or regional meetings.

Author's name/division or mission/tel.: PS/Cory Dvorkin/613-990-9608
Approval bureau/mission: PS/BPIAD/Linder
Consulted divisions/missions/departments: DFAIT/ICT/Dempsey; PS/IAD/Thorpe
Attachments: N/A

Public Safety Canada | Sécurité publique Canada

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

Canada's Cyber Security Strategy

For a stronger and more prosperous Canada

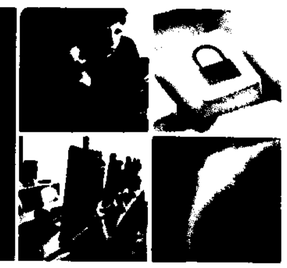
Canada-Colombia Security Consultations

February 22, 2012

Lara Thorpe, Policy Analyst, International Affairs, Public Safety Canada

Canada

Outline



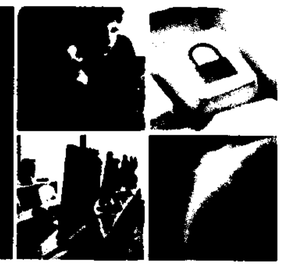
1. Why is it important to secure our digital infrastructure?

2. Government of Canada Initiatives.
   - *National Strategy and Action Plan for Critical Infrastructure*
   - *Canada's Cyber Security Strategy*

3. Roles and responsibilities within the Government.

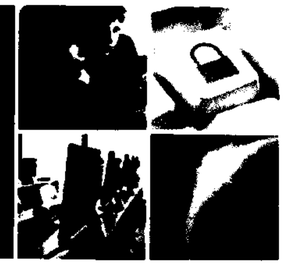
4. Progress on Implementation and Upcoming Initiatives.

Why is it important to secure our digital infrastructure?



- Sensitive and valuable information is increasingly stored online:
  - Governments
  - Industry
  - Citizens
- Makes us an attractive target:
  - Hackers
  - Criminals
  - Terrorists
  - Foreign governments
- The threat is real and evolving.

Government of Canada Initiatives

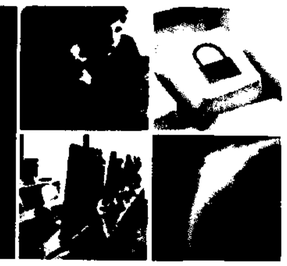


- *National Strategy and Action Plan for Critical Infrastructure* (May 2010).

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

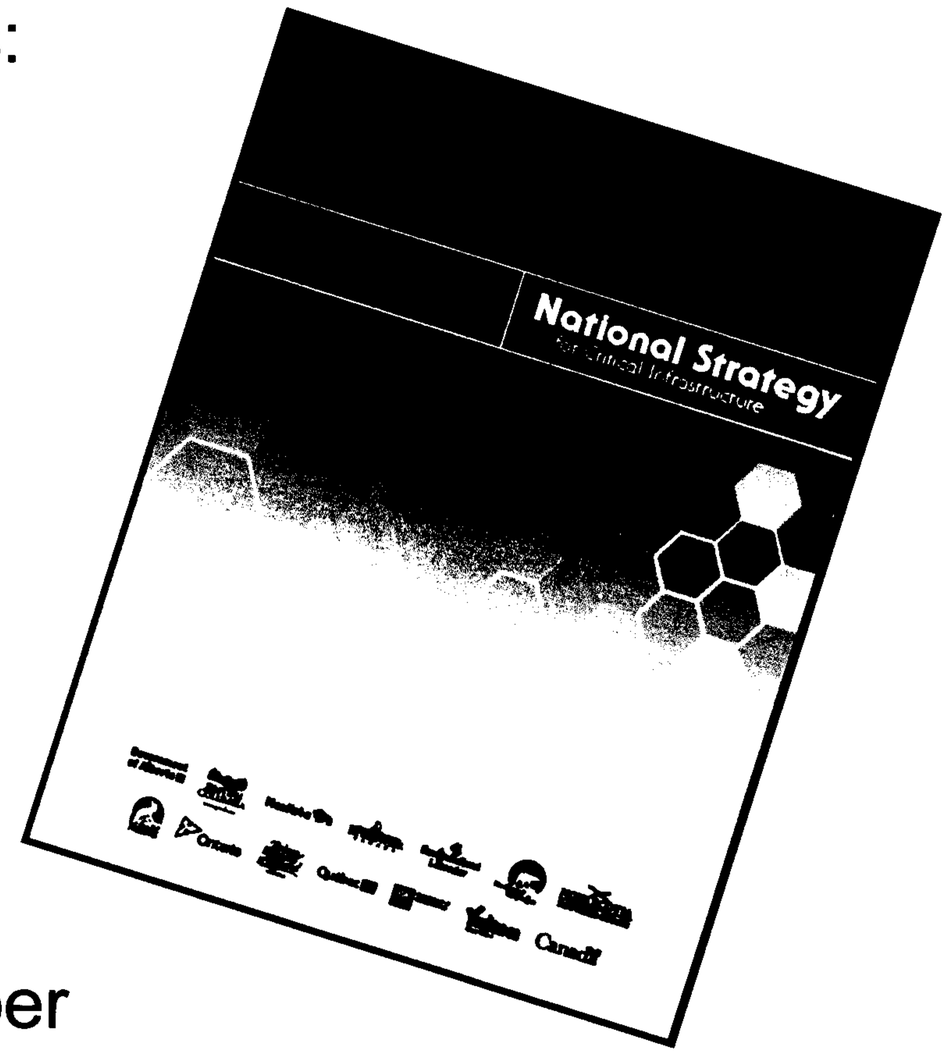
- *Canada's Cyber Security Strategy* (October 2010).

