

Page 1

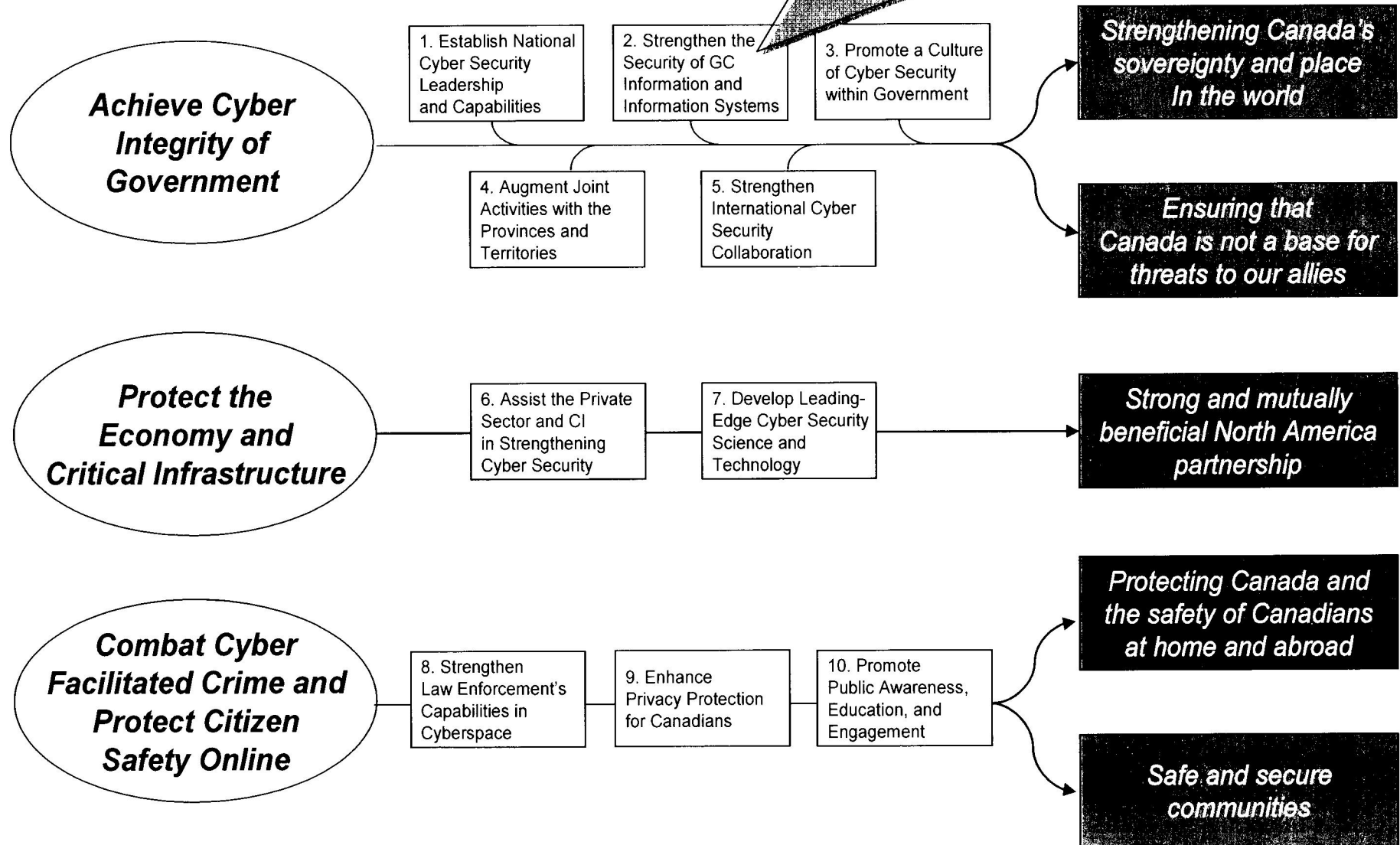
**is withheld pursuant to section
est retenue en vertu de l'article**

15(1) - Subv

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

SECRET / [REDACTED]

Context: Canada's Cyber Security Strategy



s.15(1) - Int'l

s.15(1) - Subv

s.16(2)(c)


SECRET// 

Background

- **Canadian example (spring 2008)**

- 
- 
- 
- 

- **Ad Hoc Working Group**

- 
- Membership includes: PCO, Public Safety, CSE, CSIS, Industry Canada, International Trade, TBS, PWGSC, DND
- Report back to Deputies on short and medium-term recommendations



**Pages 4 to / à 5
are withheld pursuant to sections
sont retenues en vertu des articles**

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

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

**Pages 6 to / à 7
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Subv

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

Next Steps

- Implement recommendations, subject to Deputy Minister input

- 

- 

- Within identified governance structure, provide regular updates regarding progress made against recommendations

CONFIDENTIAL
2009 02 15

Update on United States Cyber Security Initiatives

Overview

- **Comprehensive National Cybersecurity Initiative (CNCI)**
 - The 12 specific initiatives continue to evolve. These focus primarily on the federal government
 - Funding appears to be remaining intact
 - Office of Management and Budget has fenced cyber security funds
 - Melissa Hathaway, the executive within the Office of the Director of National Intelligence who led the development of CNCI, was named by the President to lead a 60 day review of cyber security plans, programs and activities across government to ensure integration and coordination with Congress and the private sector
- **Private sector report “Securing Cyberspace for the 44th Presidency” prepared by the Centre for Strategic and International Studies Commission, recommended**
 - A national cyber security strategy to encompass the CNCI and extend it beyond government
 - Elevating oversight of cyber security to the National Security Council
 - Appointment of an assistant to the President for cyberspace who would control cyber security budgets
- **A series of announcements from the Obama Administration have served to:**
 - Highlight the higher importance cyber security has in the new Administration
 - Demonstrate their apparent desire to extend current cyber security efforts beyond the federal government
 - Elevate control and accountability of cyber security efforts to the White House and National Security Council
 - Specific announcements:
 - January 21 – White House outlined the new cyber security agenda for homeland security to include strengthening federal leadership on cyber security by creating a National Cyber Advisor reporting to the President and addressing corporate espionage and cyber crime
 - January 23 – Secretary Janet Napolitano, Department of Homeland Security, asked for a review of DHS cyber security: authorities and responsibilities; relationships; programs and timeframes
 - This is one of many reviews being undertaken of DHS programs
 - DHS has been told to continue with the existing cyber initiatives
 - February 8 - National Security Adviser, James Jones announced his intention to overhaul the National Security Council to deal with

a broader set of 21st-century issues such as cybersecurity where they should be placing a far higher priority

- February 9 – President Obama directed the National Security and Homeland Security Advisors to conduct a 60-day across government review of cyber security plans, programs and activities underway throughout the government dedicated to cyber security.
 - Review will develop a strategic framework to ensure that US Government cyber security initiatives are appropriately integrated, resourced and coordinated with Congress and the private sector
 - The review appears to be addressing recommendations made in the CSIS Commission report
 - Supportive comments have been received from congressional committee chair-persons to the announcement of the review, the attention being paid to cyber security by the President and the creation of a position reporting directly to the President with responsibility for the federal cybersecurity mission
- February 12 - Dennis Blair, Director of National Intelligence, testified that item number four of emerging areas of concern is cyber security and threats to the U.S. information infrastructure posed by both state and non-state actors.

- **Overall assessment**

-
-
-



s.15(1) - Int'l

ANNEX FOR REFERENCE PURPOSES

Details

- Comprehensive National Cybersecurity Initiative – approved by President Bush in 2008
 - Results of a 2 year effort involving 23 departments and agencies lead by Melissa Hathaway, Cyber coordination Executive to the Director of National Intelligence
 - 12 specific initiatives identified, which some critics say is too focused on securing the federal government
 - Comments from US officials indicate that the Office of Management and Budget have fenced the funding to ensure allocation to continuing to counterterrorism and cyber security initiatives
 - Work on the 12 initiatives are continuing to evolve



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

- Complaints from Congress and the private sector that development and knowledge of the initiative was too secret
- “Securing Cyberspace for the 44th Presidency”, Centre for Strategic and International Studies Commission, Report of December, 2008
 - Established in August 2007, with congressional and private sector cochairs, the initiative was to identify recommendations to make a noticeable improvement in the nation’s cybersecurity
 - Major findings:
 - Cyber security is now a major national security problem for the United States
 - Decisions and actions must respect privacy and civil liberties
 - Only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure
 - Specific recommendations included
 - Create a comprehensive national security strategy for cyberspace
 - Organize for cybersecurity by appointing an assistant to the president for cyberspace, establish a Cybersecurity Directorate in the National Security Council and create a new National Office for cyberspace.
 - Rebuild partnership with the private sector
 - Develop and issue standards and guidance for securing critical cyber infrastructure, regulations for industrial control systems.

- Modernize authorities
- Build for the future through the human capital
- President Obama has indicated during briefings on cyber security that he understands the extend of the threat posed to U.S. security by cyber attacks and is committed to addressing this threat

○

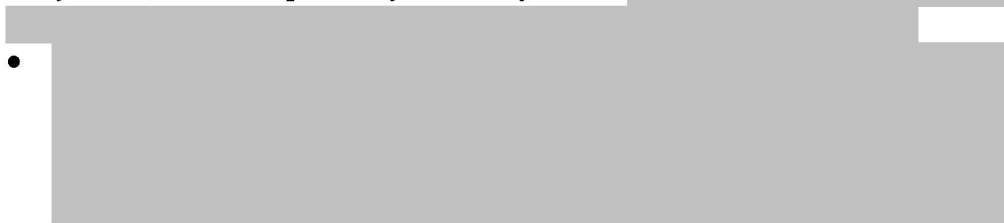



- On January 21st the White House outlined the *new cyber security agenda* for homeland security which included the following initiatives:
 - To strengthen federal leadership on cyber Security *create a National Cyber Advisor* reporting to the President
 - *Initiate R&D* to develop secure computing and next generation cyber infrastructure
 - Create new standards to *protect the IT infrastructure* that keeps America's economy safe
 - *Prevent corporate cyber-espionage* to protect trade secrets and research and development
 - *Develop cyber-crime strategy* (shutdown untraceable internet payment schemes, strengthen law enforcement)
 - Standards to *secure personal data* on government and private systems and require breach disclosure

•



- On January 23rd *DHS Secretary Janet Napolitano asked for a DHS review of cyber security: authorities and responsibilities; relationships; programs and timeframes, to be completed by February 17th* –



- On February 8th Obama's National Security Advisor, James Jones spoke about the project on National Security Reform stating that the National Security Council is evaluating how to update our capacity to combat the proliferation of weapons of mass destruction while also *placing a far higher priority on cyber security*.

- On February 9th, President Obama directed that the National Security and Homeland Security Advisors to conduct an immediate 60-day across government review (by April 8th) of cyber security plans, programs and activities underway throughout the government dedicated to cyber security. The review will develop a strategic framework to ensure that US Government cyber security initiatives are appropriately integrated, resourced and coordinated with Congress and the private sector.
 - Review to be led by Melissa Hathaway who will serve as Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils during the review period.
 - Speculation is Hathaway is on the short list along with Paul Kurtz for the post of National Cyber Advisor.
 - Comments from the Chairmen of the Senate homeland Security and Governmental Affairs Federal Financial Management Subcommittee and House Armed Services Committee and the Permanent Select Committee on Intelligence are support of the review, look forward to Congressional engagement in the review. Supportive comments include calling on the President that this critical national security issue the level of attention it deserves in order to fully protect the nation from emerging cyber threats and that a national cyber coordinator, reporting directly to the president is required to oversee a federal cybersecurity mission.
- On February 12th, the new Director of National Intelligence Director of National Intelligence Dennis C. Blair testified on the most significant global security "threats to the nation". His opening statement highlighted four emerging areas of concern:
 - The *global economic crisis* and its destabilizing impact on allies and adversaries – including the likely decreased ability of our allies to meet their defense and humanitarian obligations;
 - 2) The domestic and international impact of *global climate change*;
 - 3) Access to secure and clean *global energy* resources and management of food and water supplies, especially in light of a projected population increase of 1 billion by 2025; and
 - 4) *Cyber security and threats to the U.S. information infrastructure* posed by both state and non-state actors.

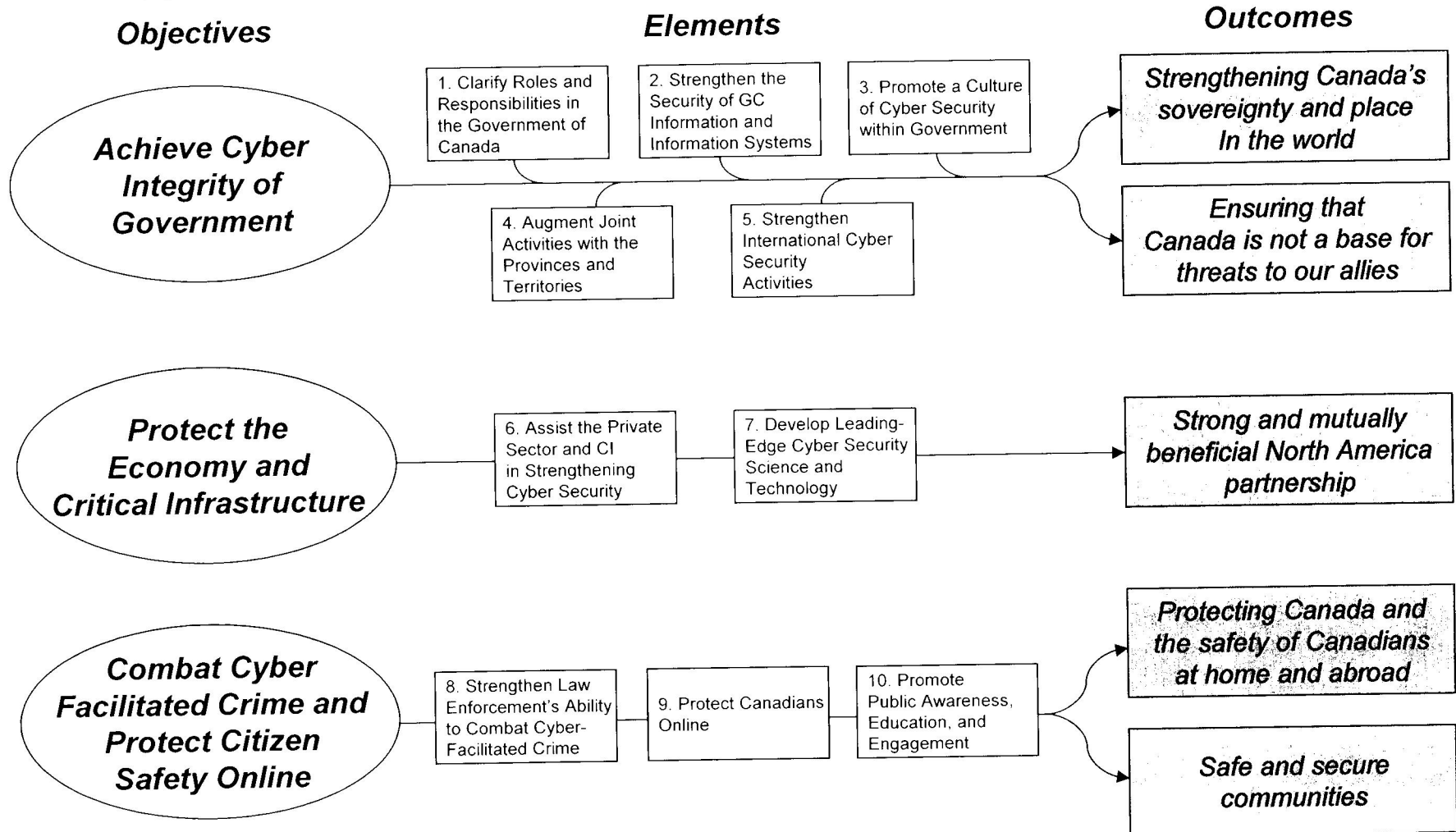
Page 14

**is withheld pursuant to sections
est retenue en vertu des articles**

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

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

Canadian Cyber Security Strategy (National)

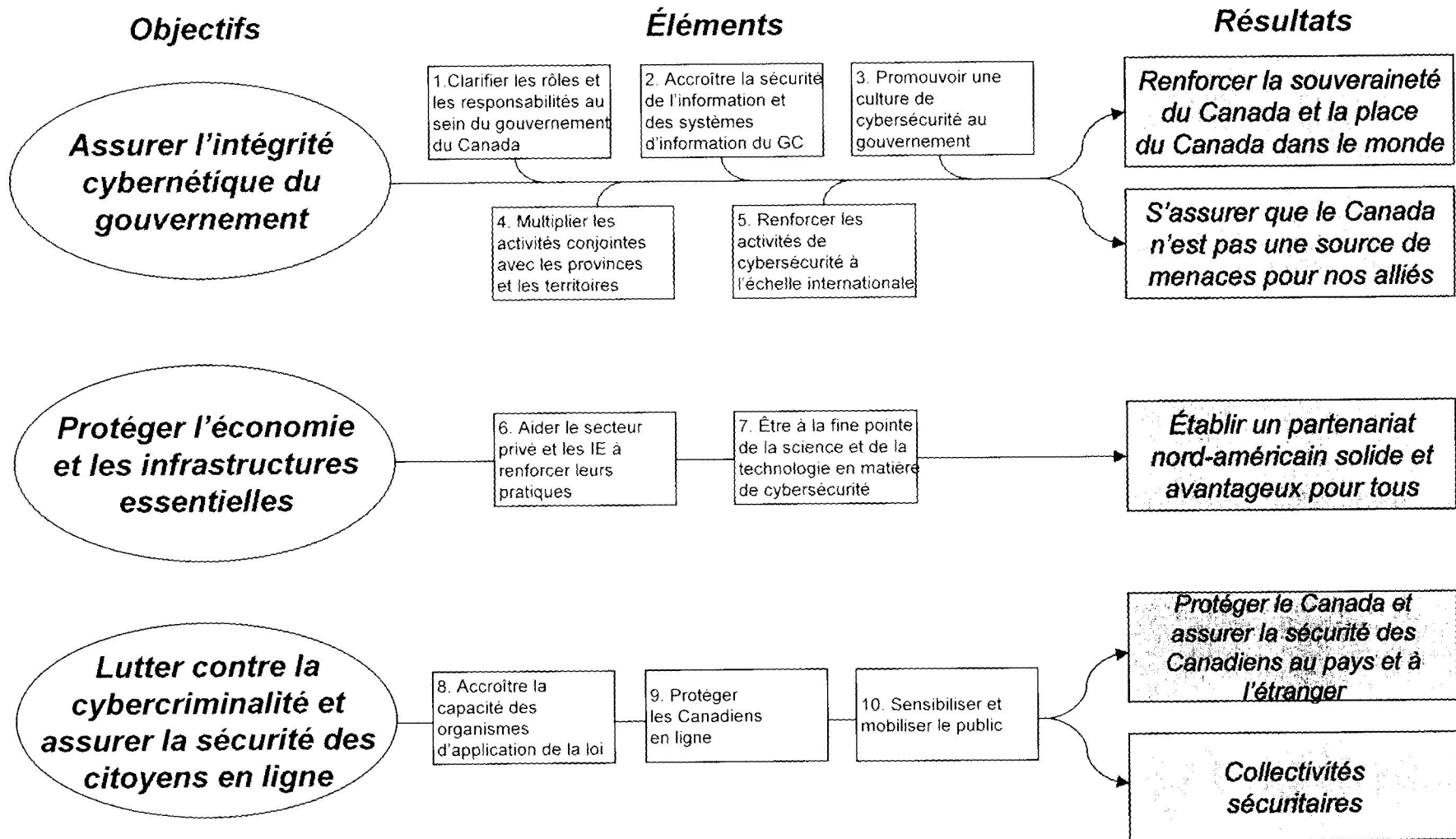


SECRET/DRAFT/ÉBAUCHE

January 16, 2009

Canada

Stratégie nationale de Cybersécurité du Canada



SECRET/DRAFT/ÉBAUCHE

16 janvier 2009

Canada



Public Safety Sécurité publique
Canada Canada

Ottawa, Canada
K1A 0P8

*Thanks.
Sec.
16/1/09*

UNCLASSIFIED

DATE:

JAN 15 2009

359406

MEMORANDUM FOR THE DEPUTY MINISTER

BOB GORDON'S SPEAKING NOTES FOR THE INTERNATIONAL SECURITY MANAGEMENT ASSOCIATION'S CONFERENCE ON CYBER SECURITY: A CANADIAN PERSPECTIVE

(Information Only)

Issue

- Please find attached, for your review and consideration, a draft speech to be delivered by Bob Gordon, Head, Cyber Security Strategy Unit, on January 21, 2009, at a conference of the International Security Management Association entitled "Cyber Security: A Canadian Perspective" (TAB A).

Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

Enclosure: (1)

DRAFT

Speaking Notes for Bob Gordon, Head, Cyber Security Strategy Unit
January 21, 2008, International Security Management Association
Cyber Security: A Canadian Perspective

I would like to begin by thanking the organizers for the opportunity to be here with you and for the chance to address this group on behalf of the Government of Canada. In particular, I would like to commend the conference organizers for having selected such a spectacular venue. Florida is a special place for a lot of Canadians. About 10% of our entire population call it home for at least part of the winter. For me, it means an escape from winter temperatures which last week in Ottawa were almost 100 °F degrees colder than it is here today.

I'm going to spend the next thirty minutes or so sketching the threat environment in which we are all now working and living, how the Canadian government has been responding to that threat and where we're going. But first I'd like to make just a few comments to provide some context.

My journey to join you today started with a pivotal point in Canada almost five years ago. In 2004, Canada announced its first National Security Policy. It articulated the core national security interests of Canada and proposed a framework for addressing the threats which we faced. Specifically, it created the department of Public Safety, to which I belong, and identified our national interest in cyber security.

The strategy outlined the threats we as a country needed to confront. Things such as terrorism; the proliferation of weapons of mass destruction; failed and failing states which contribute to spreading instability and can act as a haven for both terrorists and organized crime groups; and espionage and natural disasters. Included was recognition of the vulnerabilities in our critical infrastructure and cyberspace.

In recognition of these threats, the Government identified three enduring security interests which we, as a nation, would advance: first, the protection of Canada and the safety and security of Canadians at home and abroad; second, ensuring that Canada is not a base for threats to our allies; and third, contributing to international security.

We acknowledged that the threat of cyber attacks was real and that the consequences of such attacks could be severe. Included in the Policy was a

DRAFT

commitment to develop a National Cyber Security Strategy to reduce Canada's vulnerability to cyber attacks and cyber incidents. This leads directly to me standing in front of you today.

Public Safety is the lead portfolio within the Canadian government dealing with all matters related to public safety, including: national security; policing and law enforcement; emergency management and response; critical infrastructure protection; cyber security; border strategies; Aboriginal policing; and crime prevention. The portfolio comprises five main agencies – the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Canada Border Services Agency, the Correctional Service of Canada, and the National Parole Board. These five agencies and three review bodies have a combined budget exceeding \$9 billion and more than 63,000 employees.

The department is essentially the Canadian counterpart to the Department of Homeland Security here in the United States, and we are actively engaged with DHS on many files and projects.

The Public Safety portfolio is arguably the most complex and issue-laden in the Government of Canada. Public safety and security issues are becoming more difficult and more controversial, and the public is demanding federal leadership on a range of issues falling to the Department. This brings me directly to cyber security.

What is fascinating about cyber security is that it cuts across so many different security domains. We see security in its broadest context as having many facets, including national security, national economic security, security in the availability of critical infrastructure services, security of government as an organization, and individual security and privacy.

Cyber security affects each of these, and more than that, it ties them together. Fifty years ago, national security and personal security were very distinct topics, but now the same cyber security concerns are affecting both. That's why the cyber security challenge is both a significant threat to, and a huge opportunity for, our respective nations. Done poorly, cyber security can undermine government, business, and individual civil liberties. Done well, cyber security is a boost to your company, it helps maintain the integrity and functioning of government, it protects our critical infrastructure, and it protects us as individuals. I personally feel that cyber

DRAFT

security is one of the most strategic issues facing us today, and I'm excited to be here today to discuss it with such an influential audience.

There are three things in particular I wanted to touch on. First, I want to give you a sense of how we, in Canada, view cyber security as an issue, and of how we are characterizing the cyber threat. I expect and hope that the overall message will be very similar to what you've heard from US officials. This is a good thing. It is reassuring that our two countries concur on their analysis of the global threat picture. Having that kind of agreement greatly facilitates our joint work on cyber security. Second, I want to give you our thoughts on how government and the private sector need to engage each other on cyber security. Public/private cooperation in the areas of security and critical infrastructure protection is not a new topic. We've already learned a great deal about how best to go about it, much of which is relevant in the cyber security domain. Lastly, I want to briefly touch on what the government of Canada has done, and is doing, to address national cyber security issues.

The information age and the Internet have brought immense changes to both of our respective societies. Electronic information is now a strategic asset – almost all important information is in electronic form, and essentially all activities of government, the private sector and society depend irreversibly on access to that information and to the Internet. It is now becoming widely recognized that inadequate security of these assets is causing significant economic damage to our nations, threatening our national security and subjecting our citizens to a cyber facilitated crime wave. Hostile nation states and criminals are increasingly exploiting information systems to access information, state and industrial secrets, disrupt operations, and to make a profit. Technology allows criminals and terrorists to communicate away from the scrutiny of police and intelligence officers.

Furthermore, the rapid evolution of technology makes it extremely difficult to build systems that are reliable and secure against attacks. All sectors of our respective economies and societies – governments, private sector, not-for-profit organizations, individuals – are all being impacted. Here in North America, everything we rely on in our society – stock exchanges, financial institutions, energy infrastructures, transportation systems, border controls – would cease to function without information technology. Quite simply, governments today could not afford to deliver the services expected by

DRAFT

citizens in anyway other than via the internet. Since there is no going back to pre-computer days, there is no way to dodge the cyber threats facing us.

Those threats are as varied as the Internet itself. At one end of the spectrum, we have attacks such as web site defacements, viruses that do nothing but produce mass emails to clog up our email systems, and other forms of cyber vandalism. These threats are relatively common, but the level of sophistication is quite low. With the proper tools, threats of this nature can be mitigated to the point where their impact is minimal. Professional criminals, either acting alone or as part of an organized crime organization, work at a considerably higher level of sophistication, and have a correspondingly greater impact, through crimes such as identity theft. It has been estimated that, globally, the revenues from cyber facilitated crime have now exceeded those from the drug trade. Keeping in mind that the nature of cyber-facilitated crime makes it extremely difficult to prosecute, it is fair to assume that more and more criminals will be attracted to this area.

The upper end of professional criminal activity is the for-profit theft of sensitive corporate data and intellectual property. It is currently impossible to estimate how much damage this type of crime inflicts on our economies because there is so little reporting of incidents. What we do know is that the more we look for incidents, the more we find. This highlights the risk that poor cyber security presents for organizations that traditionally are not thought of as cyber targets. What we need to consider in the digital world is where your valuable information is available outside your normal security perimeter. Who helps you to conduct research, to prepare financial filings, to prepare patent submissions and do they share your security perspective? Your security perimeter shouldn't stop at the bounds of your organization; it should stop where your information stops. It is not difficult to imagine a scenario where the end result of years or decades of research and development is stolen electronically just prior to publication or commercialization with very little effort, and at very little risk to the thief.

At the highest levels of sophistication are the practices of foreign intelligence agencies. While the number of actors with such resources is quite small when compared to cyber criminals, there are still approximately 100 nations that possess a sophisticated cyber attack capability. These attacks are extremely difficult to detect and are used primarily for intelligence gathering, which potentially undermines our national security and for stealing intellectual property. However, there is serious concern that

DRAFT

such attacks also serve as reconnaissance for potential future attacks aimed at disabling systems. If someone can penetrate your network and exfiltrate data without your knowledge, there is no reason why they can't leave behind time-bomb programs that can be remotely activated when needed.

This situation represents a significant shift from even a few years ago. We are seeing that attacks are more frequent, sophisticated, and targeted, with the nuisance attacks fading into noise and organized criminal activity becoming more common. We must realize that even systems not considered to be sensitive may be under sustained attack by automated, undirected tools or for purposes of building a botnet. This is the case for every home computer. The definition of a "targeted" system is broader than it was only a few years ago, in that we are now seeing government, critical infrastructure, and business systems attacked for purposes of economic advantage. If you are a target, it is safe, and wise, to assume that your computers are being hit by the full gamut of these threats every single day, by multiple parties, and for a multitude of motives.

We know that foreign intelligence work is also growing, but this is very difficult to prove, as it is becoming increasingly difficult to detect. We're now seeing hardware and software products that have been compromised at the production stage, with deliberately-introduced vulnerabilities to ease attacks. This includes products such as memory sticks, digital photo frames, digital music players, and others. We're also seeing increased use of sophisticated social engineering and increased targeting of specific individuals and organizations. Overall, the trend is for attacks that are more sophisticated, more frequent, and that have more impact.

One important point to remember is that technology itself is not the problem. Information technology is neither bad nor good by itself, but rather it is an enabler and a tool. There is no question that information systems have enabled tremendous innovation in business and growth in productivity and in the global economy, and will continue to do so for the foreseeable future. Unfortunately, information technology is equally an enabler for crime and malicious use. To some extent, this is unavoidable – anything that allows two people to communicate more efficiently also allows two criminals to communicate more efficiently. But much of the threat posed by poor cyber security is a result of how we have implemented the technology, and the choices we've made in using it. These can be fixed, and more and more are being fixed, to mitigate cyber risks. In a sense, while we have adapted with

DRAFT

incredible speed to the benefits of information technology, we are lagging in our adaptation to the risks. This resulting gap has created an opportunity for criminals and adversaries to flourish, but it is a gap that can be closed.

I'd like to shift now to speaking about one of the most interesting and strategic aspects of the cyber security challenge – the relationship between the private and public sectors. I want to share with you some of what we, in the federal government, have learned over the past few years through engagement and consultations with the private sector, from our international allies, and from our own experience.

The most important thing we have learned is that cyber security is not something that can be achieved by any one party acting alone. Cyber security is a shared responsibility and requires joint action. Very few computer networks exist in isolation; a key benefit of information technology is the ability to communicate, and to do that you must interconnect your network with others. As soon as that happens, “your” network is just one piece of a much larger global network where the computer on your desk is connected to those of hackers and criminals all over the world. No matter how thick your walls or wide your moat, you can't get to the point where you can say “this cyber security thing doesn't apply to me anymore”. The problem is here to stay, and we all need to make security a part of our business.

A pointed example of this is our lack of understanding of how good or bad the situation really is. No one has visibility across the entire internet or a complete understanding of which computers are doing what. This makes it extremely difficult to usefully judge your organization's risk posture and manage your security appropriately. It complicates the role of law enforcement officials who can't get a good picture of what crimes are being perpetrated and how frequently. It makes it difficult for governments to evaluate threats to national security and to develop policies to address those threats.

A major contributor to this problem is that we don't share information with each other about what is happening. Our consultations and numerous other studies have shown that most cyber intrusions go unreported. On the whole, organizations are cautious in reporting misuse of the internet or company systems by employees or outsider data breaches due to poor security.

DRAFT

We need to address this issue head-on. There is a stigma associated with poor cyber security. Sometimes this is justified, as many losses of confidential data result from poorly configured information technology or from a lack of enforcing basic security rules. But there are also adversaries using sophisticated attacks that no current commercially tool can detect. There are hostile parties sending socially engineered emails daily to thousands of people within an organization or even across an entire sector. Statistics tell us that, with the cyber security available today, one of those emails is bound to get through and will be opened by a user. Not sharing incident information doesn't help you or anyone else, and sharing it in a trusted setting won't harm you. We need to create the right setting so that everyone involved can benefit from our collective knowledge.

We also need to work together because we purchase the same hardware and software. If you need proof that no network is an island, look at how our information technology products are produced. A single piece of equipment will contain components from many vendors, which are sold through many distributors and are produced in many different nations. Software programs are now tens or hundreds of millions of lines of code long, and many of those lines of code were produced by contractors working around the globe. There are numerous examples in the open media of equipment being faulty or deliberately compromised before it was purchased. I'm not sure what we require to address the issue of equipment compromised at source, but I do know that it will take the purchasing power and market force of us collectively, not just a single organization or government. If we don't work together on this, and on similar issues, we will each individually have to settle for stop-gap measures.

Another big change over the past few years is our understanding of the role of government in cyber security. Government does not have all the answers, but government is in a good position to make things happen. We have consistently heard from the private sector that people want government to be engaged and want government to show leadership. In areas such as promoting information sharing and working collectively, government can play the role of impartial enabler and catalyst. We have to be careful how we do this, because government can wear two hats: that of a regulator and of a partner. We need to keep those distinct; but, in the right context, government can often call a meeting or start a dialogue that others can't.

DRAFT

It was made very clear throughout all of our consultations that for any government involvement to be effective, it had to be organized and easily understood. Bluntly, we need to have our government house in order so that our approach is clear and comprehensible. Many called for a single point of contact within the Canadian government for cyber security issues, with a mandate and responsibilities that are well-publicized. It is also clear that the lead departments in each sector – Industry Canada in telecommunications, Natural Resources Canada in the energy sector, and so on – need to work with a single point of contact on cyber security. Government needs to work at bringing together its sector experts and its cyber security experts so that external partners deal with a unified front.

I should point out that, although we're focusing on cyber security today, what I've just said applies equally to critical infrastructure protection and emergency management. There is specific expertise within each government lead agency department that needs to be leveraged, but this must be done within a cohesive framework. We can't have separate information sharing mechanisms for critical infrastructure protection and for cyber security. Last spring the Canadian government released, for consultation, a draft *National Strategy and Action Plan for Critical Infrastructure*. A consistent theme in the input received is that the information sharing structure being proposed for critical infrastructure should be the same as that used for cyber security.

We have also learned a great deal about what we need to do internally to improve our own cyber security. It may seem obvious when stated, but every Canadian, every Canadian business, and every business operating in Canada will, at some point, exchange information with the federal government. And, I believe that the same holds true in your countries. Our being able to protect our citizen's information, and their dealings with the government, removes one possible route by which individual citizens, and every other entity that does business with the Government of Canada, might suffer a loss, and that is significant.

As a major user of information technology, the federal government has developed significant internal expertise and resources that we can share. When it comes to cyber security, we are a direct player in the game. When you consider the work of our lead security agencies – work that only the federal government is permitted to do under Canadian laws – it's clear that we have some highly specialized skills.

DRAFT

A final important role for government is that of interlocutor with international governments. Virtually every significant international organization of which Canada is a member – G8, NATO, OECD, APEC, OAS – is addressing the issue of cyber security. It is the role of the federal government to advance Canadian interests in those fora, and to represent the collective view of Canadians and Canadian companies.

There may also be a need for the Canadian government to engage other nations in a diplomatic setting in the context of cyber deterrence. If a nation state is turning a blind eye to, or even indirectly abetting, hostile cyber activity, it will be up to the national-level governments to engage that nation state in a dialogue and bring diplomatic pressure to bear. The protocol and diplomatic thresholds of cyber deterrence are not well understood – this is largely uncharted territory – but we believe this is something that needs to be developed in the near term.

One of the most important lessons learned that I wanted to touch on is simple – the importance of making it easier for all of us to tackle the cyber security issue. Cyber security is a tough nut to crack – we have the opportunity to better the situation enormously, but it will take a great deal of work and there are few shortcuts to take. It behoves us to do what we can to make things easier.

When it comes to sharing information, we need to make the effort to develop trust between us. We need to be sitting down, face-to-face, on a regular basis, and in a setting where we can be candid and frank. The federal government has experiences to share, and we intend to share them. There are sensitivities on both sides of the public-private debate and trust will take time to build, but we need to start the building.

A major concern has always been the ability of government to protect sensitive information that it receives. In Canada, we responded by passing the Emergency Management Act, which – among many improvements to our federal emergency management systems – amended the Access to Information Act to provide protection for critical infrastructure information shared in confidence with the government by third parties. Exemptions from disclosure, for reasons of national security and public safety, also exist under federal, provincial, and territorial legislation.

