QUESTION PERIOD NOTE

Date: March 26, 2012
Classification: UNCLASSIFIED
Branch / Agency: NS

Question Period Note

STATUS OF CANADA'S CYBER SECURITY STRATEGY

ISSUE:

Cyber security is a critical national security and economic security issue. Recent months have seen increased media interest in the topic, and the United States is putting heavy emphasis on cyber security as part of their national security efforts.

BACKGROUND:

Information is a strategic asset. In Canada, all levels of government, the economy and society in general are critically dependent on electronic and physical infrastructure which are vulnerable to exploitation by malicious actors.

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.

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. The Government of Canada has been actively working to implement *Canada's Cyber Security Strategy*.

With respect to Pillar 1 of the Strategy, "secure Government systems," the Government has:

- created a policy centre within Public Safety Canada to lead national cyber security efforts;
- strengthened network and security measures, in particular through further investments and a revision of the Government of Canada's *Information Technology Incident Management Plan*;
- transferred incident response coordination for Government of Canada systems to the Communications Security Establishment Canada, further leveraging federal capabilities to secure systems and clarifying roles and mandates; and
- created Shared Services Canada, which will consolidate and streamline the delivery of Government IT services and facilitate improved security.

Under Pillar 2 of the Strategy, "partner to secure systems outside the Government of Canada," the Government has:

- initiated dialogue on cyber security with provincial and territorial interlocutors;
- expanded engagement activities with Canada's critical infrastructure sectors, in particular through the mechanisms created by the *National Strategy and Action Plan for Critical Infrastructure*;
- included two cyber security related items as part of the Shared Vision for Perimeter Security and Economic Competitiveness;
- sought to develop meaningful partnerships with Canada's critical infrastructure sectors, including the creation of information sharing mechanisms, arrangements, and joint action plans; and
- streamlined the mandate of Public Safety Canada's Canadian Cyber Incident Response Centre to focus on national issues and provide support for provinces, territories, critical infrastructure and industry.

Pillar 3 of the Strategy, "help Canadians to be secure online," has seen:

- the launch of a national public awareness campaign "Get Cyber Safe" to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online;
- the pending, 2012, launch of Canada's anti-spam reporting centre to enforce violations of Canada's anti-spam legislation;
- the introduction of legislation which will enable the Government of Canada to ratify its commitment to the Council of Europe *Convention on Cybercrime* and provide law enforcement officers with the tools and authorities needed to undertake investigations in this digital era; and the Royal Canadian Mounted Police (RCMP) establish the Cyber Crime Fusion Centre to provide a national focal point for reporting and understanding cybercrime.

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.

STATUS OF CANADA'S CYBER SECURITY STRATEGY

PROPOSED RESPONSE:

- **The Government released *Canada's Cyber Security Strategy* in 2010 as a clear statement of the priority we place on protecting our citizens, our businesses, and our essential infrastructure from online threats. The Government continues to deliver on its commitments as laid out in the Strategy.**

- **Federal departments and agencies are working to implement their respective elements of the Strategy. We continue to strengthen the security of federal systems and deliver programs and benefits to Canadians. This means ensuring that police have the tools and authorities they need to keep pace with changes in technology, as we have proposed in Bill C-30.**

- **Among the concrete benefits the Strategy is providing is the Canadian Cyber Incident Response Centre (CCIRC), which is on the frontline in protecting our critical infrastructure. CCIRC monitors and analyzes emerging cyber risks and provides advice to the private sector on how to deal with specific cyber threats.**

- **The Government is also working with other levels of government and critical infrastructure sectors to help secure vital cyber systems outside of federal jurisdiction, including establishing joint action plans and information sharing mechanisms.**

- **The Government is raising awareness directly with citizens through our *Get Cyber Safe* campaign, which provides a trusted source of information about online risks and provides concrete advice on how Canadians can better protect themselves online.**

CONTACTS:			
Prepared by	Tel. no: (613) 990-9608	Approved by (ADM level only)	Tel. no.: (613) 990-2661
Corey Dvorkin/NS/Cyber Policy	Cell: [redacted]	Robert Dick DG National Cyber Security	Cell: [redacted]

s.19(1)

Pages 51 to / à 60

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

TAB 6

Pages 62 to / à 67

are withheld pursuant to section

sont retenues en vertu de l'article

14(a)

of the Access to Information

de la Loi sur l'accès à l'information

TAB 7

7. ROUNDTABLE

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

Future [redacted]

- situational awareness products

- SSC [redacted]

- IC - agenda on cyber

s.15(1) - Defence
s.15(1) - International

RDIMS# 432543

Last updated: October 25, 2012

UPDATE ON CANADA'S CYBER SECURITY ACTIVITIES

ISSUE

Cyber security is a high priority issue for the United States (U.S.) government and is likely to be raised in discussions during your visit to Washington, D.C.

BACKGROUND

Canada is actively pursuing cyber security activities on the domestic, and international fronts, as well as in the context of the bilateral Canada-U.S. relationship. Although we are engaged on this issue across a broad range of activities, Canada's recent investment in cyber security has been modest when compared with that of our closest allies.

The U.S. sees cyber security as a key policy priority and is very active on this issue both domestically and internationally. Notably, the U.S. government has recently unveiled a cyber security legislative reforms package as well as an *International Strategy for Cyberspace*.

CURRENT STATUS

Public Safety Canada is the lead department for implementing *Canada's Cyber Security Startegy*:

- It operates the Canadian Cyber Incident Response Centre, which will soon assume the role of a national incident response centre.
- The Government of Canada (GC) is working to update its IT Incident Management Plan and is strengthening the security of federal cyber systems by consolidating the number of Internet access points to reduce exposure.
- Communciations Security Establishment Canada is adding analytical capability to federal networks to enhance its situational awareness capacity.
- Partnerships are being created to share information with provinces and territories as well as the private sector, with a focus on high value critical infrastructure sectors, including electrical grids, telecommunications and financial networks.
- Finally, Public Safety Canada is ready to move ahead with a national awareness strategy.

Canadian and U.S. officials have been highly effective in collaborating on cyber security issues, including operations, policy development, and international engagement.

- [redacted]

- **Beyond the Border Initiative**: Two separate cyber security initiatives are currently in development. The first would harmonize our international cooperation to build support for shared objectives in cyber policy. The second initiative would establish a mechanism for increased cyber information sharing and operational coordination in case of an incident.

Engaging internationally is an important part of *Canada's Cyber Security Strategy*, and Canada is actively cooperating with the United States on cyber security both bilaterally [redacted]

Of note is the fact that the U.S. *International Strategy for Cyberspace* promotes the use of development and capacity building programs, [redacted] Although currently unfunded, opportunities for engagement, particularly with the Organization of American States, are being explored.

DESIRED CANADIAN OUTCOME

To clearly communicate to the United States officials that Canada is committed to doing its part to secure our shared critical digital infrastructure, and to further our joint interests in the international arena.

s.13(1)(a)
s.15(1) - International

TALKING POINTS

- I am pleased that Canadian and U.S. officials have been highly effective in collaborating on cyber security across a broad range of issues, both bilaterally and on the international arena.

- Canada-U.S. cooperation on securing critical cross border networks is a clear need. Progress on this is expected under the Beyond the Border initiative.

- [redacted]

- We look forward to broadening and deepening collaboration on cyber security activities between our two countries, including in areas of public awareness, information sharing, and joint incident management.

s.13(1)(a)
s.15(1) -
International

6 June 2011

UPDATE ON CANADA'S CYBER SECURITY ACTIVITIES

ISSUE

Cyber security is a high priority for the United States (U.S.) government and is likely to be raised in discussions during your visit to Washington, D.C.

BACKGROUND

Canada is actively pursuing cyber security activities on the domestic, and increasingly on the international fronts. As compared to some allies, *Canada's Cyber Security Strategy* is far more focused in its scope, and modest in allocated resources. By way of example, the U.S. spends over $3.5 billion annually on cyber security programs, whereas Canada's Strategy received an initial $90 million over five years.

The U.S. sees cyber security as a fundamental national security interest. In the American view, cyber threats are a real and current challenge to its economic prosperity and to America's role in the international order. Addressing that challenge has been the driving force guiding recent revisions to American, foreign and defence policy. In addition, the White House has issued a new *International Strategy for Cyberspace*, setting forward some clear objectives for its foreign policy machinery. Finally, a series of legislative changes proposed by the Obama Administration in May are aimed at greatly expanding the powers and authorities of the Department of Homeland Security (DHS) to monitor and secure cyber systems domestically.

CURRENT STATUS

Public Safety Canada is the lead department for implementing Canada's 2010 Startegy. It operates operates the Canadian Cyber Incident Response Centre, which will soon assume the role of a national incident response centre. The Government of Canada is working to update its IT Incident Management Plan and is strengthening the security of federal cyber systems by consolidating the number of Internet access points to reduce the exposure of Government of Canada networks. Canada's signals intelligence agency, Communciations Security Establishment Canada, is adding analytical capability to increase its awareness of what is occurring on Government networks. Partnerships are being created to share information with the private sector, with a focus on high value critical infrastructure sectors such as telecommunications and electrical sectors. Finally, Public Safety Canada is ready to move ahead with a national awareness strategy.

Aside from ongoing work in the [redacted] which are primarily focused on the international aspects of cyber security, Canada-U.S. efforts on cyber security are focused on three main areas:

- **bilateral cooperation with the U.S.** between DHS and Public Safety Canada, which is focusing on operational coordination for incident response and sharing threat information to protect cross border infrastructure.
- [redacted]

- **Beyond the Borders Vision process** Staff are working on two separate cyber security initiatives. The first would harmonize our international cooperation to build support for shared objectives in cyber policy. The second initiative would establish a mechanism for increased cyber information sharing and operational coordination in case of an incident.