The *National Strategy and Action Plan for Critical Infrastructure*



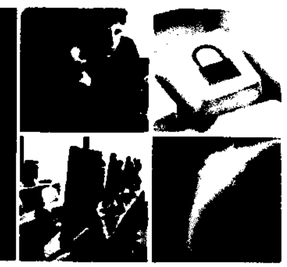
BUILDING A **SAFE** AND **RESILIENT CANADA**

- Based on three strategic objectives:
  - Build trusted and sustainable partnerships
  - Advance timely and protected information sharing
  - Implement an all-hazards risk management approach



- Strengthens resiliency of critical infrastructure sectors, including cyber infrastructure.

Canada's Cyber Security Strategy

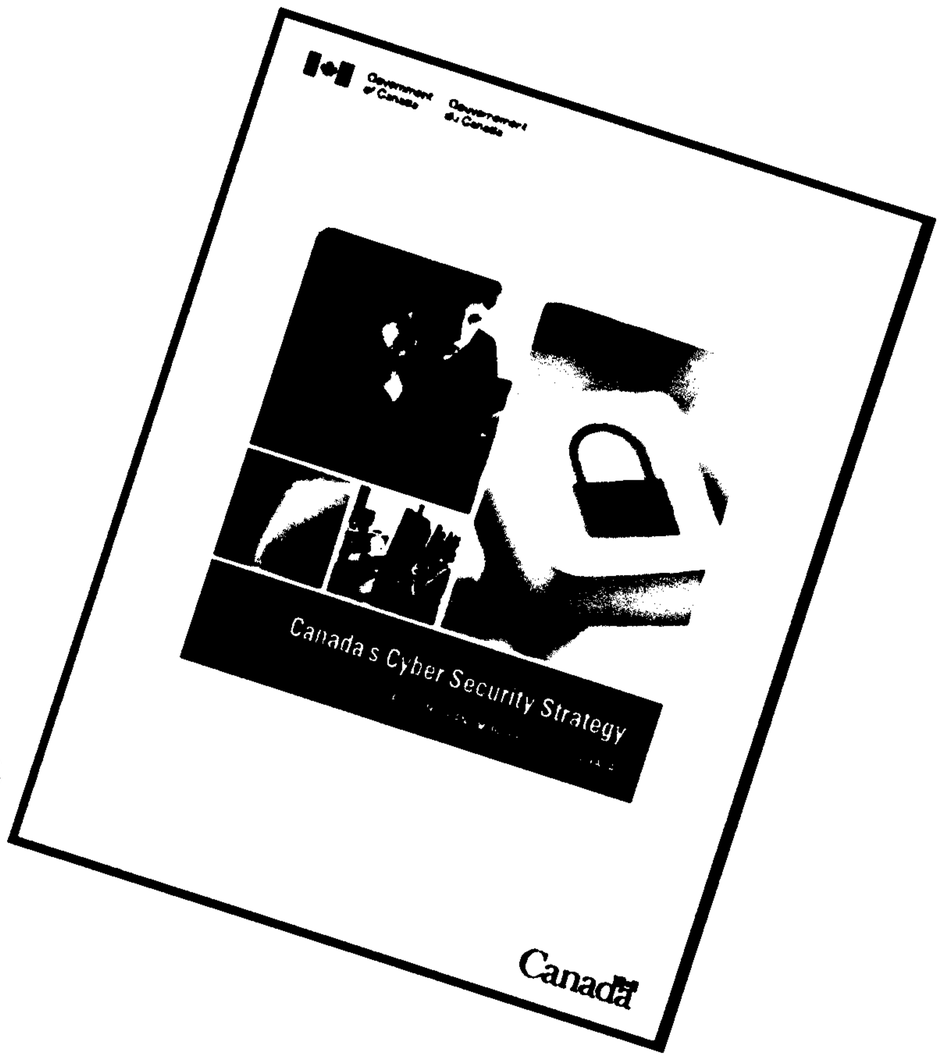


BUILDING A **SAFE** AND **RESILIENT CANADA**

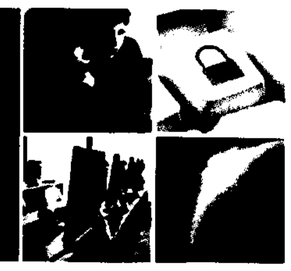
- Signals cyber security as a priority for the Government of Canada.

- Commits investment by the Government in resources.

- Coordinates and unifies domestic and international action.



Canada's Cyber Security Strategy

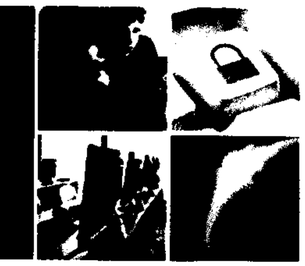


BUILDING A **SAFE** AND **RESILIENT CANADA**

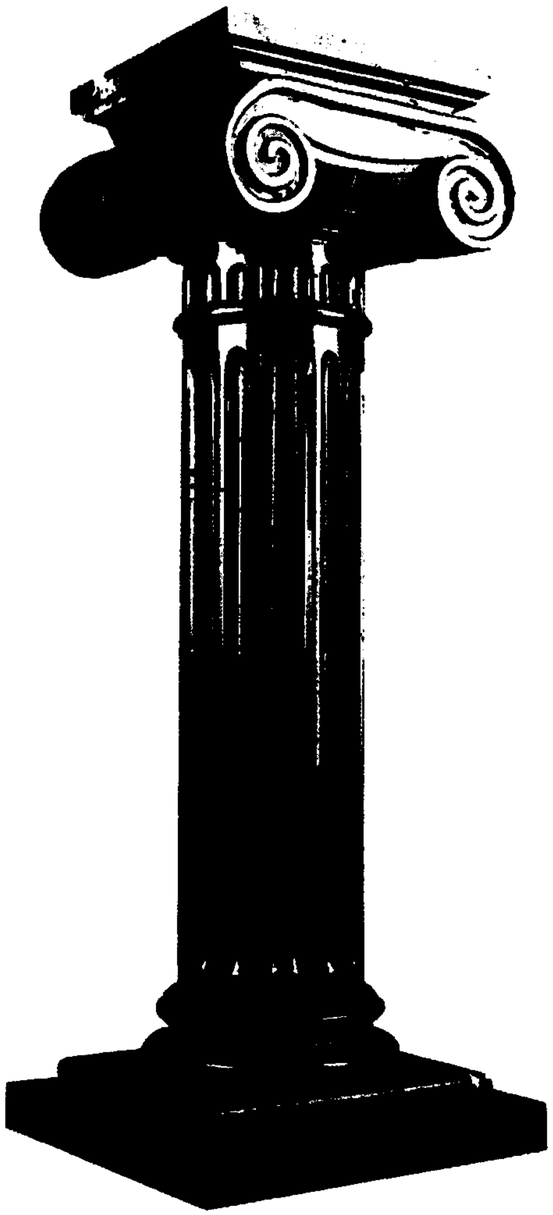
- Built on three pillars:

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

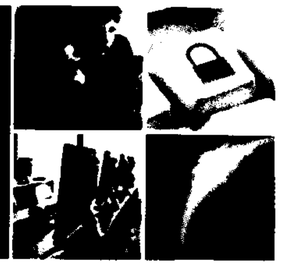


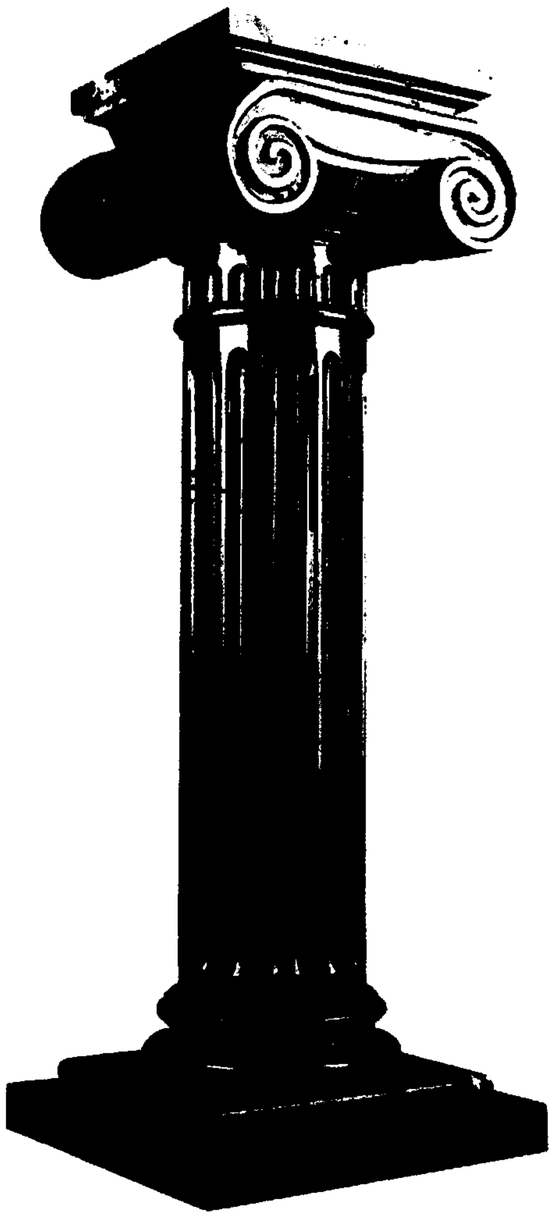
BUILDING A **SAFE** AND **RESILIENT CANADA**



- 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



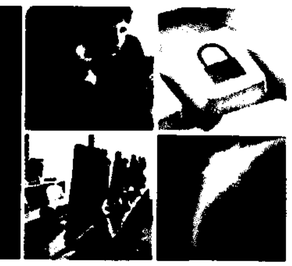


- Partner with the provinces and territories, the private and academic sectors, and international partners.