DRAFT

As I mentioned previously, the draft National Strategy and Action Plan for Critical Infrastructure sets out engagement mechanisms for industry and government to use, namely sector networks for each of the critical infrastructure sectors and a cross-sector forum to address interdependencies. Cyber security is a key element of that work. As that action plan launches this year, we will use those mechanisms to engage Canadians on cyber security issues.

More than anything, we need to take action. Even if all the details aren't worked out yet, we need to be flexible and take successes when they come – no one solution will work for everyone, no one mechanism will suit all sectors and cyber security threats will change. We will need to maintain a cohesive approach without imposing rigidity and uniformity.

We, in government, know that government doesn't have all the answers, but we are sure that some of what we know is known only to us. We need to share that with you, in the right forum and with the right protection, so that you can benefit from it. Likewise, cyber security isn't a problem that the private sector can fix on behalf of our nation, but it surely won't be fixed without the involvement of industry. Each of us has to step forward a bit to make this work, and each will benefit when we do.

With that lead-in, I want to speak now about some of the things we have done in the Canadian government and where we're going with respect to cyber security.

As with most governments and big organizations, cyber security and information security issues are nothing new and we have been actively addressing these areas for a long time. The growing recognition, in the 1990s, of the importance of critical infrastructure, and the wake-up call of Y2K, sparked numerous information security efforts across the government of Canada. It was recognized, at the time, that significant good work was already in progress in government and in industry, but there was clearly a need to take it to the next level and unify the numerous efforts. Since that time we have been advancing multiple security initiatives within government, as well as consulting with the private sector and international allies about how best to formulate an overarching strategy.

We are now at the stage where we are drafting a strategy for consideration. Our strategy development effort has two main deliverables. The first is a

DRAFT

discussion of the cyber security threat. In essence, why do leaders need to become engaged in addressing cyber security? We have an obligation to ensure decision makers have the information they need to make the right risk management judgements. The second is the go-forward strategy itself.

Effective cyber security entails securing government including putting its house in order; ensuring economic security and critical infrastructure security through engaging the private sector; and combating cyber facilitated crime and thereby protects individual citizens. We need to think about changes to government security policy and the implementation of new security technologies; collaboration with international partners, in particular the United States because of the intermeshed nature of our respective infrastructures; collaboration with various levels of government; training, education, and awareness raising, both within our own organization (that is to say, the federal government) and by other stakeholders; improved information sharing with the private sector on threats and approaches to mitigating them; a focus on new science and technology and on the educational development of a solid and sustainable cadre of cyber security experts.

I remind every audience, every consultation we have, that the strategy we propose is not intended to be a final solution to the cyber security problem in Canada; I don't believe such a thing exists. Cyber security will continue to evolve as a need and a discipline along with the evolving technology and the threat. The strategy will propose solutions for the immediate problems of today and will put in place the framework and infrastructures needed to address tomorrow's problems.

I would like to close by saying again that I see cyber security as one of the most interesting adventures. I can think of no other single domain that has the potential to so profoundly affect our national, economic, and personal security. As information technology becomes ever more integrated into the fabric of our society over the decades to come, cyber security will be a key enabler in making sure we can take advantage of the incredible and still-growing promise of information technology without becoming victims to that technology. The government of Canada is deeply committed to working with its international allies, with business and critical infrastructure sectors, and with citizens to ensure our collective cyber security practices are second to none.

DRAFT

Thank you again for the opportunity to be here.

**Pages 31 to / à 33
are withheld pursuant to sections
sont retenues en vertu des articles**

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

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

**Pages 34 to / à 37
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

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



BRIEFING NOTE
NOTE D'INFORMATION

SECRET
2009-01-20
FILE DEP-359476

DEPUTY MINISTER TRIP TO NEW ZEALAND:
CYBER SECURITY ACTIVITIES IN CANADA AND NEW ZEALAND

ISSUE

- Status of Canadian efforts to develop a National Cyber Security Strategy, and corresponding activities in New Zealand

CANADIAN CYBER SECURITY STRATEGY DEVELOPMENT

- Canada's 2004 *National Security Policy* called for a National Cyber Security Strategy and was the stimulus for multiple cyber security initiatives across government. Public Safety Canada (PS) is currently leading cross-government efforts to develop a Strategy that will unify ongoing efforts and initiate new activities required to sustain the Strategy for the long term. A draft Strategy for consideration by Deputies is planned for late winter 2009.
- The Strategy will not be a final solution to the cyber security problem. It will propose solutions for the immediate problems of today and will put in place the framework and infrastructures needed to address tomorrow's problems. s.13(1)(a)
s.15(1) - Int'l
- Each of the Five Eyes – Canada, the United States (US), the United Kingdom (UK), Australia, and New Zealand (NZ) – is currently implementing or developing new approaches to the cyber security problem.

- Canada's strategy will propose three main objectives:
 - Achieve cyber integrity of government by putting the government's house in order, establishing a national cyber security centre, and increased outreach to other nations;
 - Protect the economy and critical infrastructure through significant and expanded engagement with the private sector; and
 - Combat cyber-facilitated crime and protect citizen safety online by augmenting the cyber policing capabilities of our police authorities, amending legislation to reflect advances in technology and engaging our citizens.

NEW ZEALAND CYBER SECURITY ACTIVITIES

- In August 2008, NZ released their *Digital Strategy 2.0*, a broad strategy focused on leveraging information technology for prosperity and economic growth. The 50-page Strategy defined three outcomes – healthy environment, high-value economy, and vibrant communities and culture – and four enablers – connection, capability, confidence, and

s.13(1)(a)

s.15(1) - Int'l

SECRET

s.19(1)

content. The goal for “Confidence” (referring to cyber security) was “secure and trusted digital networks and universal understanding of online safety, security, and privacy issues”. The Strategy does not represent a cyber security strategy per se, but it does position cyber security within a broader context.

- The Government Communications Security Bureau (GCSB) is the NZ government lead for cyber security and is expected to take on a larger role with regards to national cyber security issues. GCSB is the counterpart to the CSEC [REDACTED]

- [REDACTED]

TALKING POINTS

- The Government of Canada takes the global cyber security threat very seriously. The completion of a National Cyber Security Strategy is a top priority for my department and for the government.

- Cyber security is a shared responsibility and we must work together as nations to address it. I am pleased that our respective officials have been exchanging information regularly regarding our approaches and I strongly encourage this to continue.
- To that end, I have recently created a new National Cyber Security Directorate within my department to act as the Canadian government's centre of focus on cyber security issues.

- 

s.15(1) - Int'l



Public Safety Sécurité publique
Canada Canada

Ottawa, Canada
K1A 0P8

SECRET (with attachments)

DATE:

JAN 21 2009

359278

MEMORANDUM FOR THE DEPUTY MINISTER

CYBER SECURITY DECKS

(Information)

Issue

- Enclosed, for your consideration, is the revised deck presentation for the January 28, 2009, briefing of the Minister on Cyber Security (**TAB A**). Also attached for your review is a deck on the same issue for an upcoming briefing of the National Security Advisor (**TAB B**).
- The two decks are identical except for one additional slide in the deck for the National Security Advisor which is flagged.

Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

Enclosures: (2)



Public Safety
Canada

Sécurité publique
Canada

SECRET



Cyber Security

Presentation to the National Security Advisor



Date TBD

Canada

SECRET

Issue

- Information and information systems are strategic assets for governments and the private sector.
- Securing data, systems and networks is becoming extremely difficult

-

-

-

- All sectors of economy and society – governments, private sector, not-for-profit, individuals – are impacted.

s.15(1) - Subv



Public Safety
Canada

Sécurité publique
Canada

SECRET

Cyber Security Strategy Mandate

- The National Security Policy 2004 recognized that cyber security was a major element of emergency management and established the original mandate for the Strategy
 - *Cyber-security is at the forefront of the transborder challenge to Canada's critical infrastructure... The Government will convene a high-level national task force, with public and private representation, to develop the National Cyber-security Strategy to reduce Canada's vulnerability to cyber-attacks and cyber-accidents*
- Public Safety Canada was tasked with the development of the Strategy.



Public Safety
Canada

Sécurité publique
Canada

SECRET

Context

- The Canadian economy and Canadians' quality of life are dependent on information and communication technologies (ICTs).
- Canada's key financial and economic systems cannot operate without ICTs

s.15(1) - Subv
s.16(2)(c)



Public Safety
Canada

Sécurité publique
Canada

SECRET

Context (cont'd)

- Government service delivery also dependent on ICTs
 - 130 commonly used services (e.g., tax filing, SIN and passport applications, employment insurance filing) from 34 departments and agencies are online
 - tele-health, distance education, and many services to remote communities rely upon cyber technology
 - applies to all governments
- Canadian economy relies heavily on the internet
 - Canadian online sales in 2005 were valued at \$39.2 billion
 - 82% of public sector and 48% of private sector enterprises use the internet to purchase goods and services online
 - 100% of public sector and 87% of private sector firms use the internet



SECRET


Context (cont'd)

- **Canadians have embraced the internet**
 - 58% of personal tax filings are electronic (2008 tax year)
 - 73% of Canadians 16 and older (19.2 million) went online from home in 2007
 - 46% of Canadians bank online
 - 33% of Canadians order goods or services online
 - growing dependency on tele-health and distance education services, especially in Canada's northern and remote communities



SECRET

Threat Environment

- Increasing number of cyber attacks against the government, private sector, critical infrastructure and individual Canadians – has reached a critical point.
- 
- Cyber attacks are resulting in
 - harm to the Canadian economy
 - theft of corporate intellectual property and personal information
 - disruption of delivery of critical infrastructure and business services
 - reduction of economic and negotiating advantage
 - reduction of public trust and confidence in cyber systems and Canadian institutions

s.15(1) - Subv



SECRET

Threat Environment (cont'd)

- **Criminals are showing a growing level of sophistication and technical ability and are increasingly using the internet for crime**
 - sale of stolen proprietary and government information, identity theft, child pornography, etc., are all highly profitable and low risk for criminals
 - cyber crimes are estimated by U.S. officials to have exceeded drug trafficking revenues globally
 - Internet provides a fast and secure means for criminals and terrorists to communicate and conduct business while evading law enforcement
 - theft of confidential data from Canadian businesses due to cyber attacks has doubled in 2 years
 - 86% of large Canadian organizations have experienced cyber attacks
 - estimated annual cost to Canada of identity theft alone is \$2 billion
 - in 2007, the Canadian Anti-Fraud Call Centre reported 10,366 complaints from identity theft and identity fraud victims



SECRET

Threat Environment (cont'd)

- State-sponsored cyber espionage is being conducted against Canadian government and Canadian private sector

-



- Increased risk that equipment purchased from untrustworthy sources has been altered to facilitate cyber attacks.
- Inter-connected nature of networks means that cyber security is vulnerable to the weakest link in the chain.

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



SECRET

Considerations

- Over one-fifth of the human population is online – by 2015 there will be more internet-connected devices than people on the planet.
- Cyber security has been identified by the U.S., U.K., and Australian governments as a top priority – Canada must keep pace.
- Cyber security is a serious problem that requires a collective response.
- Cyber security must be pursued multilaterally – key international fora (G8, APEC, OECD, NATO, etc.) have identified cyber security as an important issue.



SECRET

Considerations (cont'd)

- 2005 Auditor General Report: “We are concerned that, in many departments and agencies, senior management is not aware of the IT security risks and does not understand how breaches of IT security could affect operations and the credibility of the government.”
- 2008 Privacy Commissioner: “2007 was a year of data privacy disasters, highlighting the need for companies to recognize the value of personal information and take more care in securing it.”



SECRET

International Allies

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

United States (U.S.)

- In 2008, the President of the U.S. approved a "Comprehensive National Cybersecurity Initiative" and Congress has earmarked an additional \$14 billion annually in funding.
- The inter-connected nature of our economies and critical infrastructure demands that Canada not be a vulnerability.

United Kingdom (U.K.)

- [REDACTED]
- [REDACTED]

Australia

- In December 2008, the Australian government issued its first National Security Statement which identified cyber security as one of 10 key new priorities.
- [REDACTED]



SECRET

Progress to date

- Public Safety is leading inter-departmental efforts to develop a National Cyber Security Strategy.
- Work completed or underway includes
 - assessment of state of readiness in Canada's ten critical infrastructure sectors
 - development of a business case model for use by private sector to justify increased investment in cyber security
 - development of options for a made-in-Canada approach to information exchange between the government and the private sector
 - consultations and workshops with key private and public sector stakeholders
 - U.S., U.K., and Australian officials have been briefed on Canadian activities [REDACTED]

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



Public Safety
Canada

Sécurité publique
Canada

SECRET

Elements of a Cyber Security Strategy

Key elements of a cyber security strategy would include

1. Achieving cyber integrity of the federal government by
 - strengthening the security of Government of Canada information systems by updating policies and standards, expanding secure communications capabilities, enhancing security in procurement, and coordinating research and development
 - identifying federal leadership for national cyber security coordination
 - ensuring that organizations clearly understand their cyber incident response roles and responsibilities so that response actions are as rapid and well-coordinated as possible
 - educating government employees about cyber security matters
 - initiating increased cyber security collaboration with provincial and territorial governments at policy and operational levels
 - strengthening international collaboration in cyber security



SECRET

Elements of a Cyber Security Strategy (cont'd)

2. Protecting the economy and critical infrastructure by
 - assisting the private sector and critical infrastructure sectors to strengthen their cyber security practices by sharing cyber intelligence, inviting participation in cyber exercises, promoting the use of standards and certifications, etc.
 - developing leading-edge cyber security science and technology by encouraging collaborative academic, private sector and government research and development

3. Combating cyber-facilitated crime and protecting citizen safety online by
 - strengthening law enforcement's abilities to fight cyber crime, including legislation to provide for lawful access
 - promoting public awareness, education, and citizen engagement
 - enhancing privacy protections for Canadians by requiring data breach reporting



SECRET

Moving Forward

- Public Safety is coordinating a whole-of-government effort to develop a cyber security strategy.
- A first draft of the Strategy is expected to be completed in Spring 2009.
- Legislative changes are being identified and resource requirements are being assessed.
- The Strategy will provide a framework for enabling Canada to
 - adapt proactively to the dynamically evolving cyber environment
 - be a credible and trusted partner to our allies in dealing with cyber security matters
 - enhance the safety, security and prosperity of Canada and Canadians





Public Safety
Canada

Sécurité publique
Canada

SECRET



Cyber Security

Presentation to the Minister of Public Safety



January 28, 2009

Canada

SECRET

Issue

- Information and information systems are strategic assets for governments and the private sector.
- Securing data, systems and networks is becoming extremely difficult

s.15(1) - Subv



- All sectors of economy and society – governments, private sector, not-for-profit, individuals – are impacted.



SECRET

Context

- The Canadian economy and Canadians' quality of life are dependent on information and communication technologies (ICTs).
- Canada's key financial and economic systems cannot operate without ICTs

s.15(1) - Subv
s.16(2)(c)



SECRET

Context (cont'd)

- Government service delivery also dependent on ICTs
 - 130 commonly used services (e.g., tax filing, SIN and passport applications, employment insurance filing) from 34 departments and agencies are online
 - tele-health, distance education, and many services to remote communities rely upon cyber technology
 - applies to all governments
- Canadian economy relies heavily on the internet
 - Canadian online sales in 2005 were valued at \$39.2 billion
 - 82% of public sector and 48% of private sector enterprises use the internet to purchase goods and services online
 - 100% of public sector and 87% of private sector firms use the internet



SECRET

Context (cont'd)

- **Canadians have embraced the internet**
 - 58% of personal tax filings are electronic (2008 tax year)
 - 73% of Canadians 16 and older (19.2 million) went online from home in 2007
 - 46% of Canadians bank online
 - 33% of Canadians order goods or services online
 - growing dependency on tele-health and distance education services, especially in Canada's northern and remote communities




Public Safety
Canada

Sécurité publique
Canada

SECRET

Threat Environment

- Increasing number of cyber attacks against the government, private sector, critical infrastructure and individual Canadians – has reached a critical point.
- 
- Cyber attacks are resulting in
 - harm to the Canadian economy
 - theft of corporate intellectual property and personal information
 - disruption of delivery of critical infrastructure and business services
 - reduction of economic and negotiating advantage
 - reduction of public trust and confidence in cyber systems and Canadian institutions

s.15(1) - Subv



SECRET

Threat Environment (cont'd)

- **Criminals are showing a growing level of sophistication and technical ability and are increasingly using the internet for crime**
 - sale of stolen proprietary and government information, identity theft, child pornography, etc., are all highly profitable and low risk for criminals
 - cyber crimes are estimated by U.S. officials to have exceeded drug trafficking revenues globally
 - Internet provides a fast and secure means for criminals and terrorists to communicate and conduct business while evading law enforcement
 - theft of confidential data from Canadian businesses due to cyber attacks has doubled in 2 years
 - 86% of large Canadian organizations have experienced cyber attacks
 - estimated annual cost to Canada of identity theft alone is \$2 billion
 - in 2007, the Canadian Anti-Fraud Call Centre reported 10,366 complaints from identity theft and identity fraud victims



SECRET

Threat Environment (cont'd)

- State-sponsored cyber espionage is being conducted against Canadian government and Canadian private sector

-

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

- Increased risk that equipment purchased from untrustworthy sources has been altered to facilitate cyber attacks.
- Inter-connected nature of networks means that cyber security is vulnerable to the weakest link in the chain.



SECRET

Considerations

- Over one-fifth of the human population is online – by 2015 there will be more internet-connected devices than people on the planet.
- Cyber security has been identified by the U.S., U.K., and Australian governments as a top priority – Canada must keep pace.
- Cyber security is a serious problem that requires a collective response.
- Cyber security must be pursued multilaterally – key international fora (G8, APEC, OECD, NATO, etc.) have identified cyber security as an important issue.



SECRET

Considerations (cont'd)

- 2005 Auditor General Report: “We are concerned that, in many departments and agencies, senior management is not aware of the IT security risks and does not understand how breaches of IT security could affect operations and the credibility of the government.”
- 2008 Privacy Commissioner: “2007 was a year of data privacy disasters, highlighting the need for companies to recognize the value of personal information and take more care in securing it.”



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

SECRET



International Allies

United States (U.S.)

- In 2008, the President of the U.S. approved a “Comprehensive National Cybersecurity Initiative” and Congress has earmarked an additional \$14 billion annually in funding.
- The inter-connected nature of our economies and critical infrastructure demands that Canada not be a vulnerability.