While there are many similarities to the respective international agendas for cyber security, there are also notable differences. The U.S. *International Strategy for Cyberspace* promotes the strong use of development and capacity building programs to help underwrite cyber security programs abroad. Such work was not funded under Canada's Strategy, but opportunities for engagement, particularly with the Organization of American States, are being explored, although these may not be sustainable in the longer term absent additional resources. In the near term, Canada's efforts abroad will focus on the upcoming 60 nation International Cyber Conference (to be held in London in November 2011) and the International Telecommunications Union Plienpotentiary (January 2012).

Concerning Richard Clarke

Having a 30 year career in the U.S. government, Richard A. Clarke capped his service as a senior White House advisor to U.S. Presidents Bill Clinton and George H. W. Bush, focussing on counter-terrorism, cyber security, and cyberterrorism. He is best known for authoring a memo to National Security Advisor, Condoleeza Rice, the month before 9-11, which is alleged by many to warn of the pending al-Queda attacks. Having retired in 2003, Clarke spent his last years in the U.S. public service as the first White House official focused solely on cyber security. He has written two books concerning his experiences around 9-11 and terrorism, and two novels dealing with the U.S. response to fictional terrorist incidents. His newest book, which received significant notice, albeit mixed reviews, was *Cyber War: The Next Threat to National Security and What to Do About It* (2010).

Mr. Clarke's views concerning the magnitude of the cyber threat are not universally shared among experts in this field. Clarke maintains that America's strength in offensive cyber operations is potentially an asset abroad, but that America's widespread reliance on cyberspace is a significant and misunderstood vulnerability at home. The United States' lack of an effective cyber defence system, Mr. Clarke ominously warns, "will tempt opponents to attack in a period of tensions," and it could also tempt America to take pre-emptive action or escalate a cyber conflict very rapidly if attacked. This is not the path being pursued in the Pentagon's cyber strategy, which focuses on using converntional weapons to deter or respond to a cyber attack. Were a cyber war to start, Clarke warns it could easily jump international boundaries, causing cascades of collateral damage to cyber critical infrastructure to unspool around the world. His proposed response is to focus on separating critical infrastructure from "the open-to-anyone" Internet. Such a solution should be viewed with scepticism as it has serious practical impediments, given the wide reach and expanse of the Internet and the near universal economic and industrial reliance on cyber systems.

Since leaving government service he has opened a consulting firm in Washington, "Good Harbor Consulting LLP" which is principally focused on issues of cyber security and critical infrastructure protection.

s.15(1) - International

DESIRED CANADIAN OUTCOME

To clearly communicate to the United States officials that Canada is committed to doing its part to secure our shared critical digital infrastructure, and to further our joint interests in the international arena.

TALKING POINTS

- [redacted]

- Canada is comitted to working with with the U.S. on cyber security issues at a number of levels and spanning the range of civilian and military domains.

- Work is ongoing to define an Action Plan as part of the Beyond the Border Vision process, and cyber security to support information sharing and thtreat reponse to protect our shared digital infrastructure will be an important part of it.

- Securing critical cross border infrastructure is a clear need and something we want to move ahead in doing with you, especially as concerning electrical grids.

To Richard Clarke

- You've written about a number of threats to North America through cyberspace. If you had to rank your top three, what would they be?

    - Why haven't there been occurrences of cyber-terrorism, if as you say, it is both a high-return activity and something which is a fatal vulnerability for the West?

- The U. S. military, and to a lesser extent some key allies' intelligence agencies, are aggressively exploring cyber deterrence. I'm curious as to what you think cyber deterrence would mean.

    - Given your experience with terrorism, do you think this will ultimately be successful?

- And if we shouldn't be looking at a deterrence model, where do you see conduct in cyberspace going?

RDIMS: 432960

CYBER SECURITY

Issue

- Information is a strategic asset, and Canada and a growing number of countries are putting in place national cyber security strategies to address this type of threat.

CANADIAN POSITION

- Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential to maintaining an innovative, prosperous economy and a secure society

- *Canada's Cyber Security Strategy* was announced by the Government in 2010. The Strategy unifies efforts across Government and reflects our view that cyber security is both an economic and a national security issue.

BACKGROUND

- Cyber systems – computers and the Internet – are fundamental for the effective operation of Government and national security, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians. A secure cyberspace is key to Canada's competitive advantage in the global marketplace, where industry relies on secure, stable and resilient digital infrastructure to transact business and protect personal and commercially sensitive information such as intellectual property.

- In recent years, there has been an alarming increase in the number of cyber incidents directed against all levels of society. The threats are often global in nature, and involve foreign states' military and intelligence agencies, transnational cyber criminals, industrial cyber espionage, and cyber terrorists looking to further military, economic and political objectives.

CYBER SECURITY – CANADA

- *Canada's Cyber Security Strategy* is now in its second year of implementation. It is designed to engage our international allies, as well as create partnerships with the private sector in promoting the cyber security of Canada's critical infrastructure sectors. Canada's Strategy is built on three pillars:

    - Securing Government systems to protect the information that Canadians and Canadian businesses entrust to us and to secure national security activities.

    - Partnering to secure vital cyber systems outside the federal government, including the systems that control our critical infrastructure and those that hold the valuable intellectual property of Canadian business. Early priorities include the governments of the provinces/territories and the

energy, financial, and telecommunications sectors.

- Helping Canadians to be secure online, We have started a national public awareness campaign to get Canadians the information they need to protect themselves online.

- The Strategy is a whole-of-Government effort being led by Public Safety Canada, with roles being played by 11 other departments and agencies. It allocates $90 million in funding over five years (2010-2015), with $18 million in annual funding thereafter.

CYBER SECURITY ACTIVITY IN THE AMERICAS

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

- There has been no uniform response to cyber security within the hemisphere or more generally. Some nations have dealt with it as an issue for telecommunications regulation, while some have taken a law-enforcement/anti-terrorism approach. A smaller group have pursued an intelligence or military response. By way of example, in August 2010, the Brazilian army created a cyber-defense wing known as the Centro de Defesa Cibernética do Exército (Army's Center for Cybernetic Security). Canada's Strategy has elements of all of those approaches, although is only minimally focussed on the military dimension.

- Experts have noted that a lack of dedicated resources and technical expertise present significant obstacles to cyber security programs in Latin America. The Organization of American States has been trying to provide the means to pool expertise and provide a regional focus for cyber security programs. In 2003, the OAS General Assembly passed Resolution 1939 calling for the "Development of an Inter-American Strategy to Combat Threats to Cybersecurity."

- Since that time, hemispheric cyber security work has continued under the leadership of the OAS' Inter-American Committee against Terrorism (CICTE). There are four main streams to the proposed OAS Strategy:

  - information sharing with telecommunication operators;
  - fostering public-private partnerships to increase awareness and education;
  - setting technical standards to ensure information stays secure; and
  - adopting similar standards in cyber-crime legislation and policies.

- These four goals align well with Canada's own efforts, with the first two points being explicit parts of our national Strategy, while the last two points have guided our international partnerships more generally.

Drafted by: Corey Dvorkin, Public Safety/ Cyber Policy, 990-9608
Date of Draft: 5 March 2012

CYBER SECURITY IN THE AMERICAS

KEY MESSAGES TO CONVEY

- Cyber security is recognized internationally as a national security issue demanding government attention. We all rely on information systems and technology, and there is no going back to paper based systems.

- But those networks and connections need to be safe if they are to continue to help fuel innovation and prosperity. In a networked world, our cyber security is only as strong as the weakest link.

- Canada has recognized this and released its own Cyber Security Strategy in 2010, an element of which commits us to working with partners, both abroad and domestically, to pursue our shared security.

- Our Strategy reflects our outlook that cyber security has elements of national security, of economic security as well as personal security and privacy. We see the best way to achieve those goals as being through partnerships, both in Canada and internationally.

- Finally, I would like to note that dealing with cyber security in a counter terrorism/anti-crime context, as has been the case in the OAS context, does not always capture all aspects of the issue. In moving ahead with this issue we should continue to ensure that critical infrastructure protection and public engagement and awareness remain focal points of our efforts.

- ***RESPONSIVE ONLY – If Asked for Resources***: Unlike the United States, Canada has not made capacity building and development assistance a formal part of our Cyber Security Strategy.

    - While we are not in a position to make firm commitments at this time, we anticipate that we may be able to share our experiences in an experts visit or a regional workshop.

Tab A4 - Notice sent to Critical Infrastructure partners
(La version française vous sera envoyée sous pli)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
INFORMATION NOTE
****

Number: IN11-501
Date: 4 February 2011

****
Cyber Security Awareness: Detecting and Reporting Targeted Emails Attacks
****

PURPOSE
=======
The purpose of this Information Note is to provide organisations with basic information in order to assist security personnel conduct an efficient user awareness campaign against Targeted Email attacks. CCIRC has seen a high frequency of successful attacks and recommends all organizations take action to avoid being similarly victimized.

Target Audience
===============
The target audience of this Information Note is: Government and Critical Infrastructure Sector organisations.

Note: This communication, including any information transmitted with it, is intended only for the use of the target audience. It must not be disseminated, in any way, in whole or in part, to groups outside the targeted audience without the consent of the originator. If you receive this communication in error or without authorization please notify the GOC immediately.