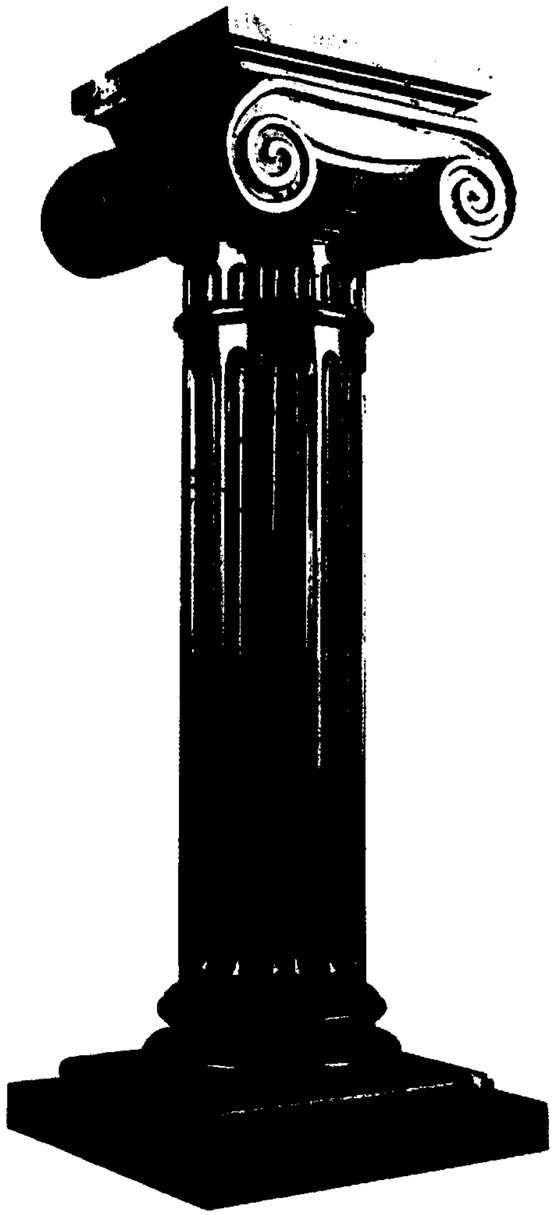
- Develop leading-edge cyber security science and technology, and innovative research and development.

- Leverage and build upon public-private partnerships to secure critical infrastructure and promote awareness.

Pillar 3: Help Canadians to be secure online

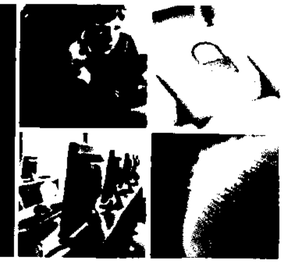


BUILDING A **SAFE** AND **RESILIENT CANADA**



- 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

Canada's Cyber Security Strategy (cont'd)



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

Support national priorities.

- **Economic prosperity.**
- **National security.**
- **Safety of Canadians.**

Leverage existing activities and investments.

- **Consultative processes.**
- **Key legislation and policies.**
- **Structural changes.**
- **Cyber Security Awareness Month.**

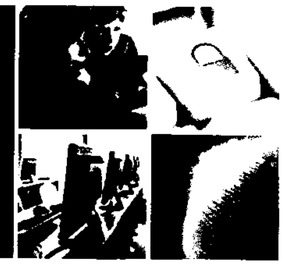
Meet our goals.