United Kingdom (U.K.)

- 
- 

Australia

- In December 2008, the Australian government issued its first National Security Statement which identified cyber security as one of 10 key new priorities.
- 



Progress to date

- Public Safety is leading inter-departmental efforts to develop a National Cyber Security Strategy.
- Work completed or underway includes
 - assessment of state of readiness in Canada's ten critical infrastructure sectors
 - development of a business case model for use by private sector to justify increased investment in cyber security
 - development of options for a made-in-Canada approach to information exchange between the government and the private sector
 - consultations and workshops with key private and public sector stakeholders
 - U.S., U.K., and Australian officials have been briefed on Canadian activities [REDACTED]



SECRET

Elements of a Cyber Security Strategy

Key elements of a cyber security strategy would include

1. Achieving cyber integrity of the federal government by
 - strengthening the security of Government of Canada information systems by updating policies and standards, expanding secure communications capabilities, enhancing security in procurement, and coordinating research and development
 - identifying federal leadership for national cyber security coordination
 - ensuring that organizations clearly understand their cyber incident response roles and responsibilities so that response actions are as rapid and well-coordinated as possible
 - educating government employees about cyber security matters
 - initiating increased cyber security collaboration with provincial and territorial governments at policy and operational levels
 - strengthening international collaboration in cyber security



SECRET

Elements of a Cyber Security Strategy (cont'd)

2. Protecting the economy and critical infrastructure by
 - assisting the private sector and critical infrastructure sectors to strengthen their cyber security practices by sharing cyber intelligence, inviting participation in cyber exercises, promoting the use of standards and certifications, etc.
 - developing leading-edge cyber security science and technology by encouraging collaborative academic, private sector and government research and development

3. Combating cyber-facilitated crime and protecting citizen safety online by
 - strengthening law enforcement's abilities to fight cyber crime, including legislation to provide for lawful access
 - promoting public awareness, education, and citizen engagement
 - enhancing privacy protections for Canadians by requiring data breach reporting



SECRET

Moving Forward

- Public Safety is coordinating a whole-of-government effort to develop a cyber security strategy.
- A first draft of the Strategy is expected to be completed in Spring 2009.
- Legislative changes are being identified and resource requirements are being assessed.
- The Strategy will provide a framework for enabling Canada to
 - adapt proactively to the dynamically evolving cyber environment
 - be a credible and trusted partner to our allies in dealing with cyber security matters
 - enhance the safety, security and prosperity of Canada and Canadians





**Public Safety
Canada**

**Sécurité publique
Canada**

SECRET



Cyber Security

**Presentation to the Minister of Public Safety
January 28, 2009**

Canada

SECRET

Issue

- Information and information systems are strategic assets for governments and the private sector.
- Securing data, systems and networks is becoming extremely difficult

s.15(1) - Subv

- All sectors of economy and society – governments, private sector, not-for-profit, individuals – are impacted.

SECRET

Context

- The Canadian economy and Canadians' quality of life are dependent on information and communication technologies (ICTs).
- Canada's key financial and economic systems cannot operate without ICTs



s.15(1) - Subv
s.16(2)(c)

SECRET

Context (cont'd)

- Government service delivery also dependent on ICTs
 - 130 commonly used services (e.g., tax filing, SIN and passport applications, employment insurance filing) from 34 departments and agencies are online
 - tele-health, distance education, and many services to remote communities rely upon cyber technology
 - applies to all governments

- Canadian economy relies heavily on the internet
 - Canadian online sales in 2005 were valued at \$39.2 billion
 - 82% of public sector and 48% of private sector enterprises use the internet to purchase goods and services online
 - 100% of public sector and 87% of private sector firms use the internet

SECRET

Context (cont'd)

- Canadians have embraced the internet
 - 58% of personal tax filings are electronic (2008 tax year)
 - 73% of Canadians 16 and older (19.2 million) went online from home in 2007
 - 46% of Canadians bank online
 - 33% of Canadians order goods or services online
 - growing dependency on tele-health and distance education services, especially in Canada's northern and remote communities

SECRET

Threat Environment

- Increasing number of cyber attacks against the government, private sector, critical infrastructure and individual Canadians – has reached a critical point.

■



s.15(1) - Subv

- Cyber attacks are resulting in
 - harm to the Canadian economy
 - theft of corporate intellectual property and personal information
 - disruption of delivery of critical infrastructure and business services
 - reduction of economic and negotiating advantage
 - reduction of public trust and confidence in cyber systems and Canadian institutions

SECRET

Threat Environment (cont'd)

- Criminals are showing a growing level of sophistication and technical ability and are increasingly using the internet for crime
 - sale of stolen proprietary and government information, identity theft, child pornography, etc., are all highly profitable and low risk for criminals
 - cyber crimes are estimated by U.S. officials to have exceeded drug trafficking revenues globally
 - Internet provides a fast and secure means for criminals and terrorists to communicate and conduct business while evading law enforcement
 - theft of confidential data from Canadian businesses due to cyber attacks has doubled in 2 years
 - 86% of large Canadian organizations have experienced cyber attacks
 - estimated annual cost to Canada of identity theft alone is \$2 billion
 - in 2007, the Canadian Anti-Fraud Call Centre reported 10,366 complaints from identity theft and identity fraud victims

SECRET

Threat Environment (cont'd)

- State-sponsored cyber espionage is being conducted against Canadian government and Canadian private sector

■



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

- Increased risk that equipment purchased from untrustworthy sources has been altered to facilitate cyber attacks.
- Inter-connected nature of networks means that cyber security is vulnerable to the weakest link in the chain.

SECRET

Considerations

- Over one-fifth of the human population is online – by 2015 there will be more internet-connected devices than people on the planet.
- Cyber security has been identified by the U.S., U.K., and Australian governments as a top priority – Canada must keep pace.
- Cyber security is a serious problem that requires a collective response.
- Cyber security must be pursued multilaterally – key international fora (G8, APEC, OECD, NATO, etc.) have identified cyber security as an important issue.

SECRET

Considerations (cont'd)

- 2005 Auditor General Report: “We are concerned that, in many departments and agencies, senior management is not aware of the IT security risks and does not understand how breaches of IT security could affect operations and the credibility of the government.”
- 2008 Privacy Commissioner: “2007 was a year of data privacy disasters, highlighting the need for companies to recognize the value of personal information and take more care in securing it.”

SECRET

International Allies

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

United States (U.S.)

- In 2008, the President of the U.S. approved a “Comprehensive National Cybersecurity Initiative” and Congress has earmarked an additional \$14 billion annually in funding.
- The inter-connected nature of our economies and critical infrastructure demands that Canada not be a vulnerability.

United Kingdom (U.K.)

- [REDACTED]
- [REDACTED]

Australia

- In December 2008, the Australian government issued its first National Security Statement which identified cyber security as one of 10 key new priorities.
- [REDACTED]

SECRET

Progress to date

- Public Safety is leading inter-departmental efforts to develop a National Cyber Security Strategy.
- Work completed or underway includes
 - assessment of state of readiness in Canada's ten critical infrastructure sectors
 - development of a business case model for use by private sector to justify increased investment in cyber security
 - development of options for a made-in-Canada approach to information exchange between the government and the private sector
 - consultations and workshops with key private and public sector stakeholders
 - U.S., U.K., and Australian officials have been briefed on Canadian activities [REDACTED]

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

SECRET

Elements of a Cyber Security Strategy

Key elements of a cyber security strategy would include

1. Achieving cyber integrity of the federal government by
 - strengthening the security of Government of Canada information systems by updating policies and standards, expanding secure communications capabilities, enhancing security in procurement, and coordinating research and development
 - identifying federal leadership for national cyber security coordination
 - ensuring that organizations clearly understand their cyber incident response roles and responsibilities so that response actions are as rapid and well-coordinated as possible
 - educating government employees about cyber security matters
 - initiating increased cyber security collaboration with provincial and territorial governments at policy and operational levels
 - strengthening international collaboration in cyber security

SECRET

Elements of a Cyber Security Strategy (cont'd)

2. Protecting the economy and critical infrastructure by

- assisting the private sector and critical infrastructure sectors to strengthen their cyber security practices by sharing cyber intelligence, inviting participation in cyber exercises, promoting the use of standards and certifications, etc.
- developing leading-edge cyber security science and technology by encouraging collaborative academic, private sector and government research and development

3. Combating cyber-facilitated crime and protecting citizen safety online by

- strengthening law enforcement's abilities to fight cyber crime, including legislation to provide for lawful access
- promoting public awareness, education, and citizen engagement
- enhancing privacy protections for Canadians by requiring data breach reporting

SECRET

Moving Forward

- Public Safety is coordinating a whole-of-government effort to develop a cyber security strategy.
- A first draft of the Strategy is expected to be completed in Spring 2009.
- Legislative changes are being identified and resource requirements are being assessed.
- The Strategy will provide a framework for enabling Canada to
 - adapt proactively to the dynamically evolving cyber environment
 - be a credible and trusted partner to our allies in dealing with cyber security matters
 - enhance the safety, security and prosperity of Canada and Canadians



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Enhancing Government Security

Treasury Board Policy Advisory Committee
2009-01-30

Peter Bruce
A/CIO for the Government of Canada
Pierre Boucher
Executive Director
Security and Identity Management

Canada



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Part 1 - Evolution of IT Security Proactive Defense Strategy

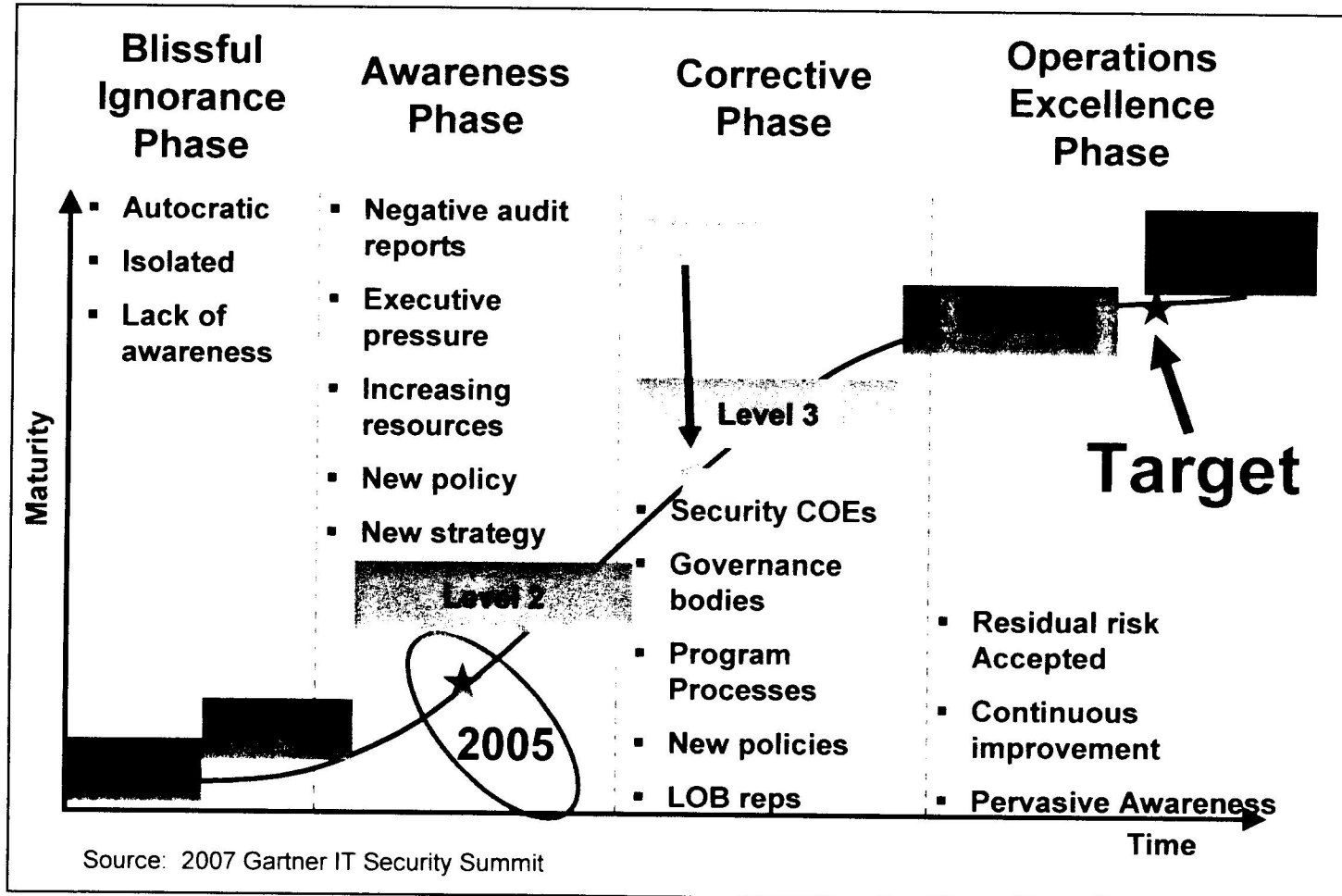
Canada

Purpose

- Highlight progress on IT Security
- Inform on:
 - IT Incident Management Plan
 - Proactive Defense Proposal
 - Consolidation of Internet Access Points
- Identify next steps

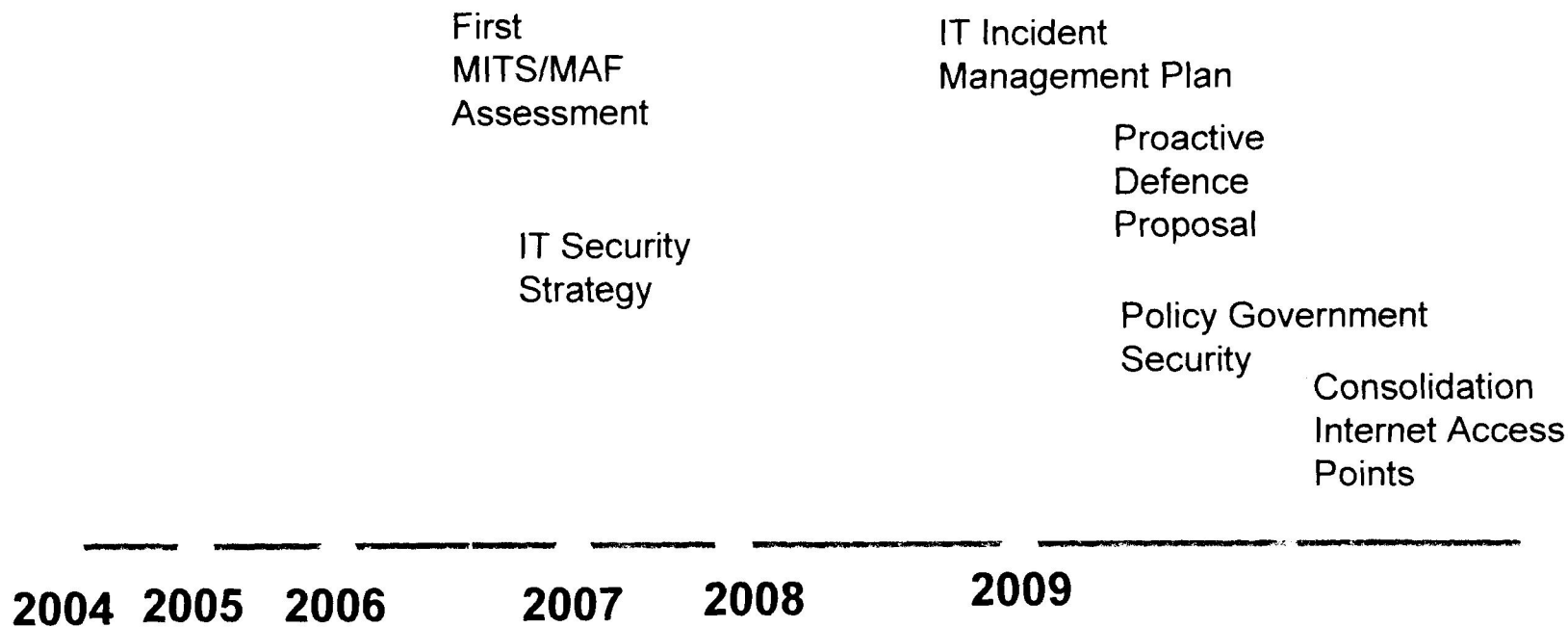


What is the target GC Enterprise IT Security Program?