ASSESSMENT
==========
The Canadian Cyber Incident Response Centre (CCIRC) regularly receives reports of organisations receiving targeted emails to various individuals, sometimes senior officials, and often falsely appearing to come (spoofed) from another trusted individual or organisation.

Targeted malicious emails, or Spear Phishing attacks, are socially engineered emails tailored to target different audiences within a community. The emails generally use well-crafted messages to entice users to follow an embedded link leading to an external website hosting a malicious file, or to open up an attachment containing a trojanized file such as a ZIP (containing a malicious executable), MS Office (Word, Excel, Power Point) or PDF document. Opening the file may activate the malicious code and lead to the compromise of the user's computer.

Due to the careful crafting of the content of these malicious emails, it is often extremely difficult, even for the most security aware users, to discern between a valid and a targeted attack email. Further more, existing detection technologies are not always able to detect these attacks, which often leverage the latest vulnerabilities in commonly used software products. As a result, targeted emails remain a very effective attack vector used by malicious actors and are best combated by well informed and diligent users.

For this reason, CCIRC is providing below a user awareness tear-line which we hope

can assist organisations who may not have recently conducted user awareness campaigns about targeted emails. Given the number of reports related to targeted email attacks in the last few weeks, CCIRC is strongly recommending that all organisations conduct a user awareness campaign to educate users at all levels, especially users in key executive positions, on how to recognize and report suspicious emails to their departmental IT security staff..

----------Tear Line

Subject: Malicious Emails Targeting specific Individuals

What are Malicious Targeted Emails

Malicious Targeted Emails, also known as Phishing emails, are crafted to look as if they are sent from a legitimate organization. These emails attempt to fool you into either visiting a bogus web site, downloading malicious content on your computer or enticing you to provide sensitive personal information by masquerading as a similar site you trust (ex: your bank), or offer the promise of something you might be interested in, contained in an attachment, such as a report, a picture, even a software patch or a joke. Recent targeted email activity used well scripted social engineering techniques and the emails appeared to originate from a sender known to the recipient and contained subject matter content relevant to the recipients' field of work or priorities of their department.

What can happen ?

The consequences of being fooled by these emails, which unfortunately often evade anti-virus and other security solutions, may be the compromise of your computer system and the installation of malicious code capable of:

- Transmitting files secretly to the attacker
- Monitoring your online transactions and activities
- Turning your computer into a "bot" under the control of the attacker to portray you as the source of the next attack;
- Logging and transmitting to an attacker every keystroke you type, including passwords and other sensitive information, before security mechanisms can detect it.

What should I look for ?

To minimize exposure it is important to highlight some of the characteristics of these suspicious emails. The following is a non-exhaustive list of items which should raise your suspicion. Unfortunately, attackers are very creative and change these tactics regularly.

* E-mails from a known individual, sometimes senior management, originating from unexpected email accounts - Consider the likelihood that an executive would send you an email with work related instructions or directions from a webmail account (e.g. hotmail, yahoo, gmail etc).

* Inconsistent subject line and URL - If the subject line and the embedded URL or attachment is inconsistently referenced, it would be better to treat that email with caution. As an example:

Subject: Report on committee recommendations
Displayed URL: http://www.yourorganisation.ca/committee/
Actual link (visible in the source code of the email, or sometimes by hovering the mouse over the link):
http://www.locateaflowershop.com.co.cc/superfile.pdf

What should I do ?

Tab A4 - Notice sent to Critical Infrastructure partners

When an email is received and suspected to be a targeted attack or phishing email, you should contact <departmental point of contact>.

Security awareness is our first line of defence! Thank you for your assistance in securing our organisation's network and email systems.

----------Tear Line

IMPACT
======

The impact of a successful infection is typically the installation of an information stealing malware on the victim computer, and/or its use in a multi-step intrusion in order to infect and exfiltrate information from additional machines on the network.
In many reported cases, the malware used had very poor anti-virus detection rate.
Detection has often been the result of timely reporting by diligent users.

SUGGESTED ACTION
================

CCIRC recommends that departments promote IT security through education and awareness, and encourage employees to report suspicious emails to designated security officials.

References
==========

http://www.publicsafety.gc.ca/prg/em/cbr/csi-eng.aspx
http://www.publicsafety.gc.ca/prg/em/cbr/csb-eng.aspx
http://www.phonebusters.com/english/home-eng.html
http://www.antiphishing.org
http://www.us-cert.gov/reading_room/emailscams_0905.pdf

Note to Readers
==============

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquires into the role of Public Safety Canada, please contact the department's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
Email: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

s.16(2)(c)

Tab A4 - Notice sent to Critical Infrastructure partners

From: Durand, Stéphanie [mailto:Stephanie.Durand@ps-sp.gc.ca]
Sent: Thursday, February 17, 2011 10:40 AM
To: [interdepartmental mailing list of Communications contacts]
Subject: CYBER SECURITY MEDIA RELATIONS PROTOCOL and COORDINATION

Colleagues,

Further to the on-going media coverage relating to recent cyber incidents, all calls related to the Government of Canada's approach to cyber security should now be directed to Public Safety Canada:

Public Safety Canada

Media Relations

613-991-0657

media@ps-sp.gc.ca

Here are the PCO approved holding lines for now. We are currently drafting a ministerial statement as well. We will share once approved.

We do not comment on the details of security related incidents.

That said, our Government takes threats seriously and has measures in place to address them.

For media calls on the specific impacts and actions taken by **individual departments** to address incidents or protect their departmental networks, individual departments are to share their responsive lines with PS prior to respond. This will ensure consistency in messaging and approach. We will be building an evergreen package for your future reference.

Please note that **internal messages** to staff shouls also be coordinated. Kindly consult Public Safety Canada for consistent messaging and a coordinated approach for employee communications on cyber security issues. We will be working closely with TBS and other key partners on this.

French will follow.

Thanks everyone for your continued collaboration.

Stéphanie

IMPLEMENTATION OF CANADA'S CYBER SECURITY STRATEGY

In the original analysis of *Canada's Cyber Security Strategy*, Deputy Ministers validated a cost of The level of funding actually received was $90M/5 years. Funding for the first year ($14.5 m) has just been received as part of the 2010 Supplemental B process.

Under that level, precedence was given to bolstering existing capabilities and towards filling critical gaps.

The Strategy's overall level of $90M/5 years is split over three areas of effort: protecting government systems (partnering with other levels of government and the private sector to protect systems outside federal jurisdiction (and a public awareness campaign aimed at protecting Canadians

Strategy work on Protecting Government Systems – 2010/11

Public Safety is analyzing policy and capability gaps within the GC, and is using new resources to strengthen strategic level situational awareness. PS receives a total of and FTEs for 2010/11, but this supports work across all three Strategy areas.

- [redacted]

PWGSC receives $ [redacted] to support its responsibilities to feed GC consolidated situational awareness of SCNet.

Dvorkin/NCSD/24 Feb 2011

UNCLASSIFIED

ONE-MINUTE REBUTTAL

IN RESPONSE TO A QUESTION FROM

MR. DON DAVIES (NDP)
MEMBER FOR VANCOUVER KINGSWAY

Notice Date: February 17, 2011

Don Davies (NDP)
Vancouver Kingsway

Government Computer Systems (Hansard p. 8336)

Mr. Don Davies (Vancouver Kingsway, NDP):
Mr. Speaker, the scope and the depth of the cyber attack on the Canadian government is truly disturbing. While the Conservatives are trying to downplay the importance of this attack, it is obvious that they did not take these threats seriously.

We now know that the hackers were able to infect the very departments that hold the purse strings of the nation just weeks before a budget, and also an agency of the Department of National Defence. We still do not know if anything else has been compromised.

Will the government tell us what departments were infiltrated, and what was the damage caused?

Hon. Vic Toews (Minister of Public Safety, CPC):
Mr. Speaker, we do not comment on the details of security-related incidents.

Our government, however, takes threats seriously and measures are in place to address them. I would point out that the next phase of our economic action plan is still in development and officials have advised that budget security was not compromised.

HOUSE OF COMMONS

OTTAWA, ONTARIO
FEBRUARY XX, 2011

Check against delivery

Let me be clear, this Government does take all threats to Canada seriously and is committed to doing its part to secure Canada's vital cyber systems, and to help Canadians protect themselves, their families and their personal information online.

The release of the Strategy signalled that our Government attaches priority to cyber security. The Strategy sets the groundwork for collaboration outside government and greater coherence within government.

The Strategy recognizes that cyber security is now a strategic issue for Canada and not just a technical problem to be fixed. It strengthens the capability of the Government to protect its own systems and to

build credibility with Canadians and international partners. And, it promotes awareness in order to change behaviour.

As a result of these measures, Mr. Speaker, Canadians can be sure that our Government is committed to keeping Canada – including our cyberspace – safe, secure and prosperous.

Thank you.

140 words (approximately 1 minute)

Prepared by: Dvorkin/Mohammed
Date: February 23, 2011

UNCLASSIFIED

FOUR-MINUTE SPEECH

IN RESPONSE TO A QUESTION FROM

MR. DON DAVIES (NDP)
MEMBER FOR VANCOUVER KINGSWAY

Notice Date: February 17, 2011

Don Davies (NDP)
Vancouver Kingsway

Government Computer Systems (Hansard p. 8336)

Mr. Don Davies (Vancouver Kingsway, NDP):
Mr. Speaker, the scope and the depth of the cyber attack on the Canadian government is truly disturbing. While the Conservatives are trying to downplay the importance of this attack, it is obvious that they did not take these threats seriously.