- **Strengthen capability.**
- **Build credibility.**
- **Promote awareness.**

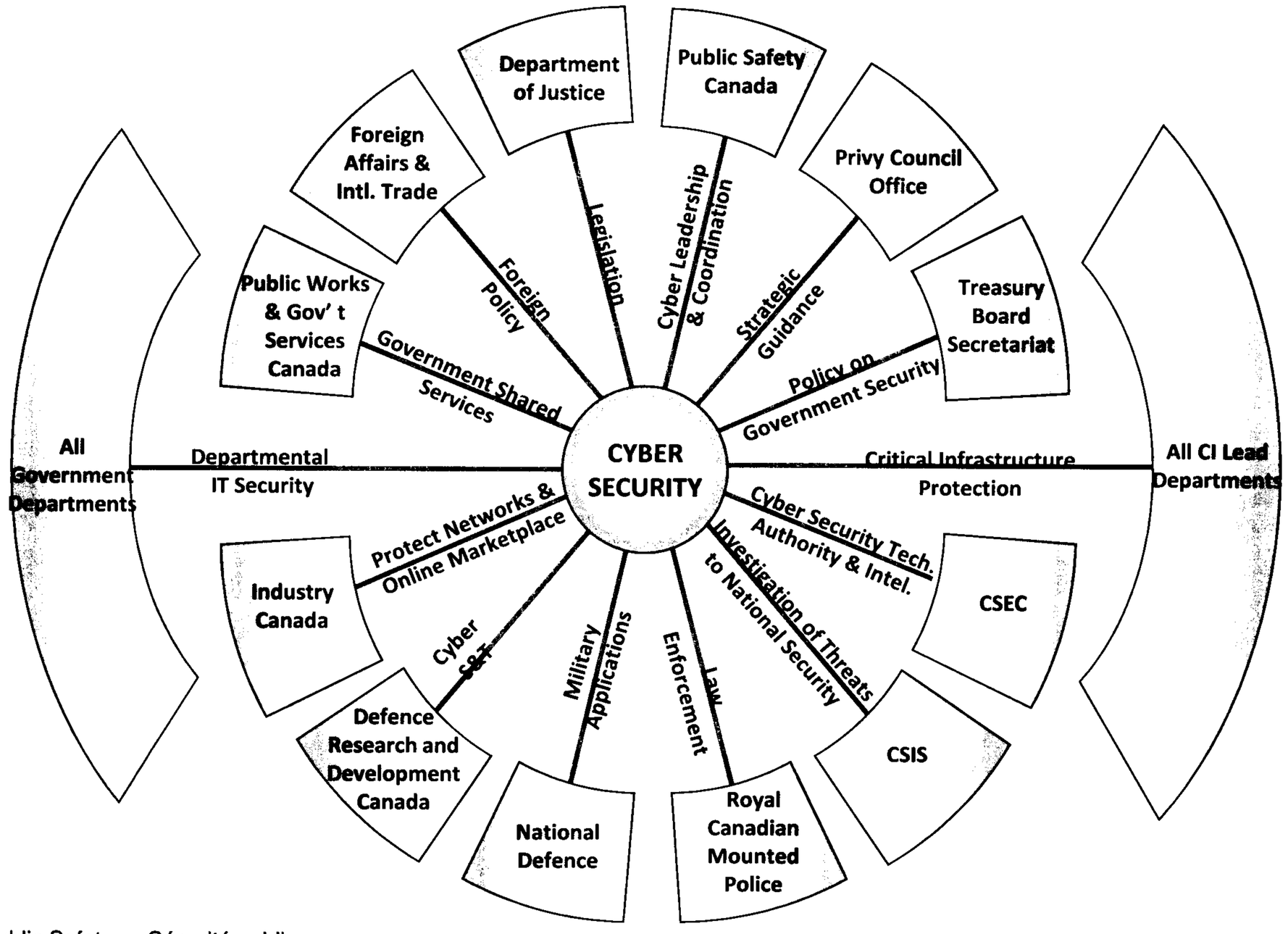
Canada's Cyber Security Strategy.

- **Secure Government systems.**
- **Secure systems outside the Government of Canada.**
- **Helping Canadians to be secure online.**

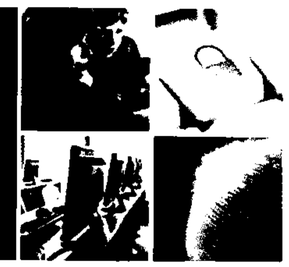
Roles and responsibilities within the Government of Canada



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



Progress on Implementation and Upcoming Initiatives



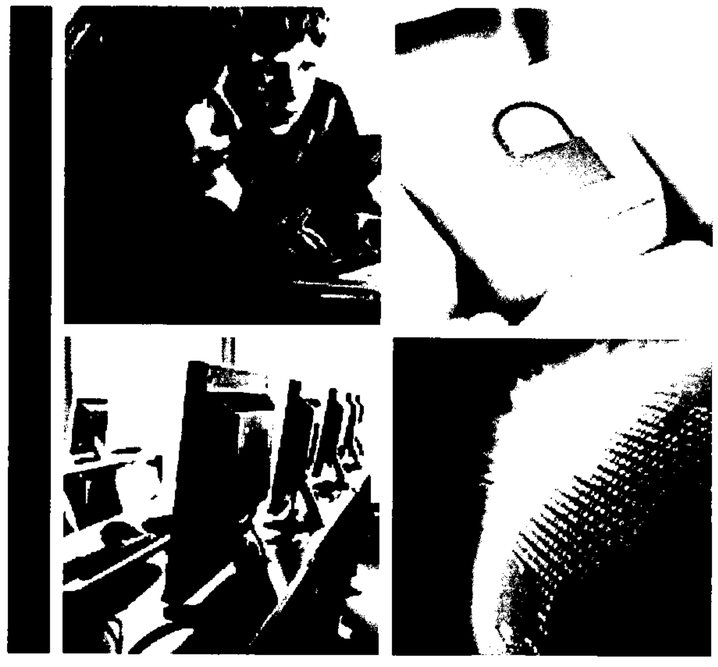
- Created a national cross-sector forum to build partnerships, improve information sharing, and address the physical and cyber vulnerabilities that span all of the sectors.
  - Established the Canadian Security Telecommunications Advisory Council.