GC Context

National Security Policy



OAG Audits and PAC highlight major IT Security deficiencies



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

GC Enterprise IT Security Program

To reduce risks to Canadians and GC programs and services

Horizontal Management & Planning

- “Acting as One”
- Strategic Plan
- Governance
- Accountability
- Performance Measurement

Collaborative Framework

- Efficient Toolsets
- Guidelines and tools
- Shared Services
- Common Procurement
- Enterprise Security Architecture

Build Community

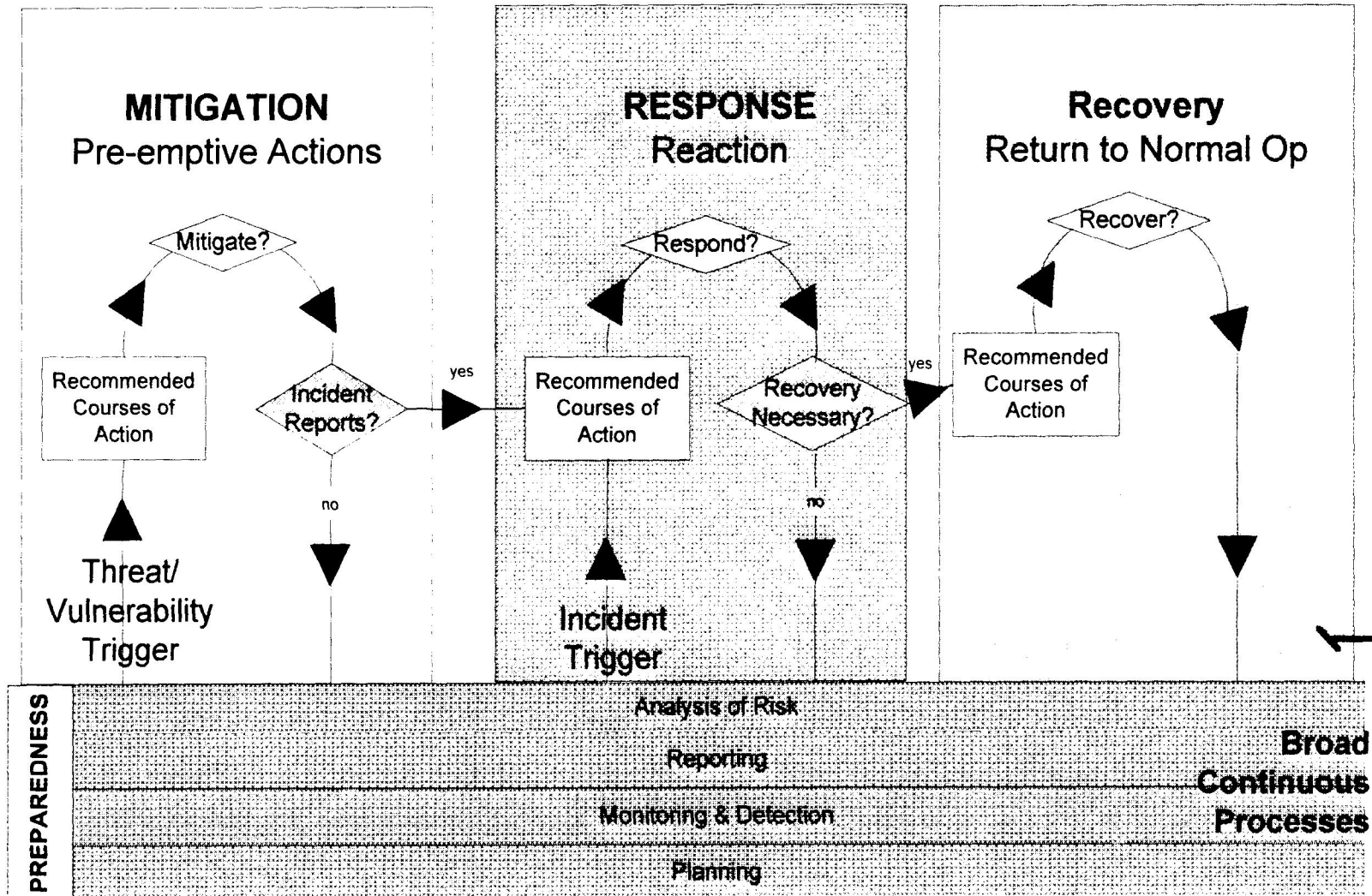
- Skilled Resources
- ITS Training & Awareness
- Community of Practice
- Pool of Skills
- ITS Portal

ITS Operational Services

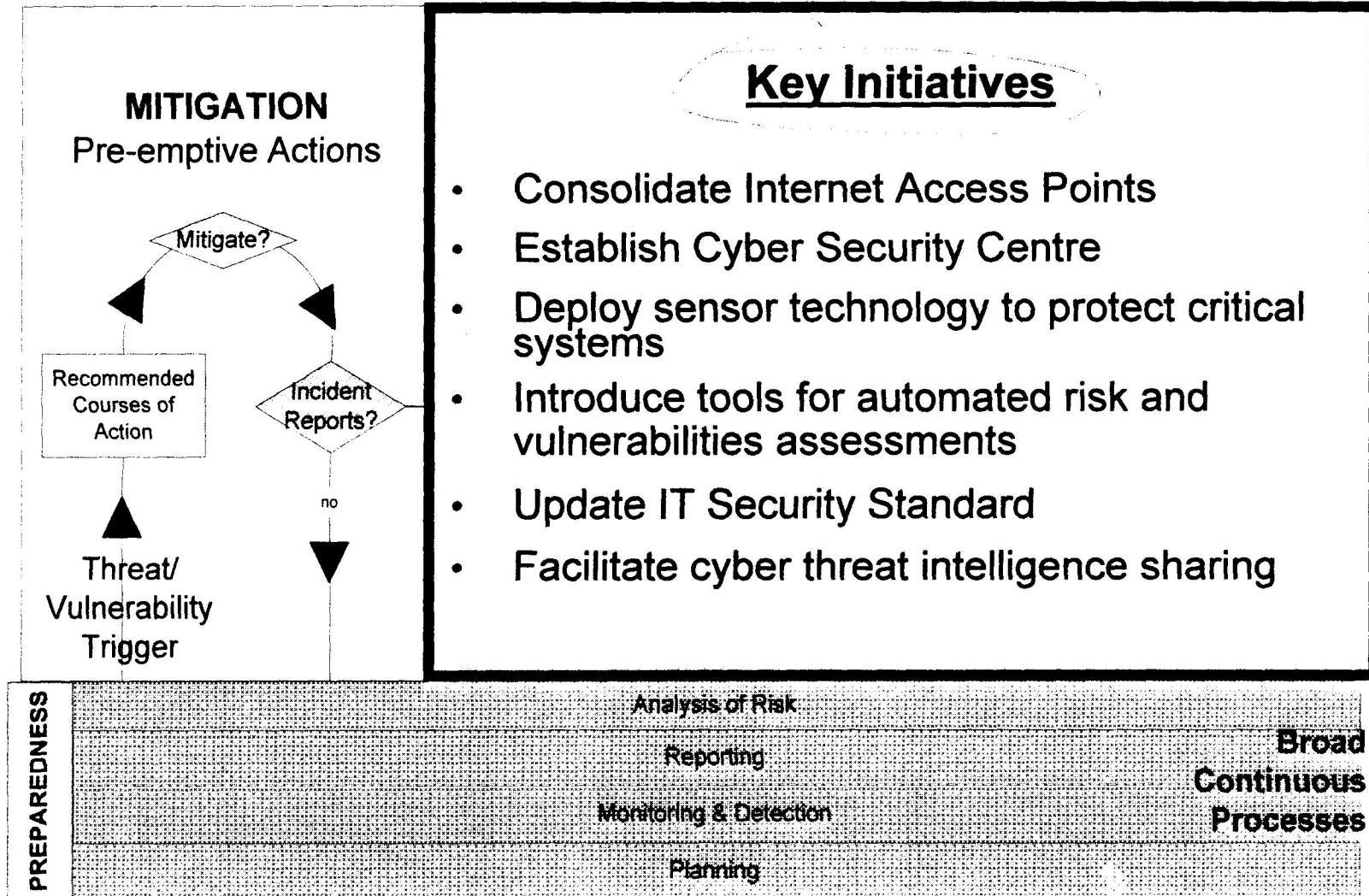
- Effective Actions
- Critical Systems
- Threat Risk Assessment
- Vulnerability Assessment
- Incident Mgt
- Monitor & Report



GC IT IMP – Operational Model



Proactive Defence strengthens the IMP



Allies Approach to Cyber Security

Initial focus is on the federal public sector.

United States

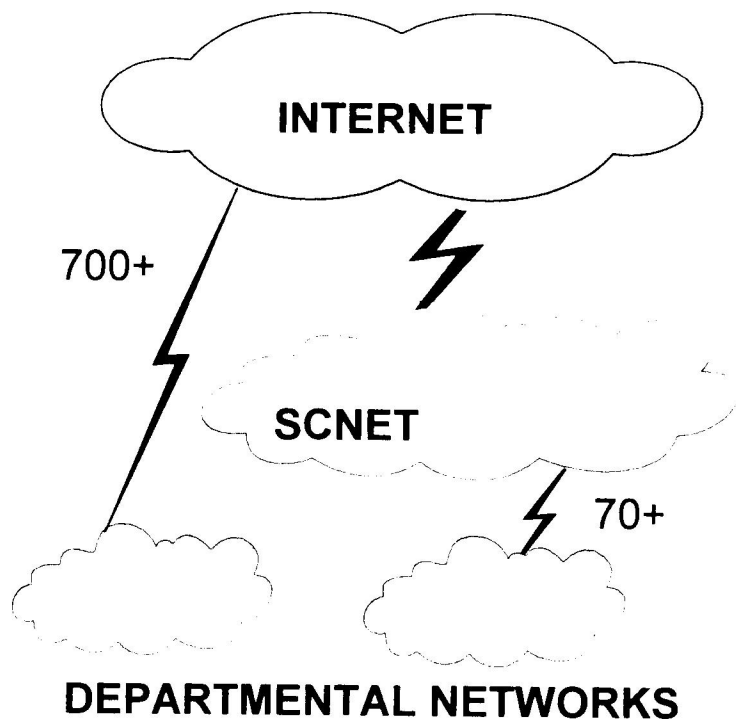
- \$14B committed to *Comprehensive National Cybersecurity Initiative* (CNCI) which includes building situational awareness and hardening of security controls
- Remains national priority with President-Elect
- Looking to Canada as a strategic partner

Australia and United Kingdom in process of finalizing cyber security strategies.

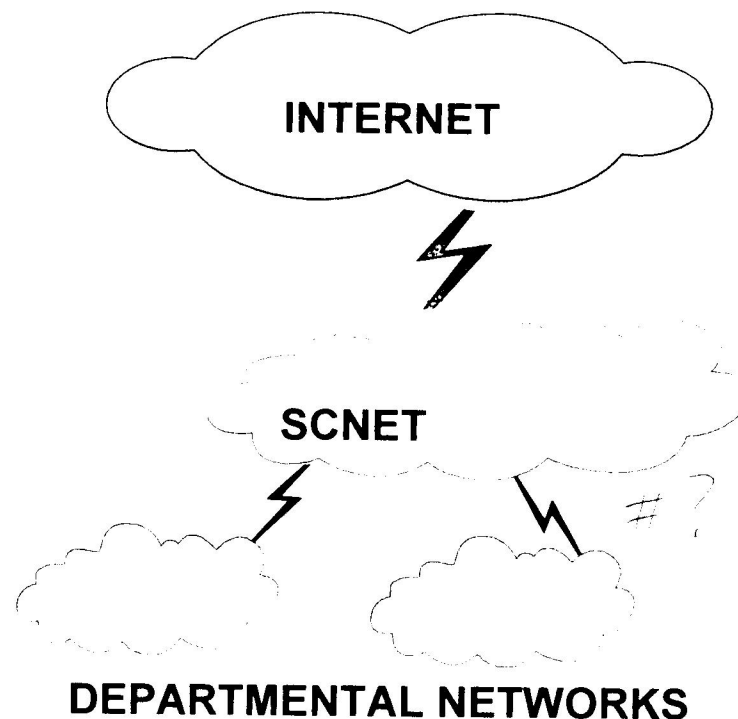


Consolidation of Internet Access Points

From this ..



To this ..



Next Steps

- ✓ Submission of GC Proactive Defense components to PS under National Cyber Security Initiative
- ✓ Update Policy Instruments
- ✓ Testing of Incident Management Plan
- ✓ Final report on Consolidation of Internet Access Points initiative March 2009
- ✓ Support departments and agencies in development of implementation approaches and plans





Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Part 2 - Policy Suite Renewal Policy on Government Security and Directives

Purpose

- To update on the evolution of threats to GC operations
- To provide an overview revised Policy on Government Security and related activities



Drivers for Change

Evolving threat environment

...

Increased incidents of identity theft and financial losses ...

Results of 2007-08 MAF assessments ...

TBS Policy Suite Renewal ...

Increased visibility and scrutiny by OAG, PAC, media ...

What's Changed

... Departmental and GC-wide governance enables collaboration and coordination

... Identity management as foundation for trust

... Departmental Security Plan integrates corporate security with departmental priorities

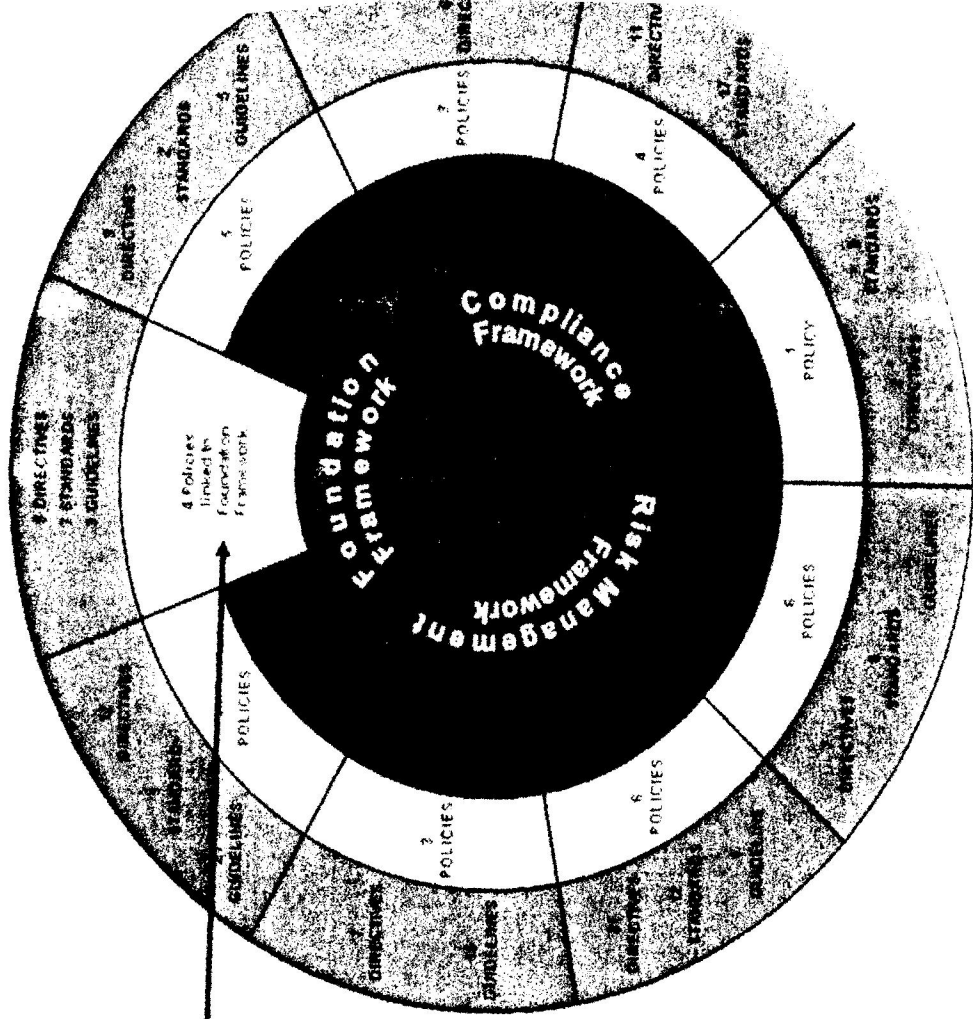
... Four principles of accountability

... Roles, responsibilities, and accountabilities clarified



Renewed TB Policy Suite

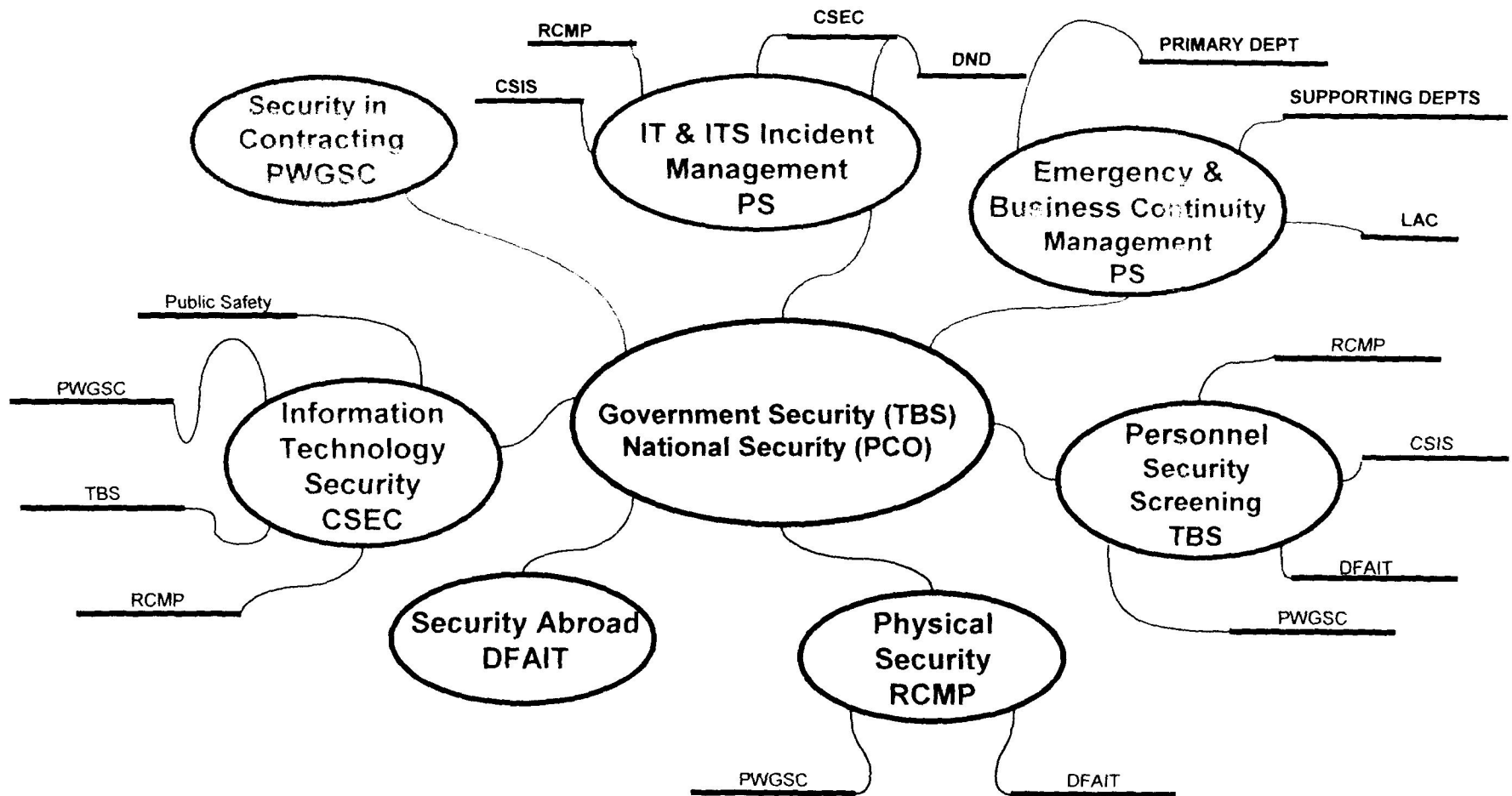
The Policy on Government Security is a foundation policy