We now know that the hackers were able to infect the very departments that hold the purse strings of the nation just weeks before a budget, and also an agency of the Department of National Defence. We still do not know if anything else has been compromised.

Will the government tell us what departments were infiltrated, and what was the damage caused?

Hon. Vic Toews (Minister of Public Safety, CPC):
Mr. Speaker, we do not comment on the details of security-related incidents.

Our government, however, takes threats seriously and measures are in place to address them. I would point out that the next phase of our economic action plan is still in development and officials have advised that budget security was not compromised.

HOUSE OF COMMONS

OTTAWA, ONTARIO
FEBRUARY XX, 2011

Check against delivery

I am pleased to address the question raised in the House by the member from Vancouver Kingsway on February 17, 2011, regarding Government computer systems.

While I cannot comment on the details of security-related incidents, I can assure you that our Government does take all threats to Canada seriously and is committed to keeping cyber networks secure and resilient.

As Honourable Members will know, cyber security affects us all.

Cyber attacks can take many forms and can have serious consequences. Individuals can be

bankrupted or have their identities stolen. Businesses can be robbed of confidential information and intellectual property. Military and national security operations can be compromised. And the systems that control critical infrastructure, such as our power grids, water treatment plants and telecommunications networks, can be disrupted.

Canadians – individuals, industry and governments – are embracing the many advantages that cyberspace offers, and our economy and quality of life are the better for it. But those who wish to do us harm are also taking advantage of cyber technology.

And while Canada is not alone in this space, we are an increasingly attractive target for foreign military

and intelligence services, criminals, and terrorists.

We are a nation rich in resources with a prosperous economy, which is why we need to work collaboratively to protect our national security, economic prosperity and quality of life.

More than ever, we are dependent upon collective security and resiliency to ensure both our individual and national security in cyberspace.

This is why our Government delivered on its 2010 Speech from the Throne commitment to implement a cyber security strategy to protect our digital infrastructure.

As Honourable Members will know, our Government launched *Canada's Cyber Security Strategy* in October of last year.

The Strategy includes measures to help secure Government digital systems to better protect the private information of Canadians. It will allow us to partner with our provincial, territorial, international, private sector and academic partners to protect vital cyber systems outside the Government of Canada. And it includes measures to help Canadians to be secure online.

The Strategy is permissive in that it sets a broad framework that is meant to endure for the long term, and commits to specific actions to make rapid

progress. Cyber security, as we all know, will require an ongoing effort.

The Strategy leverages current cyber security activities and weaves them into an integrated framework.

For example, the Strategy leverages the partnerships being established under the *National Strategy and Action Plan for Critical Infrastructure*.

It supports the ongoing efforts by our law enforcement community to work with partners and international allies in cracking down on those who use the Internet for crime and illegal activities.

Our Strategy complements the Government's efforts to promote the digital economy and builds upon legislation introduced by our Government, such as the recently passed anti-spam legislation, and amendments to the *Criminal Code* to create new offences related to obtaining, possessing and trafficking in identity documents or identity information.

Let me be clear; our Government is concerned about the security of Canadians. Through *Budget 2010: Leading the Way on Jobs and Growth*, we allocated $90 million over five years, and $18 million in ongoing funding, towards the cyber Strategy.

Through these resources and support, this Government trusts that *Canada's Cyber Security Strategy* provides the strategic framework to pursue the challenges and opportunities presented in cyberspace.

Thank you.

556 words (approximately 4 minutes)

Prepared by: Dvorkin/Mohammed
Date: February 23, 2011

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

Meeting with Mr. Erik S.M. Akerboom
Netherlands National Coordinator for Counter-Terrorism
December 2, 2010

DATE:

File No. : 375775

MEMORANDUM FOR THE DEPUTY MINISTER
c.c.: Lynda Clairmont

CYBER SECURITY

(Information only)

BACKGROUND - CANADA

- Cyber systems – computers and the Internet – are fundamental for the effective operation of Government, 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. Just as cyberspace is constantly evolving, so too are the cyber threats to our security, prosperity and quality of life.

- 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. Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

- *Canada's Cyber Security Strategy* was announced by the Government on October 3, 2010. The Strategy unifies efforts across Government and enhances cyber security activities, engages the private sector in promoting the cyber security of Canada's critical infrastructure, and promotes safety online for citizens. It 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; and,

- Helping Canadians to be secure online, through improved awareness and access to the information they need to protect themselves.

- The Strategy is a whole-of-Government effort being led by Public Safety Canada, with the key roles being played by 11 departments and agencies. It allocates $90 million in funding over five years, with $18 million ongoing.

BACKGROUND – NETHERLANDS

- The Netherlands do not, as yet, have a dedicated cyber security program, but are working towards developing one. That said, the threat has been publicly recognized: the Dutch General Intelligence and Security Service (the Dutch analogue to CSIS) has released a public brochure explicitly warning the general public about digital espionage.

- Within the Dutch government, interdepartmental coordination of cyber security is handled by the Ministry of Security through its national security division, while cyber crime is handled by the Ministry of Justice. Cyber terrorism falls under Mr. Akerboom's purview, as National Coordinator of Counter-Terrorism. Interestingly, cyber defence is a shared responsibility between the Ministry of Defence and the Ministry of Security. Finally, national critical infrastructure protection against cyber threats is handled by the Ministry of Economics, which is different than the Canadian model, where that responsibility lies with Public Safety Canada.

- In debate over the 2010 defence budget, then-Defence Minister Eimert van Middelkoop was questioned by parliamentarians as to what efforts were being undertaken to secure the Netherlands against the cyber threat. His written response suggests that the Netherlands may be preparing to engage significantly in cyber security, and he also shed new light on previously unknown activities. He noted that Amsterdam had been following cyber security developments in countries such as 'the United States, the United Kingdom and Germany,' and had begun to engage private sector partners in the Netherlands, which he acknowledged have a crucial role to play. He stated it was the intention of the Dutch government to:

  - create and begin implementing a cyber security strategy;
  - develop a cyber incident response plan;
  - explore the legal aspects of cyber intelligence gathering and information sharing; and,
  - engage with NATO on cyber defence and specifically with the Alliance's Cyber Security Centre of Excellence in Tallinn, Estonia (to date, Canada has not engaged with Centre).

- [redacted]

- Even absent a formal cyber strategy, Dutch authorities have taken some enormously significant actions to secure their cyberspace. In October 2010, the Dutch High Crime Tech Team took down 143 servers in Holland affiliated with the 'Bredolab' botnet. This botnet, with origins in Russia, has infected over 30 million computers worldwide since being deployed in July 2009, and is designed to steal personal and financial information. The same day, acting on information provided by Dutch authorities, Armenian police arrested a 27-year old man, alleged to have been running this botnet, while he was trying to leave that country. Some 100,000 Dutch computer users were contacted by the Dutch police – who hacked into the botnet controls to spread the police message - and warned their machines were infected. This had prompted public questioning over whether Dutch police exceeded their authority and breached privacy laws.

- It bears noting that Armenia and the Netherlands are both full parties to the European Convention on Cybercrime, which might have provided the legal framework for this operation. Canada has signed, but not ratified the Convention, although the Government has introduced Bill C-52 ('Lawful Access') which would allow ratification. It is highly questionable whether Canadian authorities could stage a similar counter-botnet operation under current law.

DISCUSSION:

- [redacted] Certainly there are some parallels: the Netherlands is a federated nation with twelve provinces, and a parliament (split nearly equally among five main parties) which is now learning to operate largely on the basis of consensus and coalitions. The Netherlands also has a strong tradition of social and civil-society engagement, with historically much less emphasis placed on national security issues.

- [redacted]

- From a Canadian perspective, the recent Dutch operation against the 'Bredolab' botnet is extremely interesting. It would be highly instructive to know how the

decision to bring down the botnet was reached inter-departmentally and how it was carried out, what legal or privacy constraints were considered, and whether these actions are viewed as pushing the limits of Dutch law.

SUMMARY PARAGRAPH:

- Like many other countries, Canada is concerned about the increasing threats emanating from cyberspace. The Government of Canada has taken action to address these threats, and it released *Canada's Cyber Security Strategy* this October. Over its first five years, the *Strategy* will strengthen our cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world. It will be the basis for expanding international cooperation, ensuring that Canadian expertise and resources can contribute to addressing this threat and help secure the global commons of cyberspace. It will also support the policy and legislative development necessary to address issues like the 'Bredolab' botnet and other emerging threats.

KEY MESSAGES TO CONVEY:

- Information and communication systems play a key role for us all in achieving prosperity in all Western countries. As our dependence on cyber systems increases, so too does the value of an attack on them.

- On October 3, 2010 the Government of Canada announced the launch of *Canada's Cyber Security Strategy*.

- The Strategy is the Government's plan to bolster the nation's response to cyber threats. It is centered on three main pillars: securing government systems; partnering to secure vital systems outside the federal Government; and, helping Canadians be secure online.

- Over its first five years, the *Strategy* will strengthen our cyber systems and critical information infrastructure, support economic growth and protect Canadians.

- Engaging internationally is part of this Strategy, and we have seen cyber security emerge as a major issue within NATO. We can't afford any weak links in cyberspace.

KEY QUESTIONS TO ASK:

- I understand that **your government is developing a cyber security strategy** of its own. How is that unfolding and what sort of timelines do you see? What are the threats you are trying to address?