- Met with provincial and territorial governments to shape a joint action plan to guide collaboration on cyber security matters.

- Cyber Security Awareness Month held each October.

Public Safety Canada | Sécurité publique Canada

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



www.publicsafety.gc.ca/cyber

Canada

Briefing Note for Canadian Delegation to ASEAN Regional Forum Meeting on Counter Terrorism and Transnational Crime (ARF CTTC), March 16-17, 2012

s.15(1) - Int'l

s.15(1) - Subv

CYBER ISSUES

ISSUE

The following provides a brief on key current cyber issues.

CANADIAN POSITIONS

Cyber norms:

Cyber security: Canada is concerned about the rising threats emanating from cyberspace

Cybercrime: Canada fully supports the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*)

Cyber terrorism: Canada does not generally use this term as it is ill-defined, understood to be a catch-all term to refer to any activity that terrorists conduct on the Internet.

Canada addresses terrorist activity online through its counter terrorism efforts, and not through a separate cyber-specific approach.

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."

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]

The U.K., with the support of [redacted] Canada, 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 multi-stakeholder 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;
- 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. [redacted]

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.

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.

TALKING POINTS

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 multi-stakeholder 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) - Subv
s.21(1)(a)

[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.

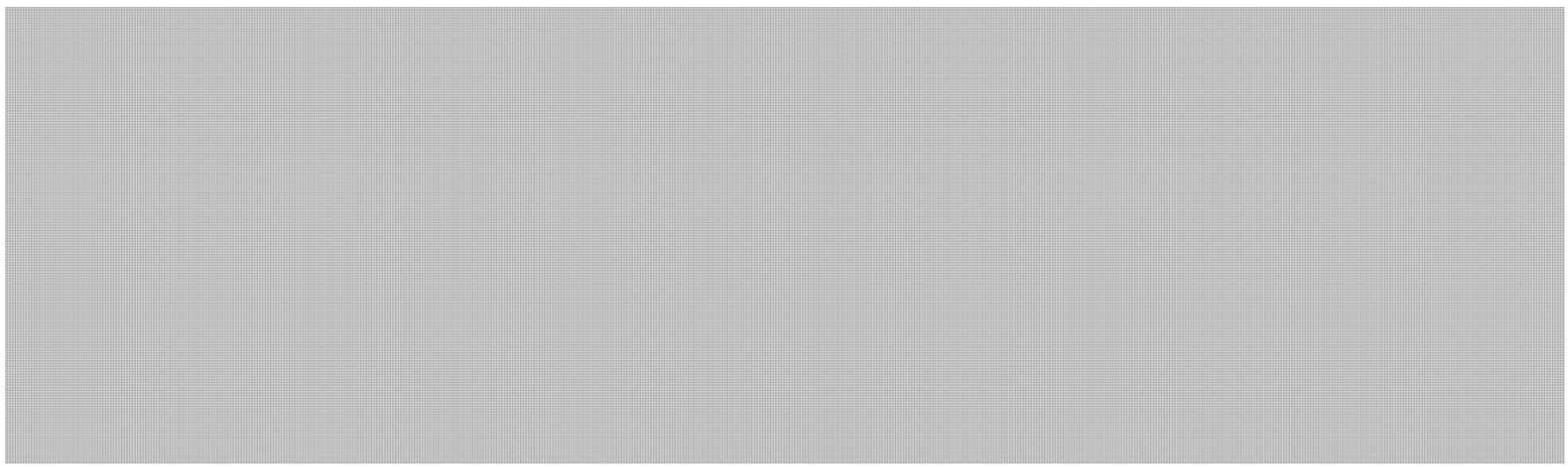
Cybercrime

- 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.21(1)(a)

- 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*.



Pages 1473 to / à 1521

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