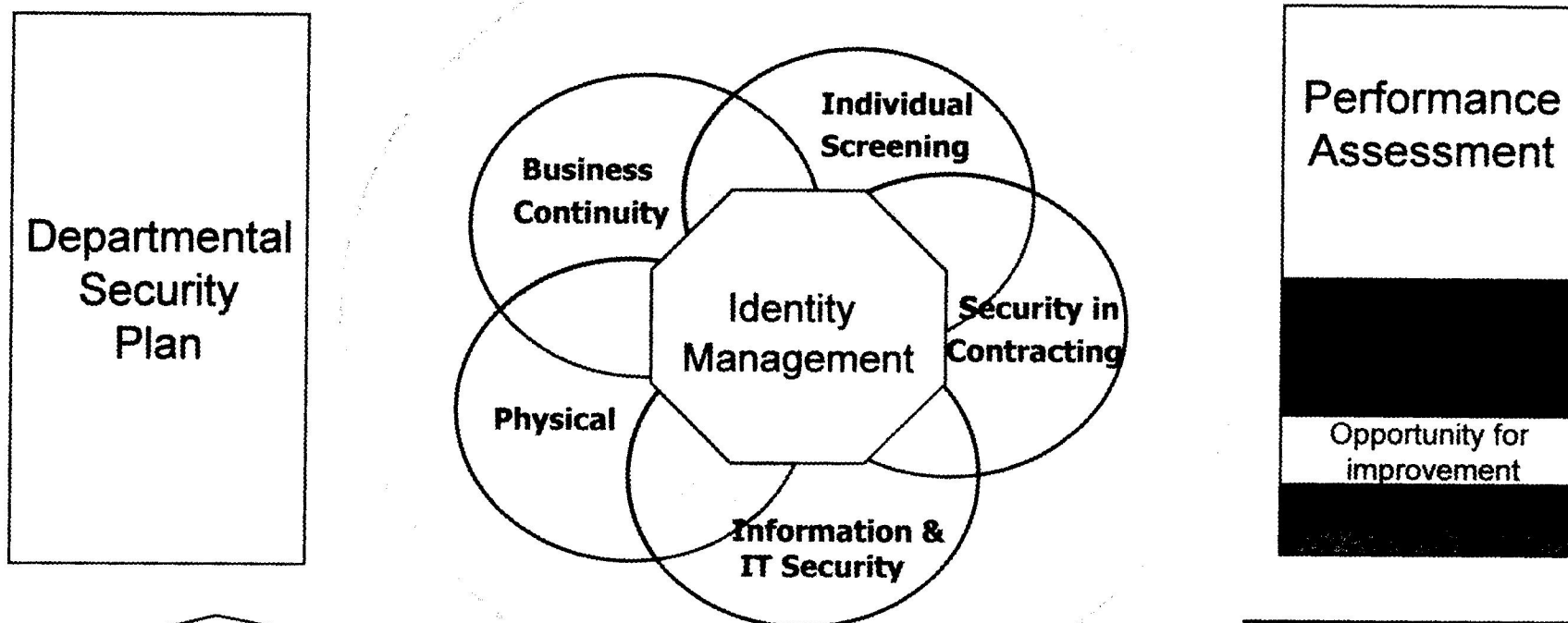
FROM: 16	TO: 9
2 Policies	1 Policy
0 Directives	2 Directives
14 Standards	6 Standards

via Secrétaire du Conseil du Trésor du Canada

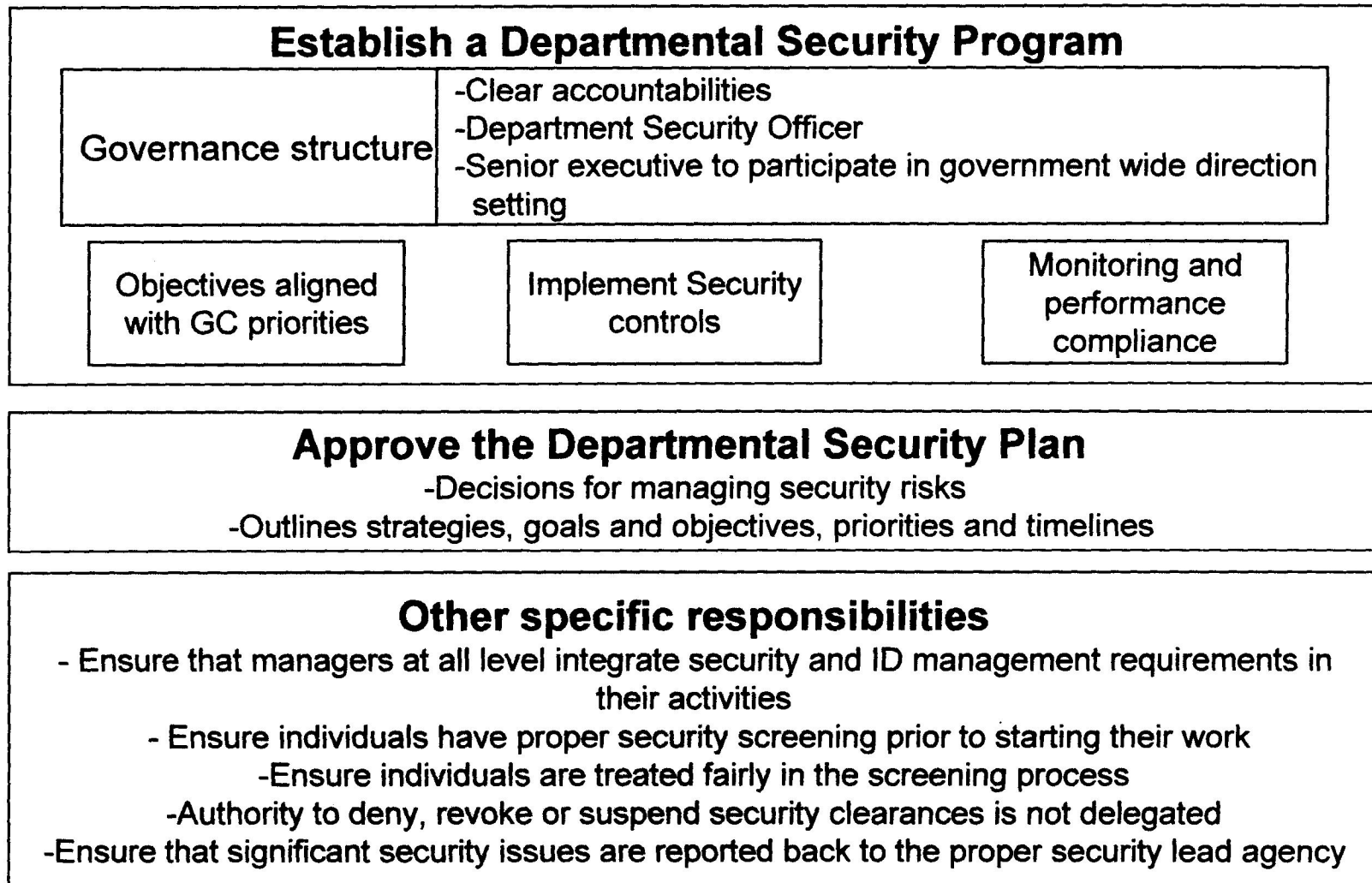
Leadership and Support of GC-Wide Security Policy and Operations



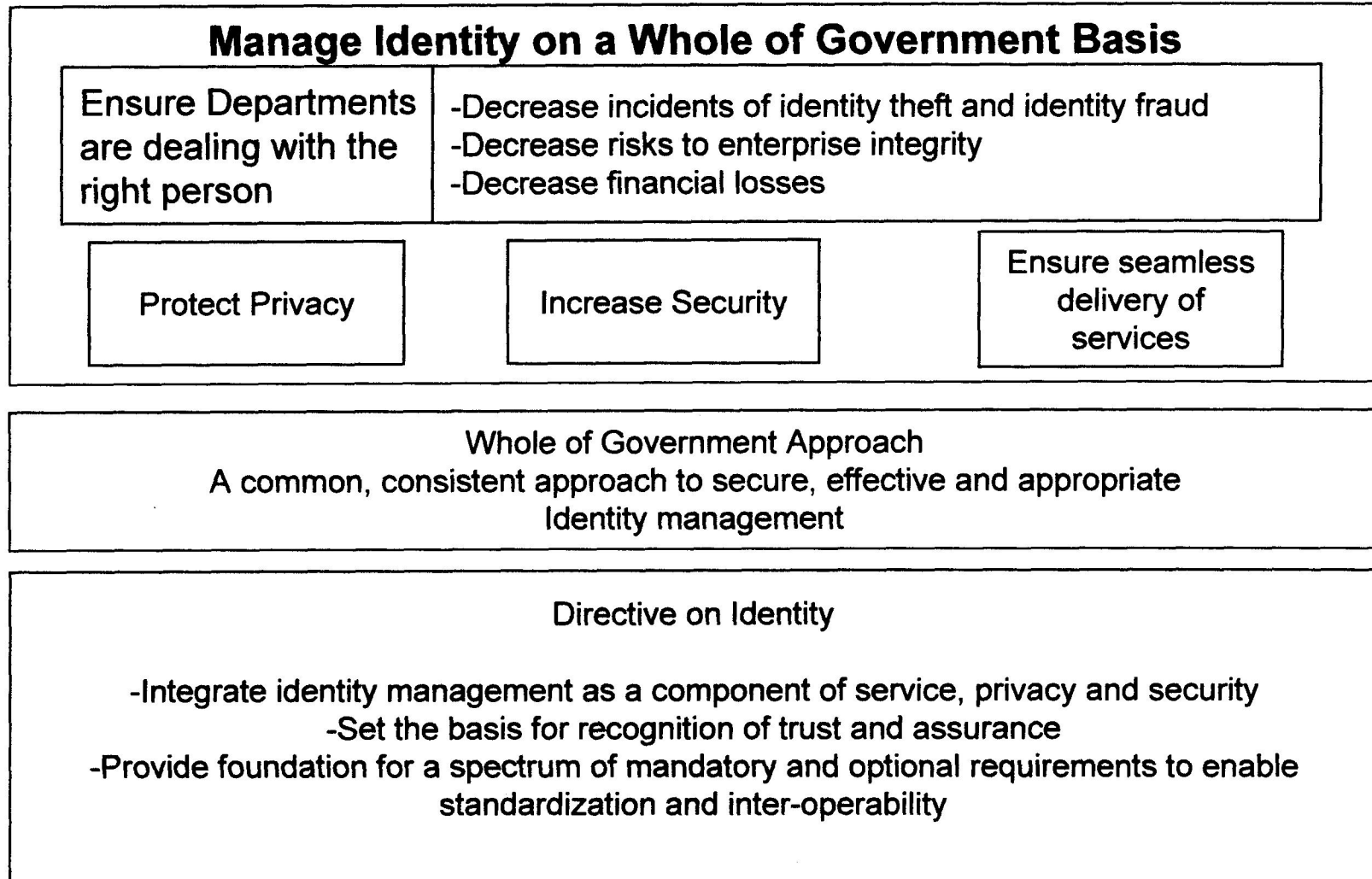
Integrated Security Approach



Policy on Government Security – Responsibilities of Deputy Heads



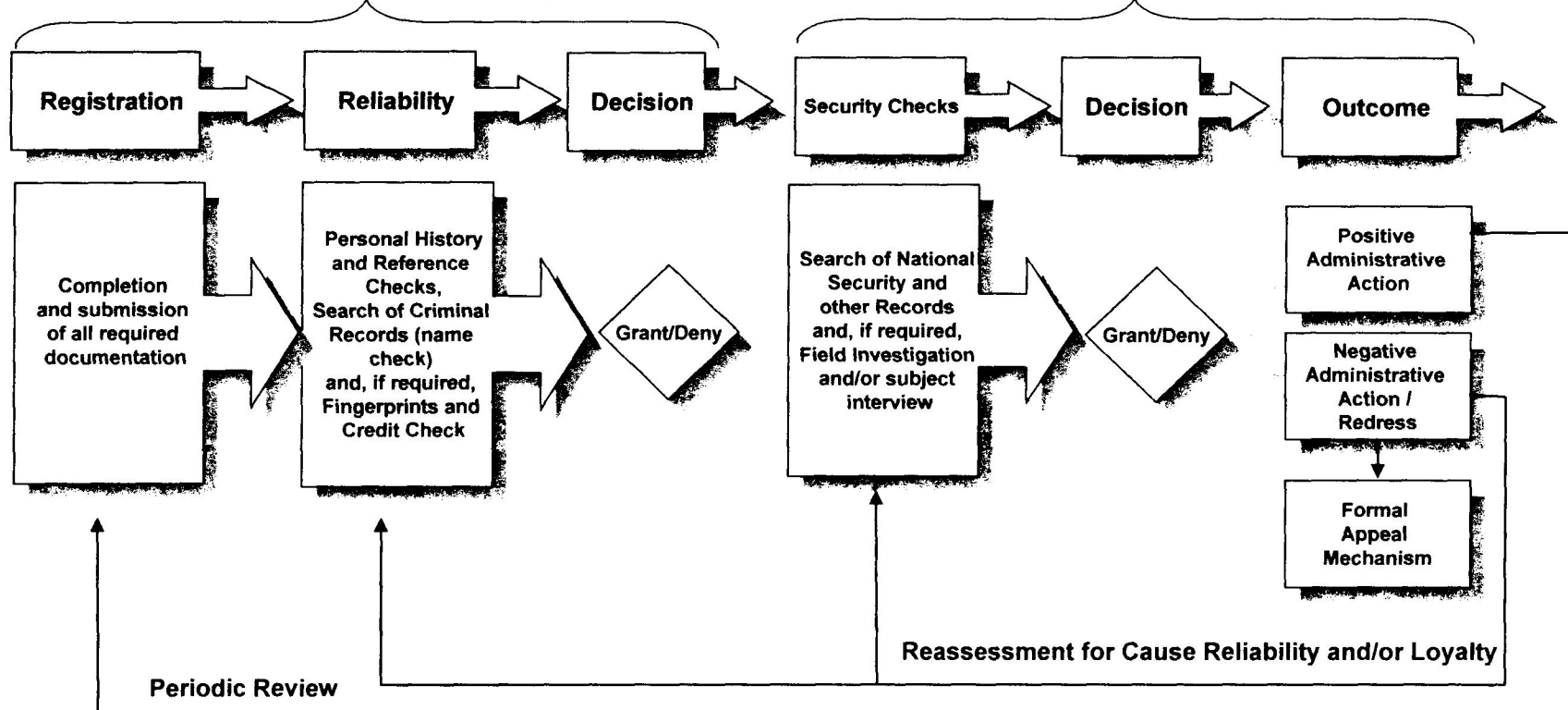
Directive on Identity Responsibilities of Deputy Heads



Reviewing the Individual Screening Standard

Reliability Status Check
(applies to 100% of Public Service & screened contractors)

Security Clearance Check
(applies to roughly 23% of Public Service & 40% of screened contractors)



Recommendations are forthcoming to enhance the individual screening standard and improve the integrity of the process

Canada 

s.15(1) - Int'l

s.15(1) - Subv

SECRET - [REDACTED]

Deputy Ministers Committee on National Security

Cyber Security - Ad Hoc Meeting

Friday, 20 February 2009
10:30 a.m. – 12:00 p.m.
Room 414, Langevin Block

Minutes

In attendance:

Marie-Lucie Morin (Chair - PCO)
Suzanne Hurtubise (PS)
[REDACTED] (CSIS)
John Adams (CSEC)
Robert Fonberg (DND)
Helen McDonald (IC)
John Ossowski (TBS)

Barbara Anderson (Finance)
Louis Levesque (International Trade)
Yves Côté (JUS)
William J.S. Elliot (RCMP)
François Guimont (PWGSC)
Rennie Marcoux (PCO – S&I)
Fraser Fowler (PCO S&I – Note taker)

Invitees:

Lynda Clairmont (PS)
Bob Gordon (PS)
Shelly Bruce (PCO - S&I)

Item 1: National Cyber Security Strategy (Public Safety)

- Public Safety officials provided an update to Deputies on the evolving national cyber strategy. In the ensuing discussion, Deputies acknowledged the priority of addressing cyber threats, particularly in the context of risks and vulnerabilities inherent in Canada's critical infrastructure. They also noted the complexity of building a national strategy which encompasses not only Canadian citizens, but also a broad range of both inter-jurisdictional and private sector stakeholders. In this regard, Deputies supported the intention of Public Safety to develop a private sector engagement strategy as part of its national cyber security strategy.

• [REDACTED]

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

[REDACTED]

[REDACTED] Deputies requested more information regarding the US investment strategy for the CNCI, and for the findings of the 60-day comprehensive review of cyber activities conducted at the request of the President Obama. [REDACTED]

[REDACTED]

- In reviewing the various cyber-related initiatives linked to the strategy, Deputies requested that the priorities, phasing and costs be revisited by ADMs. [REDACTED]

[REDACTED] To that end, Deputies requested a clear articulation of the benefits to be achieved through the completion of the various initiatives.

- Deputies were supportive of the draft strategy presented by Public Safety and encouraged the ADM advisory group to continue with its efforts. Deputies agreed to meet again in two months to resume the discussion [REDACTED]

[REDACTED]

Action Items:

- [REDACTED]
- [REDACTED]
- [REDACTED]

Page 111

**is withheld pursuant to sections
est retenue en vertu des articles**

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

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

Page 112

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1) - Subv

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

s.15(1) - Subv

- 5 -

SECRET - 

RDIMS: 418026 v5



Public Safety
Canada

Sécurité publique
Canada

SECRET



Cyber Security

Response to Minister's Questions



March 16, 2009

Canada

SECRET

Cyber Security Strategy Mandate

- The National Security Policy 2004 recognized that cyber security was a major element of emergency management and established the original mandate for the Strategy.

“Cyber-security is at the forefront of the transborder challenge to Canada’s critical infrastructure... The Government will convene a high-level national task force, with public and private representation, to develop the National Cyber-security Strategy to reduce Canada’s vulnerability to cyber-attacks and cyber-accidents”

- Public Safety Canada (PS) was tasked with the development of the Strategy.
- Communications Security Establishment Canada is one of 15 departments and agencies working with PS to develop the cyber security strategy.