- **Responsive:** In dealing with our own private sector - which in Canada also holds much of the critical infrastructure - we have found that they wish to avoid having to deal with the Government in multiple venues. As such we have tried to use existing mechanisms, such our National Strategy and Action Plan for Critical Infrastructure, to get the cyber security message across.

- **Responsive 2:** Industry knows generally what threats they face, and have a vested interest in protecting themselves. What the private sector seems most interested in is getting access to the relevant intelligence that Government has, so they can take informed and timely action to best defend their business. Information sharing to the private sector may be one of our larger policy and operational challenges, and it's something we are still working through.

- The Government is taking action to move forward and ratify the Council of Europe Convention on Cybercrime, which we signed in 2001. In that light, the actions by Dutch police against the **Bredolab botnet** last month are very interesting.

  - Press reports seem to indicate it was controversial in the Netherlands. Was it pushing the limits of what is allowed under your law?

  - Given the increasing cyber threats, such actions – whether nationally or with international coalitions - might become the norm in the future. Citizens will expect their governments to protect them.

  - [redacted]

s.21(1)(a)

Author's name: Corey Michael Dvorkin, Cyber Policy Division, 990-9608
Approving Authority: Robert Dick, DG National Cyber Security Directorate, 990-2661
Date: 30 November 2010

MISPA Preparatory Meeting
November 18-19, 2010

CYBER SECURITY

BACKGROUND - CANADA

- Cyber systems – computers and the Internet – are fundamental for the effective operation of Government, 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. Just as cyberspace is constantly evolving, so too are the cyber threats to our security, prosperity and quality of life.

- 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. Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

- *Canada's Cyber Security Strategy* was announced by the Government on October 3, 2010. The Strategy unifies efforts across Government and enhances cyber security activities, engages the private sector in promoting the cyber security of Canada's critical infrastructure, and promotes safety online for citizens. It 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; and,

  - Helping Canadians to be secure online, through improved awareness and access to the information they need to protect themselves.

- The Strategy is a whole-of-Government effort being led by Public Safety Canada, with the key roles being played by 13 departments and agencies. It allocates $90 million in funding over five years, with $18 million ongoing.

BACKGROUND – ORGANIZATION OF AMERICAN STATES (OAS)

- Amongst OAS countries, only the United States and Canada have released formal cyber security strategies, although the OAS has been looking at cyber security for several years.

- On June 10, 2003, the OAS General Assembly passed Resolution 1939 calling for the "Development of an Inter-American Strategy to Combat Threats To Cybersecurity." This is to be developed in coordination with the OAS' Inter-American Committee against Terrorism, the Inter-American Telecommunication Commission, and the Ministers of Justice/ Attorneys General of the Americas' Group of Governmental Experts on Cyber-Crime.

- The commitment to a shared approach to cyber security was reiterated later that year by the Special Conference on Security in Mexico City, from October 28-29, 2003, where OAS member states agreed to "develop a culture of cybersecurity in the Americas by taking effective preventive measures to anticipate, address, and respond to cyber attacks, whatever their origin, fighting against cyber threats and cybercrime, criminalizing attacks against cyberspace, protecting critical infrastructure and securing networked systems."

- Since that time, cyber security work has continued under the leadership of the OAS' Inter-American Committee against Terrorism (CICTE), and work on the OAS Strategy is ongoing. 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.

- As part of the CICTE working group, the OAS has also been looking to develop plans for the creation of hemisphere-wide 24/7 Computer Security Incident Response Teams (CSIRTs), capable of rapidly sharing cyber security information and providing technical guidance to support mitigation and recovery efforts in the event of a cyber incident. The last virtual meeting of the CSIRT team was held on June 17, 2010, while training workshops for various hemispheric CSIRT personnel were recently held in St. John's, Antigua and Barbuda from July 12-15, 2010, Panama City, Panama from July 6-10, 2010, and Santo Domingo, Dominican Republic from April 14-16, 2010. The OAS also regularly supports other operational and technical visits and exchanges to help facilitate the exchange of best practices.

STRATEGIC RECOMMENDATIONS

- While there is no assigned funding in *Canada's Cyber Security Strategy* dedicated to international capacity building, Canadian activities on this front will be delivered

within existing resources. For example, Public Safety Canada is sending a technical expert to a workshop on cyber security best practices in Montevideo, Uruguay from November 15-17, 2010, in response to an OAS request.

TALKING POINTS

How does this topic affect Canada, key states, and the international community?

- Cyber security is recognized internationally as a national security issue demanding government attention. We all rely on information systems and technology, and we are all looking to expand those networks – a point made explicit at the Third Summit of the Americas, held in Quebec City, Canada in 2001, where our leaders committed to further increasing connectivity in the Americas.

- But those networks and connections need to be safe if they are to continue to help fuel innovation and prosperity. Canada has recognized this and released its own Cyber Security Strategy on October 3, 2010, an element of which commits us to working with our international partners to pursue our shared security.

- The draft OAS Strategy is an initiative that we support. In fact, several of its tenets – public-private partnerships, increasing awareness and education, and information sharing with telecommunication operators – can be seen in *Canada's Cyber Security Strategy*.

What is Canada doing about this topic?

- On October 3, 2010, the Government of Canada announced *Canada's Cyber Security Strategy* to provide a national approach to this issue. The Strategy unifies efforts across Government and enhances cyber security activities, engages the private sector in promoting the cyber security of Canada's critical infrastructure and economic interests, and promotes safety online for citizens.

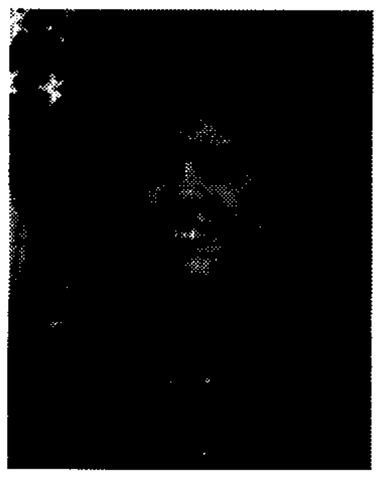
What does Canada desire to have done about this topic?

- Canada supports the ongoing work to address cyber security being undertaken by the Inter-American Committee against Terrorism. In a networked world, our cyber security is only as strong as the weakest link. As *Canada's Cyber Security Strategy* begins to align resources and programs internally, we will explore how we can share our experience.

    - Responsive Only: While we are not in a position to make firm commitments at this time, we anticipate that we may be able to share our experiences in an experts visit or a regional workshop.

- Similarly, efforts to establish a hemispheric Computer Security Incident Response Team capability are commendable, and something we continue to support. Where possible, consideration should be given to expanding future cooperation on this front.

- Finally, I would like to note that dealing with cyber security in a counter terrorism/anti-crime context, as has been the case in the OAS context, does not always capture all aspects of the issue. In moving ahead with this issue and developing the draft OAS Strategy, we should continue to ensure that critical infrastructure protection and public engagement and awareness remain focal points of our efforts.



Bilateral with U.S. Secretary of Homeland Security Janet Napolitano

Halifax International Security Forum

Halifax, NS
November 5-6, 2010

CANADA'S CYBER SECURITY STRATEGY

Background:

Cyber systems – computers and the Internet – are fundamental for the effective operation of Government, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians. Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

The interconnectedness of cyber systems means that these systems are only as strong as their weakest link. Cyber security is a shared responsibility – no single country, government, organization or individual can truly secure its networks in isolation. The United States, the United Kingdom and Australia have all developed new cyber security strategies, and all Canada's allies maintain a high interest in related Canadian activities.

Cyber security also has an important bi-lateral dimension. Canada the U.S. and eleven international partners participated in Cyber Storm III in September, an international exercise simulating a large-scale cyber-attack on critical infrastructure. Cyber security and critical infrastructure protection was a topic at last month's Emergency Management Consultative Group meeting held in Washington, and it will be raised at the forthcoming Permanent Joint Board of Defence meeting in January, which is being hosted by Canada at NORAD Headquarters in Colorado Springs.

Canada's Cyber Security Strategy:

*Canada's Cyber Security Strate*gy (the Strategy) was announced by the Government on October 3, 2010. The Strategy unifies efforts across Government and enhances cyber security activities, engages the private sector in promoting the cyber security of Canada's critical infrastructure, and promotes safety online for citizens.

The Strategy is built on three pillars:

- securing Government systems to protect the information entrusted to us by Canadians, 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

- helping Canadians to be secure online, through improved awareness and access to the information they need to protect themselves.

The Strategy allocates $90 million in funding over five years, with $18 million ongoing. Twelve departments and agencies are formally part of the Strategy, although not all received funding. Public Safety Canada (PS) will receive $32.1M/five years for policy leadership and coordination, and for spearheading efforts at private sector engagement and public awareness. The RCMP will receive $7.5M/five years, and there is additional funding allocated to CSIS for national security work.

Strategy implementation is underway, and activities are beginning or already underway on a range of operational, policy and engagement activities. One of the key engagement areas is with the private and Critical Infrastructure (CI) sectors. These activities will occur under the aegis of the National Cross Sector Forum, established under the *National Strategy and Action Plan for Critical Infrastructure*, and the first meeting is scheduled for December 1, 2010. Four sectors (telecommunications, finance, energy and government) are early priorities for cyber security engagement.

Background – U.S. Activities

The U.S. "Cyberspace Policy Review" was released on May 29, 2009. This was an extremely ambitious document covering the full range of threat reduction, deterrence, international engagement and incident response activities, including roles for law enforcement, diplomacy, military and intelligence agencies. Cyber security activities in the U.S. are led by "cyber czar" Howard Schmidt, who is the formally titled the White House Cybersecurity Coordinator.

Operationally, the U.S. Department of Homeland Security (DHS) has been the American lead, although the Department of Defense (DoD) has been increasingly active, as has the National Security Agency (NSA) and the newly created U.S. Cyber Command. Some analysts have commented that it is not immediately clear that these numerous missions and visions for cyber security are complimentary.

As part of a major international speech in Brussels this September, U.S. Deputy

Secretary of Defense William Lynn announced the five pillars of the forthcoming Pentagon cyber security strategy:

- Cyberspace must be recognized as a warfare domain equal to land, sea, and air
- Any defensive posture must go beyond "good hygiene" to include sophisticated and accurate operations that allow rapid response
- Cyber defenses must reach beyond the Pentagon's "dot-mil" domain into commercial networks, "as governed by Homeland Security"
- Cyber defenses must be pursued with international allies for an effective shared warning of threats
- U.S. technological dominance must be maintained, and the military's acquisitions process needs to be improved to keep up with the speed and agility of the information technology industry.

[redacted]

[redacted] On October 13, 2010 DHS and DoD announced they had signed a Memorandum of Understanding covering cyber security. The agreement embeds DoD cyber analysts within DHS to better support the National Cybersecurity and Communications Integration Center (NCCIC) and sends a senior DHS official to the NSA, along with a support team comprised of DHS privacy, civil liberties and legal personnel.

[redacted]

CYBER SECURITY KEY MESSAGES:

- Robust continental security can only be achieved through a "whole of nation" collaborative effort. The free movement of trade, commerce, people, information and ideas between our two nations is critical to our shared economic, security and defence interests.

- We certainly recognize the risks. On October 3, 2010 the Government of Canada announced the launch of Canada's first Cyber Security Strategy. It is an initial five-year plan designed to take our national efforts to the next level.

- It is centered on three main pillars: securing government systems; partnering to secure vital systems outside the federal Government; and, helping Canadians be secure online.

- It will do this by leveraging existing initiatives and building on connections to the private sector and to key allies.

- Many parts private sectors already have close linkages, which creates the need for us to ensure that Government actions don't resonate negatively across the border.

- Implementation of the Strategy has already begun and we will be looking at engaging with your Government more closely in the months ahead.

- Given our shared border and deep connections in defence and security, we will be cooperating very closely with the United States across all sectors (PS/DHS; DND/DoD; RCMP/FBI ; and many others).

- Aside from ensuring there are no internal national obstacles to cooperation, we will need to ensure that our respective leads on the various elements of cyber security are clear.

- In Canada, those efforts will be led by Public Safety Canada.

- We would be interested in learning more about the MoU on cyber security you have just concluded with DoD.

Corey Dvorkin, Public Safety Canada, National Cyber Security Directorate, 990-9608. November 1, 2010

RDIMS 309072
October 5, 2010

Ministerial Statement

- Mr Speaker, I am pleased to announce that on October 3, 2010, this Government launched its first Cyber Security Strategy. The release of the Strategy marks the first step in delivering on our Government's 2010 Speech from the Throne commitment to working with the provinces, territories and the private sector to implement a cyber security strategy to protect our digital infrastructure.

- In the digital age, our nation, our economy and our quality of life are only as secure as our digital infrastructure.

- Our economy, daily government operations, communications and many of the necessities of life, including energy and public utilities, now depend on computers, networked devices and the Internet. For example, as of September 2009, over 26 million Canadians were connected to the Internet. That amounts to nearly 80 percent of the population.

- Our economic prosperity and quality of life increasingly depend on trust and confidence in the security and reliability of our critical infrastructure.

- Protecting the cyber systems that Canada and Canadians depend on is a new role for Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

- Canada's competitive position in the global economy depends on secure digital infrastructure. In addition to our Government's digital economy strategy, which will ensure that Canada remains a global economic leader in the years to come, our economic leadership will also be based on a stable, reliable and secure digital infrastructure. As will our way of life.

- That is why our Government takes cyber security very seriously and is doing its part to protect Canadians by taking action.

- We know that cyberspace is not just a place where law-abiding Canadians do business, socialize, or access government services. Rather, our infrastructure is increasingly facing significant threats. Those threats include sophisticated cyber espionage conducted by well-financed and state-backed organizations. They include organized criminal syndicates, terrorists developing cyber attack capabilities, and individual but highly skilled hackers.

- Cyber attacks can shut down and deny command and control of vital systems, and cause physical damage. For example, for several weeks in April 2007, botnets involving over one million computers in 20 countries disrupted Estonia's government websites, emergency response services, banks, news and communications services. Similar attacks were launched against Georgia during Russia's 2008 ground offensive into that country.

- Canada and Canadians are not immune to these constantly evolving and changing threats. That's why our Government has played a leadership role in responding to emerging cyber threats and keeping our digital infrastructure safe.

- Under Prime Minister Harper's leadership, our Government has already taken action by introducing tough new laws to crack down on cyber crime and through public awareness events such as Cyber Security Awareness month, which serves to remind all Canadians of the risks online and some of the steps they can take to protect themselves.

- But today we are doing more.

- Our government is committing $90 million to *Canada's Cyber Security Strategy* over the next five years in order to significantly enhance our ability to meet the cyber threat.

- The Strategy is Canada's plan to meet these threats. It will do this in several ways:

- First, we will continually strengthen the security of our Government systems in order to keep pace with the rapidly evolving cyber security threats. Those who would harm us will not rest, and we won't either.

- Securing government systems is an essential first step in protecting the information that Canadians and Canadian businesses entrust to us and to securing the systems that help keep our borders open to trade and travellers and our economy open for business, and to deliver nearly 130 federal programs, services and benefits to Canadians.

- The Strategy will increase our Government's capability to detect, defend, deter and neutralize cyber threats. We will work to reduce the number of Internet access points across the Government's networks and we will create an Integrated Cyber Crime Fusion Centre to increase the capability to detect and analyze cyber crime.

- But cyber security is a shared responsibility, and our Government is not alone in wanting to protect and secure the digital systems upon which we all depend.

- So second, we will strengthen partnerships with the provinces, territories and the private sector by improving information sharing, research and cooperation.

- We will partner with other levels of government and the private sector to secure vital systems outside the federal government. We will help ensure that the systems that control our critical infrastructure – such as water, electricity, natural gas and banking – remain up and running in the face of cyber threats and that personal information remains safe.

- The Government is committed to putting in place the mechanisms and structures to lead and coordinate cyber security efforts. We can and must do better, and we will start by putting in place protocols to share information with one another about threats

and mitigation strategies, but also by focusing on cyber security as a cross-cutting policy issue that requires the attention of senior leaders – Ministers, Deputies, CEOs.

- *Canada's Cyber Security Strategy* will leverage existing networks – such as those announced under the National Strategy and Action Plan for Critical Infrastructure. We will provide new opportunities for governments and industry to better collaborate on cyber security issues, because our systems are all interconnected, and we are only as secure and strong as our weakest link. For example, by encouraging joint public/private sector initiatives to identify and share best practices to address threats to the security of the process control systems that run from everything from our electrical grids to manufacturing processes in factories.

- Third, Canada's Cyber Security Strategy will help to enhance Canadians' awareness of cyber security. This Government will be leading public awareness and outreach activities to inform Canadians of the potential risks they face and the actions they can take to protect themselves and their families online. We will also increase Canadians' awareness of common online crimes and will promote safe cyber security practices through the use of websites, creative materials and outreach efforts.

- By helping Canadians be secure online, we enable our citizens to take the necessary steps to protect themselves and their families from identity theft, fraud, and other kinds of cybercrimes, and to prevent their computers from being taken over by criminals.

- The responsibility for cyber security cannot be compartmentalized, and it can't be delegated. Cyber security is everyone's responsibility. That's why our Government has followed through on its commitment.

- That is what the Strategy we have announced is all about.

- It's about working together to keep our personal information safe online and to ensure that the critical services we rely on are protected. It's about working together to guard against cyber threats that are continually evolving.

- It's about making sure we continue to provide the solid foundation of a secure digital infrastructure that our future economic prosperity depends on.

- It's about national security and it's about economic security. It's about securing the Canada we want to have.

- It's about leadership and taking action, which our government has done since we were first elected in 2006. We've taken decisive action to crack down on crime and keep Canadians safe. And, we're going to continue to do that when it comes to cybercrime and protecting our digital infrastructure.

s.19(1)

CANADA'S CYBER SECURITY STRATEGY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND INFORMATION ABOUT THE GOVERNMENT OF CANADA'S NEW NATIONAL CYBER SECURITY STRATEGY.

PROPOSED RESPONSE:

- **This Government takes cyber security very seriously. We have already done a lot, by introducing tough new laws to crack down on cyber crimes and spam and better protect Canadian's personal information. And on October 3rd we launched Canada's first national strategy for cyber security to do even more.**

- ***Canada's Cyber Security Strategy* is our Government's plan for meeting the evolving cyber threat, and our commitment to strengthen the security of government systems that we rely on for national security, to deliver programs services and benefits to Canadians, and to keep the personal and confidential information of Canadians and businesses private.**

- **Our Government will leverage existing relationships with owners and operators of critical infrastructure, and establish new partnerships with the provinces and territories to help secure vital cyber systems outside the federal government.**

- **Canadians are worried about cybercrime and protecting themselves, their families and their privacy online. Our Government will get them the information they need to help them do so. This Strategy will allow us to do more to keep Canada and Canadians safe in the digital age.**

- **This Strategy will ensure our secrets are secure, and protect our industries and the research and innovation that fuel our economy. It will help Canadians to connect safely to each other and to the world.**

- **It is a 21st Century plan for a 21st Century nation.**

CONTACTS:			
Prepared by Rose Coelho, Director Cyber Policy, National Cyber Security Directorate, EMNS	Tel. no. Ph: (613) 993-9537 Cell:	Approved by (ADM level only) Lynda Clairmont, ADM EMNS	Tel. no. Ph: (613) 990-4976 Cell:

Question Period Note

CANADA'S CYBER SECURITY STRATEGY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND INFORMATION ABOUT THE GOVERNMENT OF CANADA'S NEW NATIONAL CYBER SECURITY STRATEGY.