Public Safety
Canada

Sécurité publique
Canada

SECRET

Why is a cyber security strategy necessary?

- Information and information systems are strategic assets for government and the private sector.
- Securing data, systems and networks is becoming extremely difficult

s.15(1) - Subv



- All sectors of economy and society – government, private sector, not-for-profit, individuals – are impacted.



SECRET

Why is a cyber security strategy necessary? (cont'd)

- The Canadian economy and Canadians' quality of life are dependent on information and communication technologies (ICTs).
- Canada's key financial and economic systems cannot operate without ICTs

-

-

s.16(2)(c)



SECRET

Why is a cyber security strategy necessary? (cont'd)

- Government service delivery also dependent on ICTs
 - 130 commonly used services (e.g., tax filing, SIN and passport applications, employment insurance filing) from 34 departments and agencies are online
 - tele-health, distance education, and many services to remote communities rely upon cyber technology
 - applies to all levels of government
- Canadian economy relies heavily on the internet
 - Canadian online sales in 2005 were valued at \$39.2 billion
 - 82% of public sector and 48% of private sector enterprises use the internet to purchase goods and services online
 - 100% of public sector and 87% of private sector firms use the internet



SECRET

Scope of National Cyber Security Strategy

- National scope including government, private sector and society
- National strategy will enhance cyber security in these three areas



SECRET

Progress to date

- This effort builds on government work already completed and currently underway within key departments and agencies, including Treasury Board Secretariat, Communications Security Establishment, RCMP, CSIS, Industry Canada, and others
 - Update of the Government Security Policy
 - [REDACTED]
 - Incident Management Plan
 - Technology upgrades
 - Various legislative amendments
 - Education for managers and civil servants

s.15(1) - Def



Public Safety
Canada

Sécurité publique
Canada

SECRET

Progress to date – cont'd

- Work completed includes engagement with private sector
 - Assessment of state of readiness in Canada's ten critical infrastructure sectors, including finance, energy, communications, and transport
 - Assessment of cyber interdependencies in Canada's ten critical infrastructure sectors
 - Development of a business case model for use by the private sector to justify increased investment in cyber security
 - Development of options for a made-in-Canada approach to information exchange between the government and the private sector
- Draft National Strategy and Action Plan for Canada's ten Critical Infrastructure sectors developed by PS



Public Safety
Canada

Sécurité publique
Canada

SECRET

Progress to date (cont'd)

- Consultations and workshops with key private and public sector stakeholders
- Public Awareness Campaign
 - Designation of October 2007 as Cyber Security Awareness month and mass distribution of information pamphlets (matches similar action by the U.S. and U.K.)



Public Safety
Canada

Sécurité publique
Canada

SECRET

What will be different

- Public Safety is coordinating a whole-of-government effort to develop a cyber security strategy.
- The Strategy will provide a framework for enabling Canada to
 - adapt proactively to the dynamically evolving cyber environment
 - be a credible and trusted partner to our allies in dealing with cyber security matters
 - enhance the safety, security and prosperity of Canada and Canadians



QP Note

Cyber Security

ISSUE:

Cyber Security note for the Minister's appearance at Standing Committee on Main Estimates

PROPOSED RESPONSE:

- **Information and information systems are strategic assets. Cyber security is about safeguarding these assets from cyber-based threats.**
- **Cyber vulnerabilities may be exploited by hostile states, organized crime groups, terrorists, and hackers.**
- **Like its allies, Canada is not immune to these threats.**
- **Securing cyber data and systems is an evolving challenge shared by governments, the private sector, and individuals around the world.**
- **Public Safety Canada has been leading the federal government's efforts to develop a National Cyber Security Strategy. This work builds on several years of research, analysis, and consultative activities with an array of government and private sector stakeholders, domestically and internationally.**
- **Completing and implementing a National Cyber Security Strategy is a priority for the Government.**

BACKGROUND:

As reflected in the 2009-10 Report on Plans and Priorities, development of a whole-of-government approach to Cyber Security is a key priority of the department of Public Safety.

The information age and the Internet have brought immense changes to Canada and to Canadians.

Information and information systems are strategic assets for government and the private sector. Much of our information is in electronic form. Many of the essential activities of government, the private sector, and society depend on access to that information and to the Internet. However, securing these critical data, systems and networks is extremely difficult. Hostile nation states and criminals are increasingly exploiting information systems to access confidential state and industrial information, to disrupt operations, and to steal intellectual property and money. Technology allows criminals and terrorists to communicate and operate away from the scrutiny of police and intelligence officers. The rapid evolution of technology makes it extremely difficult to build systems that remain reliable and secure against attacks. All sectors of our economy and society – governments, private sector, not-for-profit, individuals – are impacted.

In 2008, Public Safety carried out public opinion research in order to better understand the practices employed by Canadians to ensure the safety of their online activities. The study found that while many Canadians use the Internet for sensitive transactions, most (77%) are also concerned about the security of their personal information.

Cyber security is a shared responsibility – no single country, government, organization or individual can truly secure their networks in isolation, we must all do our part.

The National Cyber Security Strategy should:

- Achieve Cyber Integrity of Government
- Protect Critical Assets and Information
- Combat Cyber Facilitated Crime and Protect Citizen Safety Online

Resources

\$5m was originally allocated for the development of the *National Cyber Security Strategy*. Funding to continue developing the strategy has been committed through internal reallocation within the department.

Progress in enhancing Canadian Cyber Security

The current Canadian Cyber Incident Response Centre within Public Safety Canada continues to serve government and critical infrastructure sectors by coordinating Canadian participation in international cyber exercises and responses to hundreds of cyber events while also producing a variety of advisories and technical reports on vulnerabilities and mitigation strategies.

In support of the development of the Strategy, Public Safety has completed numerous activities, including consultations with the private sector and discussions with international partners.

Across government, cyber security efforts will build on work, both completed and ongoing, by key departments and agencies including Treasury Board Secretariat, Communications Security Establishment Canada, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and Industry Canada.

Canada and the United States, in developing their strategies to enhance cyber security, have recognized the importance of international collaboration, especially for highly interconnected sectors like energy, communications and banking.

CONTACTS:			
Prepared by Bob Gordon	Tel. no. (613) 949-7380	Approved by Lynda Clairmont	Tel. no. (613) 990-4976

QP Note

National Cyber Security Strategy

ISSUE: To provide information regarding development of the *National Cyber Security Strategy* for the Minister's appearance at Standing Committee on Main Estimates.

PROPOSED RESPONSE:

- **Information and information systems are strategic assets that must be protected in the "Information Age".**
- **While the Internet has brought many benefits it has also exposed us to daily global threats. Everything and everyone is now interconnected.**
- **Securing data, systems and networks is an evolving challenge shared by governments, the private sector, and individuals around the world.**
- **Cyber security looks to protect against the unauthorized access to information systems or disclosure of sensitive information. At risk are state secrets, personal information, corporate trade secrets, and the availability of essential services.**
- **Cyber attacks come from hostile nation states, organized crime, terrorists, and hackers.**
- **Since all sectors of the economy and society are impacted, the Government of Canada is developing a National Cyber Security Strategy to better manage cyber security risks.**
- **Public Safety Canada has been working across government and with the private sector to develop a National Cyber Security Strategy.**
- **The purpose of the initiative is to produce a strategy that will**

coordinate existing capabilities and initiatives, and identify required new initiatives to enhance Canadian cyber security.

- **The initiative builds on several years of research, analysis, and consultative activities both domestically and internationally.**
- **The completion and implementation of a National Cyber Security Strategy is a priority for my department and for the Government.**

BACKGROUND:

As reflected in the 2009-10 Report on Plans and Priorities, development of a whole-of-government approach to Cyber Security is a key priority of the department of Public Safety.

The information age and the Internet have brought immense changes to Canada and to Canadians.

Information and information systems are strategic assets for government and the private sector. Much of our information is in electronic form. Many of the essential activities of government, the private sector, and society depend on access to that information and to the Internet. However, securing these critical data, systems and networks is extremely difficult. Hostile nation states and criminals are increasingly exploiting information systems to access confidential state and industrial information, to disrupt operations, and to steal intellectual property and money. Technology allows criminals and terrorists to communicate and operate away from the scrutiny of police and intelligence officers. The rapid evolution of technology makes it extremely difficult to build systems that remain reliable and secure against attacks. All sectors of our economy and society – governments, private sector, not-for-profit, individuals – are impacted.

In 2008, Public Safety carried out public opinion research in order to better understand the practices employed by Canadians to ensure the safety of their online activities. The study found that while many Canadians use the Internet for sensitive transactions, most (77%) are also concerned about the security of their personal information.

Cyber security is a shared responsibility – no single country, government, organization or individual can truly secure their networks in isolation, we must all do our part.

The National Cyber Security Strategy should:

- Achieve Cyber Integrity of Government
- Protect Critical Assets and Information
- Combat Cyber Facilitated Crime and Protect Citizen Safety Online

Resources

\$5m was originally allocated for the development of the *National Cyber Security Strategy*. Funding to continue the development the strategy has been committed through internal reallocation within the department.

Progress in enhancing Canadian Cyber Security

The current Canadian Cyber Incident Response Centre within Public Safety Canada continues to serve government and critical infrastructure sectors by coordinating Canadian participation in international cyber exercises and responses to hundreds of cyber events while also producing a variety of advisories and technical reports on vulnerabilities and mitigation strategies.

In support of the development of the Strategy, Public Safety has completed numerous activities, including consultations with the private sector and discussions with international partners.

Across government, cyber security efforts will build on work, both completed and ongoing, by key departments and agencies including Treasury Board Secretariat, Communications Security Establishment Canada, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and Industry Canada.

Canada and the United States, in developing their strategies to enhance cyber security, have recognized the importance of international collaboration, especially for highly interconnected sectors like energy, communications and banking.

CONTACTS:

Prepared by
Bob Gordon

Tel. no.
(613) 949-7380

Approved by
Daniel Lavoie

Tel. no.
(613) 990-2743



Public Safety
Canada

Sécurité publique
Canada


SECRET



Briefing for:

Executives:

**National Security Agency
Communications Security
Establishment Canada**



April 24, 2009

Canada

UNCLASSIFIED

Public Safety Canada

- Created in 2003 to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians.
- Works with five agencies and three review bodies
- Delivers programs and develops policy for:
 - Emergency management
 - National security
 - Law enforcement
 - Corrections
 - Crime prevention
- Annual budget exceeds \$9 billion with approx. 63,000 employees

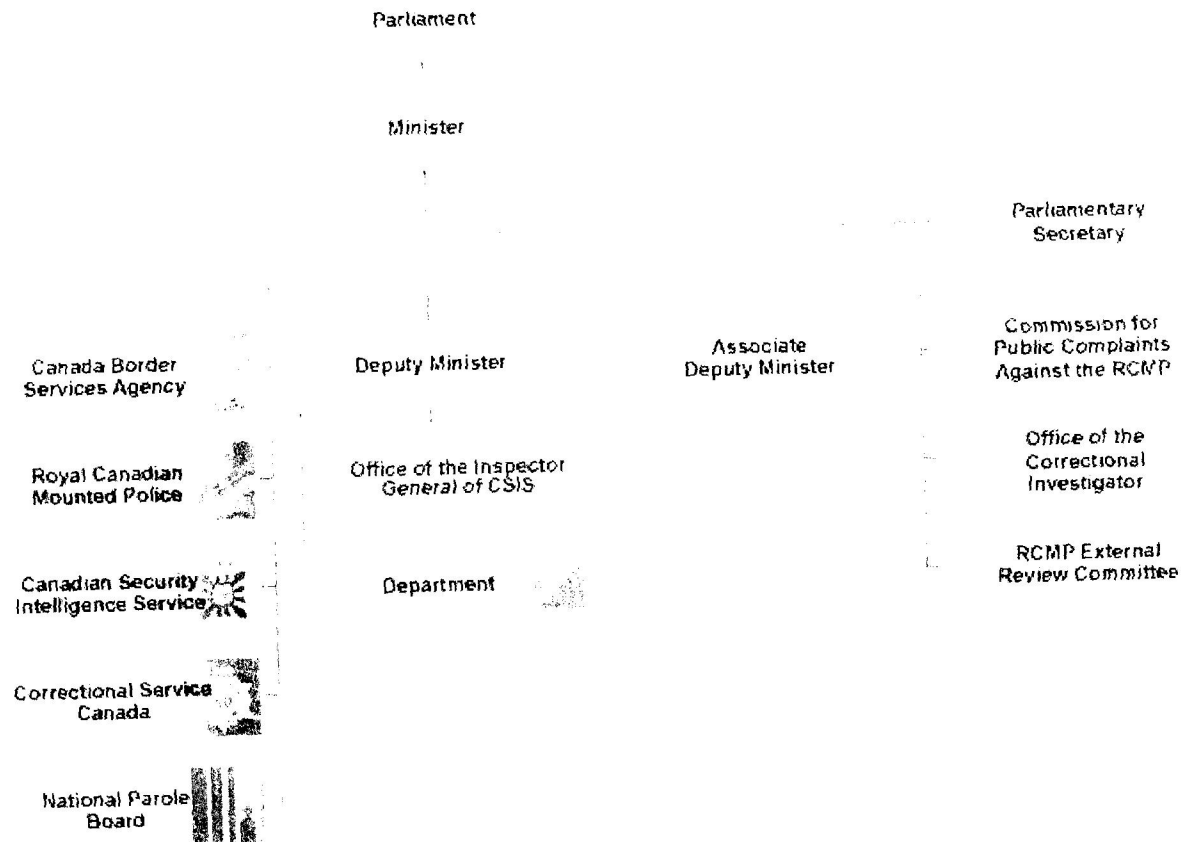


Public Safety
Canada

Sécurité publique
Canada

UNCLASSIFIED

Public Safety Portfolio



SECRET

How We're Capturing the Issue

- Information and information systems are strategic assets for governments and the private sector.
- Securing data, systems and networks is becoming extremely difficult
 - hostile nation states and criminals are increasingly exploiting information systems to access information, state and industrial secrets, disrupt operations, and make a profit
 - technology allows criminals and terrorists to communicate away from the scrutiny of police and intelligence officers
 - the rapid evolution of technology makes it extremely difficult to build systems that are reliable and secure against attacks
- All sectors of economy and society – governments, private sector, not-for-profit, individuals – are impacted.



UNCLASSIFIED

Cyber Security Strategy Mandate

- The National Security Policy 2004 recognized that cyber security was a major element of emergency management and established the original mandate for the Strategy
 - *Cyber-security is at the forefront of the transborder challenge to Canada's critical infrastructure... The Government will convene a high-level national task force, with public and private representation, to develop the National Cyber-security Strategy to reduce Canada's vulnerability to cyber-attacks and cyber-accidents*
- Public Safety Canada was tasked with the development of the Strategy.



UNCLASSIFIED

Canadian Context

- Government service delivery also dependent on ICTs
 - 130 commonly used services (e.g., tax filing, SIN and passport applications, employment insurance filing) from 34 departments and agencies are online
 - tele-health, distance education, and many services to remote communities rely upon cyber technology
 - applies to all governments
- Canadians have embraced the internet
 - 58% of personal tax filings are electronic (2008 tax year)
 - 73% of Canadians 16 and older (19.2 million) went online from home in 2007
 - 46% of Canadians bank online
 - 33% of Canadians order goods or services online
 - growing dependency on tele-health and distance education services, especially in Canada's northern and remote communities



UNCLASSIFIED

Considerations

- 2005 Auditor General Report: “We are concerned that, in many departments and agencies, senior management is not aware of the IT security risks and does not understand how breaches of IT security could affect operations and the credibility of the government.”
- 2008 Privacy Commissioner: “2007 was a year of data privacy disasters, highlighting the need for companies to recognize the value of personal information and take more care in securing it.”
- Cyber security must be pursued multilaterally – key international fora (G8, APEC, OECD, NATO, etc.) have identified cyber security as an important issue.