ISSUE:

Cyber security is recognized internationally as a national security issue demanding government attention. There has been recent media interest in the topic, focusing on alleged espionage activities by China, and on reports that cyber viruses have now been "weaponized" and are being used by states against each other. Several of Canada's allies have begun to implement cyber security strategies to protect themselves, and Canada has announced its own cyber security strategy to provide a national approach to this issue.

BACKGROUND:

Cyber systems – computers and the Internet – are fundamental for the effective operation of Government, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians.

Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

In the last year, there has been an increase in the number of cyber incidents directed against all levels of society leading to increased attention to the topic by our key allies, in particular the United States. The threats are daily and global, involving: foreign states' military and intelligence agencies, transnational cyber-criminals, industrial cyber espionage, and cyber terrorists looking to further military, economic and political objectives.

The interconnectedness of cyber systems means that these systems are only as strong as their weakest link. Cyber security is a shared responsibility – no single country, government, organization or individual can truly secure its networks in isolation; others must also do their part. The United States, the United Kingdom and Australia have all developed new cyber security strategies and maintain a high interest in related Canadian activities.

Recent media reports have focused on the "Stuxnet" virus, which appears to be designed to target computer systems used in the control systems of the nuclear energy industry. Suggestions have been made it was specifically engineered to deliberately cripple the computers involved in the (alleged) Iranian nuclear weapons program. The Government of Canada has been actively involved in mitigating efforts in Canada to cleanse similar systems and ensure they remain unaffected.

Coincidentally, this week Canada, the United States and ten other countries participated in Cyber Storm III, an international exercise simulating a large-scale cyber-attack on critical infrastructure.

Canada's Cyber Security Strategy unifies and enhances cyber security activities within government, to engage the private sector in promoting the cyber security of Canada's critical infrastructure, and to promote safety online for citizens.

CANADA'S CYBER SECURITY STRATEGY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND INFORMATION ABOUT THE GOVERNMENT OF CANADA'S NEW NATIONAL CYBER SECURITY STRATEGY.

PROPOSED RESPONSE:

- **Le gouvernement en place prend la cybersécurité très au sérieux. Nous avons déjà beaucoup fait dans ce dossier, en nous attaquant à la cybercriminalité et à l'envoi de pourriels, et en nous efforçant de mieux protéger les renseignements personnels des Canadiens. Dans cette optique, le 3 octobre, nous avons lancé la première stratégie de cybersécurité du Canada pour en faire encore plus.**

- **La *Stratégie nationale de cybersécurité* représente le plan qu'a mis sur pied notre gouvernement pour faire face à l'évolution constante de la menace à la cybersécurité. Elle nous permettra également de respecter nos engagements visant à renforcer la sécurité des systèmes gouvernementaux sur lesquels nous comptons pour assurer la sécurité nationale ainsi que les services de programmes et autres prestations pour les Canadiens, et pour veiller à ce que les renseignements personnels et confidentiels des Canadiens et des entreprises restent privés.**

- **Notre gouvernement tirera profit des liens déjà établis avec les propriétaires et exploitants d'infrastructures essentielles, et il mettra en place de nouveaux partenariats avec les représentants provinciaux et territoriaux pour assurer la sécurité des systèmes cybernétiques vitaux qui ne relèvent pas du gouvernement fédéral.**

- **Les Canadiens se préoccupent de la cybercriminalité ainsi que de la nécessité de se protéger et de protéger leur famille et leurs renseignements personnels en ligne. Notre gouvernement leur fournira l'information nécessaire pour assurer leur protection. Cette stratégie nous permettra d'en faire encore plus pour assurer la sécurité du Canada et des Canadiens dans cette ère numérique.**

- **Elle nous permettra également de veiller à ce que nos secrets ne soient pas divulgués au grand jour, et à protéger nos industries ainsi que les recherches et les innovations qui alimentent notre économie.**

Elle aidera aussi les Canadiens à se connecter entre eux et avec le monde, et ce, en toute sécurité.

- **Il s'agit d'un plan du 21e siècle pour un pays du 21e siècle.**

CONTACTS:			
Prepared by Rose Coelho, Director Cyber Policy, National Cyber Security Directorate, EMNS	Tel. no. Ph: (613) 993-9537 Cell: [redacted]	Approved by (ADM level only) Lynda Clairmont, ADM EMNS	Tel. no. Ph: (613) 990-4976 Cell: [redacted]

s.19(1)

QUESTION PERIOD NOTE

Date: October 4, 2010
Classification: UNCLASSIFIED
Branch / Agency: EMNS/Cyber

Question Period Note

CANADA'S CYBER SECURITY STRATEGY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND INFORMATION ABOUT THE GOVERNMENT OF CANADA'S NEW NATIONAL CYBER SECURITY STRATEGY.

ISSUE:

Cyber security is recognized internationally as a national security issue demanding government attention. There has been recent media interest in the topic, focusing on alleged espionage activities by China, and on reports that cyber viruses have now been "weaponized" and are being used by states against each other. Several of Canada's allies have begun to implement cyber security strategies to protect themselves, and Canada has announced its own cyber security strategy to provide a national approach to this issue.

BACKGROUND:

Cyber systems – computers and the Internet – are fundamental for the effective operation of Government, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians.

Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

In the last year, there has been an increase in the number of cyber incidents directed against all levels of society leading to increased attention to the topic by our key allies, in particular the United States. The threats are daily and global, involving: foreign states' military and intelligence agencies, transnational cyber-criminals, industrial cyber espionage, and cyber terrorists looking to further military, economic and political objectives.

The interconnectedness of cyber systems means that these systems are only as strong as their weakest link. Cyber security is a shared responsibility – no single country, government, organization or individual can truly secure its networks in isolation; others must also do their part. The United States, the United Kingdom and Australia have all developed new cyber security strategies and maintain a high interest in related Canadian activities.

Recent media reports have focused on the "Stuxnet" virus, which appears to be designed to target computer systems used in the control systems of the nuclear energy industry.
Suggestions have been made it was specifically engineered to deliberately cripple the computers involved in the (alleged) Iranian nuclear weapons program. The Government of Canada has been actively involved in mitigating efforts in Canada to cleanse similar systems and ensure they remain unaffected.

Coincidentally, this week Canada, the United States and ten other countries participated in Cyber Storm III, an international exercise simulating a large-scale cyber-attack on critical infrastructure.

Canada's Cyber Security Strategy unifies and enhances cyber security activities within government, to engage the private sector in promoting the cyber security of Canada's critical infrastructure, and to promote safety online for citizens.

QUESTION PERIOD NOTE

Date: September 30, 2010
Classification: UNCLASSIFIED
Branch / Agency: EMNS/Cyber

Question Period Note

CYBER SECURITY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND THE STATUS OF THE GOVERNMENT OF CANADA'S EFFORTS TO DEVELOP A NATIONAL CYBER SECURITY STRATEGY.

ISSUE:

Cyber security is increasingly being recognized as a national security issue demanding government attention. There has been recent media interest in the topic, focusing on alleged espionage activities by China, and on reports that cyber viruses have now been "weaponized" and are being used by states against each other. Several of Canada's allies have begun to implement cyber security strategies to protect themselves, and Canada has acknowledged it intends to do the same.

BACKGROUND:

Cyber systems – computers and the Internet – are fundamental for the effective operation of Government, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians.

Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

In the last year, there has been an increase in the number of cyber incidents directed against all levels of society leading to increased attention to the topic by our key allies, in particular the United States. The threats are daily and global, involving: foreign states' military and intelligence agencies, transnational cyber-criminals, and cyber terrorists looking to further military, economic and political objectives.

The interconnectedness of cyber systems means that these systems are only as strong as their weakest link. Cyber security is a shared responsibility – no single country, government, organization or individual can truly secure their networks in isolation; others must also do their part.

Recent media reports have focused on the "Stuxnet" virus, which appears to be designed to target computer systems used in the control systems of the nuclear energy industry.
Suggestions have been made it was specifically engineered to deliberately cripple the computers involved in the (alleged) Iranian nuclear weapons program. The Government of Canada has been actively involved in mitigating efforts in Canada to cleanse similar systems and ensure they remain unaffected.

Coincidentally, this week Canada, the United States and ten other countries participated in Cyber Storm III, an international exercise simulating a large-scale cyber-attack on critical infrastructure.

Canada is developing a national cyber security strategy to unify and enhance cyber security activities within government, to engage the private sector in promoting the cyber security of Canada's critical infrastructure, and to promote safety online for citizens. An announcement is expected very soon.

The United States, the United Kingdom and Australia have all developed new cyber security strategies and maintain a high interest in related Canadian activities.

CYBER SECURITY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND THE STATUS OF THE GOVERNMENT OF CANADA'S EFFORTS TO DEVELOP A NATIONAL CYBER SECURITY STRATEGY.

PROPOSED RESPONSE:

- **The Government of Canada takes cyber security very seriously and is doing its part to protect the cyber systems that Canada and Canadians depend on.**

- **My department is leading cross-government efforts to enhance the cyber integrity of government and protect Canada's critical digital infrastructure and secure our digital economy.**

- **Canadians are worried about cyber-facilitated crime and protecting themselves, their families and their way of life online, and our Government will help them do that.**

- **As announced in the Speech from the Throne, our Government is committed to working with the provinces and territories to implement a cyber security strategy to protect our digital infrastructure.**

- **These efforts would build on significant efforts already underway in Government, and be based on consultations with the private sector and our international allies.**

- **This Strategy will be a key first step to ensuring Canada and Canadians are safe in the digital age.**

CONTACTS:			
Prepared by Rose Coelho, Director Cyber Policy, National Cyber Security Directorate, EMNS	Tel. no. Ph: (613) 993-9537 Cell:	Approved by (ADM level only) Lynda Clairmont, ADM EMNS	Tel. no. Ph: (613) 990-4976 Cell:

s.19(1)

Question Period Note

CYBER SECURITY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND THE STATUS OF THE GOVERNMENT OF CANADA'S EFFORTS TO DEVELOP A NATIONAL CYBER SECURITY STRATEGY.

ISSUE:

Cyber security is increasingly being recognized as a national security issue demanding government attention. There has been recent media interest in the topic, focusing on alleged espionage activities by China, and on reports that cyber viruses have now been "weaponized" and are being used by states against each other. Several of Canada's allies have begun to implement cyber security strategies to protect themselves, and Canada has acknowledged it intends to do the same.

BACKGROUND:

Cyber systems – computers and the Internet – are fundamental for the effective operation of Government, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians.

Protecting the cyber systems that Canada and Canadians depend on is a new role of Government in the 21st Century, and is essential for guaranteeing Canada can maintain an innovative, prosperous economy and a secure society.

In the last year, there has been an increase in the number of cyber incidents directed against all levels of society leading to increased attention to the topic by our key allies, in particular the United States. The threats are daily and global, involving: foreign states' military and intelligence agencies, transnational cyber-criminals, and cyber terrorists looking to further military, economic and political objectives.

The interconnectedness of cyber systems means that these systems are only as strong as their weakest link. Cyber security is a shared responsibility – no single country, government, organization or individual can truly secure their networks in isolation; others must also do their part.

Recent media reports have focused on the "Stuxnet" virus, which appears to be designed to target computer systems used in the control systems of the nuclear energy industry.
Suggestions have been made it was specifically engineered to deliberately cripple the computers involved in the (alleged) Iranian nuclear weapons program. The Government of Canada has been actively involved in mitigating efforts in Canada to cleanse similar systems and ensure they remain unaffected.

Coincidentally, this week Canada, the United States and ten other countries participated in Cyber Storm III, an international exercise simulating a large-scale cyber-attack on critical infrastructure.

Canada is developing a national cyber security strategy to unify and enhance cyber security activities within government, to engage the private sector in promoting the cyber security of Canada's critical infrastructure, and to promote safety online for citizens. An announcement is expected very soon.

The United States, the United Kingdom and Australia have all developed new cyber security strategies and maintain a high interest in related Canadian activities.

CYBER SECURITY:

AN OVERVIEW OF CYBER SECURITY ISSUES AND THE STATUS OF THE GOVERNMENT OF CANADA'S EFFORTS TO DEVELOP A NATIONAL CYBER SECURITY STRATEGY.

RÉPONSE SUGGÉRÉE :

- **Le gouvernement du Canada prend la cybersécurité très au sérieux et il contribue à la protection des systèmes informatiques sur lesquels s'appuient le Canada et les Canadiens.**

- **Mon ministère dirige les efforts intergouvernementaux visant à améliorer la cyberintégrité du gouvernement, à protéger l'infrastructure numérique essentielle du Canada et à sécuriser notre économie numérique.**

- **La cybercriminalité inquiète les Canadiens. Ils veulent se protéger et protéger leurs familles ainsi que leur mode de vie en ligne, et notre gouvernement les aidera à le faire.**

- **Comme nous l'avons annoncé dans le discours du Trône, notre gouvernement est déterminé à oeuvrer de concert avec les provinces et les territoires pour mettre en oeuvre une stratégie de cybersécurité qui protégera notre infrastructure numérique.**

- **Ces efforts tireront parti des efforts déterminants déjà engagés au sein du gouvernement et ils s'appuieront sur des consultations auprès du secteur privé et de nos alliés internationaux.**

- **Cette stratégie constituera une première étape clé pour assurer la sécurité du Canada et des Canadiens à l'époque numérique.**

CONTACTS:			
Prepared by Rose Coelho, Director Cyber Policy, National Cyber Security Directorate, EMNS	Tel. no. Ph: (613) 993-9537 Cell: [redacted]	Approved by (ADM level only) Lynda Clairmont, ADM EMNS	Tel. no. Ph: (613) 990-4976 Cell: [redacted]

Branch / Agency: EMNS/Cyber

s.19(1)

MAR 16 2010

CYBER SECURITY

Supps C 2009-2010	$ N/A	p.
Main Estimates 2010-2011	$ N/A	p.

PROPOSED RESPONSE:

- **The Government of Canada takes cyber security very seriously and is doing its part to protect the cyber systems that Canada and Canadians depend on.**

- **Cyber systems – computers and the Internet – are fundamental components of the effective operation of Government, the economic prosperity of Canada, and the social and cultural vibrancy of Canadians.**

- **Cyber security is a growing challenge that is shared by governments, industry and individuals and is increasingly being recognized as a national security issue requiring attention.**

- **Public Safety Canada is leading cross-government efforts to produce a cyber security strategy to enhance the cyber integrity of government, to engage with key stakeholders to protect critical infrastructure and our economy, and to combat cyber-facilitated crime and protect Canadians online.**

- **The strategy will be based on consultations with the private sector and our international allies, and will build on significant efforts already underway in order to be feasible and prudent in the current fiscal climate.**

CYBER SECURITY

QUESTIONS AND ANSWERS:

Q1 How does Public Safety Canada address the challenge of cyber security?
A1 Public Safety Canada continues to develop and expand national and international partnerships on cyber security with industry, law enforcement agencies and other governments both domestic and international, to encourage lawful information sharing and to prevent, detect and mitigate cyber incidents.

Public Safety Canada houses the Canadian Cyber Incident Response Centre (CCIRC), which is responsible for monitoring threats and coordinating the federal response to cyber incidents. The CCIRC operates to ensure greater resiliency to cyber security risks affecting the Government of Canada and critical infrastructures. The Centre is co-located with the Government Operations Centre and is a key component of the Government's all-hazards approach to national security and the protection of critical infrastructure.

Public Safety Canada is leading cross-government efforts to produce a cyber security strategy to enhance cyber security in Canada.

Q2 What is the Government currently doing about cyber security?
A2 The Government continues to protect Canada's cyber networks, identify vulnerabilities and intrusions, and defend against malicious cyber activity. A number of Government departments, including Public Safety Canada, the Royal Canadian Mounted Police, the Communications Security Establishment Canada and the Canadian Security Intelligence Service work together to investigate, evaluate and respond to cyber threats.

The Government works closely with its allies in the United States and other international partners to better understand the cyber threat environment and to collectively mitigate cyber threats as they are identified.

The Government has taken a number of steps to enhance its own cyber integrity and to better protect Canadians from cyber crime and protect them online. In 2009, the *Policy on Government Security* was revised to clarify roles and responsibilities for cyber security. On February 22, 2010, Bill S-4, *An Act to amend the Criminal Code (identity theft and related misconduct)*, which creates new offences targeting the activities which support identity related crime, came into force. The Government continues to develop other mechanisms to give law enforcement agencies the tools that they need and to provide Canadians the protection that they expect.

Q3 How does the Government plan to address cyber security?
A3 The 2010 Speech From the Throne indicated that the Government will work with provinces, territories and the private sector to implement a cyber-security strategy to protect its digital infrastructure. The Budget 2010 commitment to develop a digital economy strategy will, among other things, contribute to improved cyber security practices by industry and consumers and will enable the ICT sector to create new products and services and accelerate the adoption of digital technologies. A strong digital economy will contribute to a more prosperous and competitive Canada. SFT quote "Working with provinces, territories and the private sector, our Government will implement a cyber-security strategy to protect our digital infrastructure."

Q4 What are the elements of the cyber security strategy?
A4 A national cyber security strategy will build upon existing efforts to: unify and enhance cyber security activities within government; deal with the prevention, detection and response to cyber crimes; and recognize that cyber security is a responsibility shared by governments, industry, the private sector, academia and individuals around the world. A national cyber security strategy will further promote ongoing efforts to increase public awareness and best practices among citizens and will be consistent with the Government's commitment to provide a high degree of protection of its own government systems.

Q5 What are the cyber risks and threats facing Canadians?
A5 Cyber security has emerged globally as a national and economic security issue requiring immediate attention, and increasingly, as a social issue affecting the daily lives of Canadians. The cyber threat can involve foreign states' military and intelligence agencies, transnational cyber-criminals, and cyber terrorists looking to further military, economic and political objectives. At a national level, the impact of cyber incidents can include: the loss of state secrets; economic disruption and the possible disruption of critical services; and consumer scams and identity theft. Cyber attacks can also pose a threat to the privacy of individuals and citizens need to take a proactive approach to cyber security by using effective cyber security tools and implementing strong cyber security practices in their homes and businesses.