SECRET

Progress to date

- Public Safety is leading inter-departmental efforts to develop a National Cyber Security Strategy.
- Work completed or underway includes
 - assessment of state of readiness in Canada's ten critical infrastructure sectors
 - development of a business case model for use by private sector to justify increased investment in cyber security
 - development of options for a made-in-Canada approach to information exchange between the government and the private sector
 - consultations and workshops with key private and public sector stakeholders
 - U.S., U.K., and Australian officials have been briefed on Canadian activities [REDACTED]

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

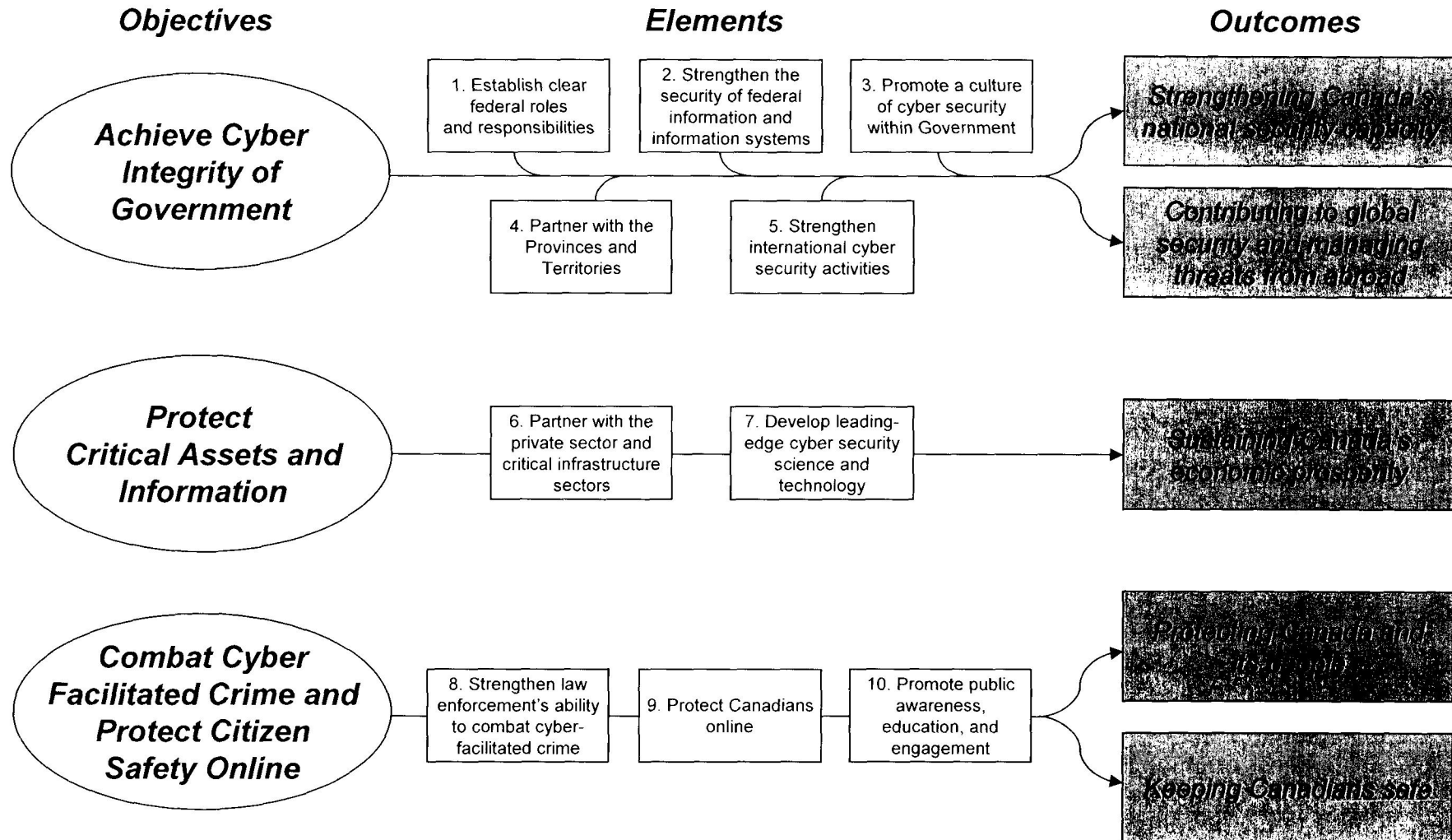


Public Safety
Canada

Sécurité publique
Canada

SECRET

Cyber Security For A Strong and Resilient Canada



SECRET

Notional Elements of a Cyber Security Strategy

Key elements of a cyber security strategy may include

1. Achieving cyber integrity of the federal government by
 - strengthening the security of Government of Canada information systems by updating policies and standards, expanding secure communications capabilities, enhancing security in procurement, and coordinating research and development
 - identifying federal leadership for national cyber security coordination
 - ensuring that organizations clearly understand their cyber incident response roles and responsibilities so that response actions are as rapid and well-coordinated as possible
 - educating government employees about cyber security matters
 - initiating increased cyber security collaboration with provincial and territorial governments at policy and operational levels
 - strengthening international collaboration in cyber security



SECRET

Elements of a Cyber Security Strategy (cont'd)

2. Protecting critical assets and information by
 - assisting the private sector and critical infrastructure sectors to strengthen their cyber security practices by sharing cyber intelligence, inviting participation in cyber exercises, promoting the use of standards and certifications, etc.
 - developing leading-edge cyber security science and technology by encouraging collaborative academic, private sector and government research and development
3. Combating cyber-facilitated crime and protecting citizen safety online by
 - strengthening law enforcement's abilities to fight cyber crime, including legislation to provide for lawful access
 - promoting public awareness, education, and citizen engagement
 - enhancing privacy protections for Canadians by requiring data breach reporting



SECRET

Cyber Security and Critical Infrastructure Protection Strategy

- Developing a unified approach to these two issues is a high priority
- Past and international experience has demonstrated:
 - Complete integration of approaches and mechanisms doesn't work
 - Completely separate approaches leads to duplication of effort and lack of focus
- We are working to find the right interaction between the two and will design our organization and outreach accordingly



Public Safety
Canada

Sécurité publique
Canada

SECRET

Moving Forward

- Public Safety is coordinating a whole-of-government effort to develop a cyber security strategy.
- A first draft of the Strategy is expected to be completed in Spring 2009.
- [REDACTED]
- Legislative changes are being identified and resource requirements are being assessed.
- The Strategy will provide a framework for enabling Canada to
 - adapt proactively to the dynamically evolving cyber environment
 - be a credible and trusted partner to our allies in dealing with cyber security matters
 - enhance the safety, security and prosperity of Canada and Canadians

s.15(1) - Int'l



Public Safety
Canada

Sécurité publique
Canada



To / À: [redacted] CSEC
[redacted] CSIS
Robert Walker, DRDC
Colleen Swords, DFAIT
John Turner, DND
Daniel Thérien, DOJ
Helen McDonald, IC
Rennie Marcoux, PCO
Jane Meyboom-Hardy, PWGSC
Maurice Chénier, PWGSC
Bruce Rogerson, RCMP
Peter Bruce, TBS

May 8, 2009

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

From / De: Lynda Clairmont, PS

Subject / Upcoming meeting of [redacted] responsible for Cyber Security
Objet: (Action Requested)

Good morning,

This provides an update on the status of preparations for the upcoming meeting of [redacted] tentatively scheduled for June 29-30, 2009, and requests your assistance in preparing for that meeting.

Background



s.13(1)(a)

s.15(1) - Int'l

SECRET



Next Steps

I am looking to you for your support, as needed, in developing the Canadian objectives and positions in advance of the meeting, and in following through on agreed-upon actions. As the agenda for the meeting is finalized, specific discussions will be initiated through the DG Cyber Interdepartmental that will engage the appropriate departments and agencies in developing Canadian positions.

My thanks in advance for your assistance in furthering this important work. Should you have any questions, please don't hesitate to contact me or Colleen D'Iorio, Director General, National Cyber Security.

Best regards,

Lynda Clairmont



BRIEFING NOTE NOTE D'INFORMATION

Classification: Unclassified

Docket number: 362783

Date: May 29, 2009

PURPOSE:

To provide a summary of the key findings of the United States' (U.S.) 60 day review to assess policies and structures for cyber security (60 Day Review)

BACKGROUND:

On May 29, 2009, the U.S. released its report on the findings of the 60 Day Review, entitled "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure". (TAB A)

The review addressed all activities associated with the security of the information and communications infrastructure, including computer network defence, law enforcement investigations, military and intelligence activities, information assurance, counterintelligence, counterterrorism, telecommunications policies, and general critical infrastructure protection.

In conjunction with the release of the report is the launch of a White House website dedicated to the 60 day review (<http://www.whitehouse.gov/CyberReview/>). This website includes the public report as well as more than 100 issues papers submitted by government and private sector stakeholders.

CURRENT STATUS:

The report structures the findings and options for action under five key topics: leading from the top; building capacity for a digital nation; sharing responsibility for cyber security; improving information sharing and incident response; and building the architecture of the future. Key recommendations for each of these topics are:

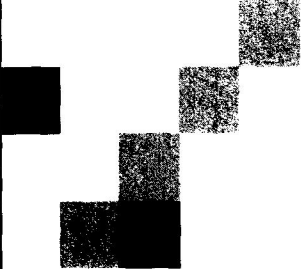
- **Leading from the top:** The report recommends the appointment of a cyber security policy official at the White House reporting to both the National Security Council and the National Economic Council. The U.S. President committed to the establishment of a "Cyber Security Coordinator" to fulfill this mandate, however, the individual to fill this position has not yet been named. One of the principal initiatives of the Cyber Security Coordinator will be to clarify authorities, roles, and responsibilities for cyber security-related activities across the federal government.
- **Building capacity for a digital nation:** The need for a national cyber security public awareness strategy is identified as a key recommendation. This includes promoting cyber security risk awareness for citizens, developing an education system to enhance cyber security understanding, expanding scientific, engineering, and market leadership in information technology, expanding and training the workforce to protect the nation's competitive advantage, and helping organizations and individuals manage cyber security risk.

- Sharing responsibility for cyber security: The report focuses on the need for improved and enhanced partnerships with both the private sector and international partners. Specifically, it identifies the need for government and industry leaders, both nationally and internationally, to delineate roles and responsibilities, integrate capabilities, and take ownership of the problem to develop holistic solutions. These efforts should seek, in collaboration with the private sector, to improve the security of interoperable networks by developing global standards, expanding the legal system's capacity to combat cyber crime, continuing to develop and promote best practices, and maintaining stable and effective Internet governance.
- Improving information sharing and incident response: The report identifies the need for a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident. It recommends that all levels of government work with industry to improve plans and resources to detect, prevent, and respond to significant cyber security incidents. Because such incidents are likely to affect interconnected networks across government and industry sectors, it stresses that coordination of these plans and activities is important before, during, and after significant incidents.
- Building the architecture of the future: This area addresses the need for additional research and development initiatives. In particular, the need is identified for the federal government to work with industry on the development of next-generation secure computers and networking for national security applications, new standards for cyber security and physical resilience, and standards for securing personal data. It highlights the need to create federal policy to address national security requirements, protect intellectual property, and ensure the availability and continuity of infrastructure, without inhibiting innovation or creating inefficiencies.

Included in the report are action plans for the near and mid-term which encompass 24 recommended actions. The near-term plan includes the preparation of a national strategy to secure the information and communications infrastructure. The mid-term plan calls for the development of efficient and effective mechanisms to obtain strategic warning, maintain situational awareness and inform incident response capabilities.

Canada is developing a National Cyber Security Strategy that is intended to achieve cyber integrity of government, protect the economy and critical infrastructure, combat cyber-facilitated crime and protect citizen safety online. The tenets identified in the 60 Day Review are generally consistent with those that are being addressed by the Canadian strategy.


Prepared By:
Ryan Hunt
National Cyber Security Directorate



Can-US EMCG

Cyber Security Working Group

October 20, 2009



Context

- Cyber security has been identified by both governments as a national security priority
- *Borderless nature of cyberspace creates a need for international cooperation and collaborative action to overcome information infrastructure protection challenges, especially in times of crisis*
- Existing commitments and related work
 - *Very strong linkages in the security and intelligence community*
 - Ongoing information exchange on cyber security initiatives at the strategic level
 - Good collaboration between national cyber incident response centres
 - Bilateral involvement in both CyberStorm I and II

1

Key Areas for Future Collaboration

- Policy, Programs, and Capabilities Development
 - Review ongoing developments in each nation's cyber security strategies
 - Share best practices for programs and activities of mutual concern, such as control systems security and cyber security awareness
- Computer Security Incident Response Team (CSIRT) Collaboration
 - Continue to enhance US-CERT/CCIRC collaboration and information sharing
- Cyber Incident Management
 - Share national approaches on cyber security incident management and promote cohesion and collaboration
- Exercise Collaboration
 - CyberStorm III (Fall 2010)
 - Enhance Usual 5 and International Watch and Warning Network (IWWN) activities
- Coordination of engagement in various multilateral fora

2

Proposed Workplan

- Fall 2009
 - Initial planning activities for CyberStorm III
 - Bilateral engagement between US-CERT/CCIRC
 - Usual 5 / IWWN engagement
 - Information sharing on national approaches and plans
- Winter 2010
 - Continue CyberStorm III development activities
 - Improving US-CERT/CCIRC interactions and information sharing
- Spring/Summer 2010
 - Final preparations for CyberStorm III
 - Usual 5 / IWWN ongoing engagement
 - Analysis of opportunities for further cooperation

3

**Pages 148 to / à 149
are withheld pursuant to sections
sont retenues en vertu des articles**

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

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

SECRET

Deputy Ministers' Committee on Cyber

Thursday, June 4, 2009
1:30 p.m. to 3:00 p.m.
Room 411, Langevin Block

Minutes

Committee Members Present:

Marie-Lucie Morin, National Security Advisor to the Prime Minister (Co-chair)
Suzanne Hurtubise, Deputy Minister, Public Safety (Co-chair)
Rennie Marcoux, Assistant Secretary, Privy Council Office
John Adams, Chief, Communication Security Establishment
Francois Guimont, Deputy Minister, Public Works and Government Services
John Sims, Deputy Minister, Justice

Substitutes:

[REDACTED] Deputy Director, Canadian Security Intelligence Service
John Ossowski, Assistant Secretary, Treasury Board
Helen McDonald, Assistant Deputy Minister, industry Canada
Bill Sweeney, Deputy Commissioner, Royal Canadian Mounted Police
Bill Pentney, Associate Deputy Minister, National Defence

Also Present:

Claude Carrière, Foreign and Defence Policy Advisor to the Prime Minister

Not Present:

Louis Levesque, Deputy Minister, International Trade

Supporting Officials Present:

Dan Hallman, A/Chief of Staff for the National Security Advisor
John Richard, Analyst, PCO Security and Intelligence (Note-taker)

Introductory remarks

- The National Security Advisor (NSA) opened the meeting with a quick overview of cyber security in today's global environment with respect to both the private and public sectors.

Item 1: Cyber Security Threat (PS/CSE/CSIS)

- [REDACTED]

s.15(1) - Int'l
s.15(1) - Subv
s.16(2)(c)

SECRET

- The Chief of the Communications Security Establishment (CSE) opened his remarks by adding some of the following Canadian context;
 - Explaining that Canada is the ninth most “wired” nation with the US being the first.
 - Indicating that cyber crime has now surpassed the drug trades and now exceeds 2 billion dollars in Canada alone.
 - Stating that the Government of Canada offers in excess of 100 online services and outlined known vulnerabilities and past exploitations of some of those systems.



Item 2 a: Update on National Cyber Security Strategy

- The DM of PS provided a brief presentation to provide an update on the status of the draft cyber security strategy.



SECRET

s.14(a)

-

[Redacted]

s.15(1) - Int'l

s.15(1) - Subv

Action Items:

-

[Redacted]

Item 2 b: Update on US 60 Day review

- Discussions around the newly announced results of the US review on its cyber policies resulted in discussions and comparisons to Canada's own strategy. [Redacted]
- [Redacted]
- US have announced the creation of its new cyber Czar however has not yet indicated who would fill that position.

Item 2 c: Update on [Redacted] meeting

-

[Redacted]

-

Item 2 d: Way ahead discussion

-


[Redacted]

-

s.14(a)

s.21(1)(b)

SECRET

- 
- Due to this perception, it was felt that a strong engagement strategy is needed to bring both public and private sectors up to speed with respect to cyber issues and more specifically cyber security issues.

- 

Action Items:

- 
- 
- PS to continue to develop the Canadian cyber strategy over the next several months.
- PS to conduct an analysis of United States and Canadian cyber strategies with a view to determining the “delta” between the two.

InfoXpress – 451828
WebCIMSS – 2009-SI-00236

SECRET




**Meeting with the President of the United States,
Lunch with members of the Council on Foreign Relations, and
Dinner with House and Senate Leaders
September 15, 2009**

Issue

- Background information on national cyber security activities (Canada-US focus)

Background


- The Governments of Canada and of the United States share the view that cyber security is a serious issue demanding immediate strategic action. Our nations share an excellent and close working relationship on cyber security. The main tenets of our respective strategic efforts are aligned and compatible.
- Cyber security is a pan-government activity, led in Canada by Public Safety in close collaboration with the Communications Security Establishment Canada, the Royal Canadian Mounted Police, National Defence, and others. These organizations also maintain strong bilateral relationships with their direct US counterparts, including the Department of Homeland Security, the National Security Agency, the Federal Bureau of Investigation, the Department of Defense, and others.
- Both governments have been active in cyber security and related fields such as critical infrastructure protection and signals intelligence for decades, and both nations have significant capability. 
- Canada is currently developing a National Cyber Security Strategy that will aim to achieve cyber integrity of government, protect critical assets and information in the private sector and critical infrastructure, and combat cyber-facilitated crime and protect Canadians online. A draft Strategy is due to Ministers this fall for consideration.
- In 2008, the United States launched a significant cyber security initiative focusing almost exclusively on U.S. government systems (the Comprehensive National Cybersecurity Initiative, or CNCI). This initiative closely parallels the government-focused pillar of the proposed Canadian strategy.
- The Obama administration continued the CNCI and launched an extensive 60 day review to examine all aspects of U.S. cyber security policy. The results, announced personally by President Obama in May 2009, focused on extending cyber security efforts to include the private sector and the citizenry. These themes essentially mirror the two remaining pillars of the proposed Canadian strategy.

s.15(1) - Int'l

s.13(1)(a)

s.15(1) - Int'l

SECRET

- International engagement has been a strong recurring theme across U.S. cyber security efforts. The U.S. has explicitly indicated to Canada that 

Speaking Points

- Cyber security is an important shared responsibility requiring a coordinated and focused effort both domestically and internationally.
- The Government of Canada takes cyber security very seriously and is doing its part.
- My department is leading cross-government efforts to produce a cyber security strategy and implementation plan that will ensure the cyber integrity of government, engage the private sector in protecting critical infrastructure and our economy, combat cyber-facilitated crime and protect Canadians online.
- The strategy will be based on consultations with the private sector and ongoing discussions with our international allies, and will build on significant efforts already underway within government



Public Safety
Canada

Sécurité publique
Canada

SECRET



Securing North American Cyber Space

The 224th Meeting of the Permanent Joint Board on Defence, Canada-US



November 9, 2009

Canada

SECRET

Issue

- Information and information systems are strategic assets for governments and the private sector.
- Securing data, systems and networks is becoming extremely difficult.
- All sectors of economy and society – national security, economic security, law enforcement – are impacted.
- Are existing bi-lateral mechanisms for dealing with traditional threats suitable for emerging cyber security threats?



SECRET

Context

- Government service delivery is dependent on information and communication technologies (ICTs)
- The Canadian economy and Canadians' quality of life are dependent on ICTs
- Canada's key critical infrastructures cannot operate without ICTs
- Canadians have embraced the Internet
- Similar statements are equally applicable to the United States



SECRET

Consequences of cyber attacks

- An estimated 1.7 million Canadians were victims of identity theft in 2008 (McMaster University, 2009)
- Estimated annual cost to Canada of identity theft alone is \$2 billion (McMaster University, 2009)
- Canadian publicly traded companies experience an estimated nine breaches per year. This translates into an average loss, per company, of more than \$675,000 annually. (2009 study conducted by TELUS and the University of Toronto)
- 86% of large Canadian organizations have experienced cyber attacks (Computer Associates, June 2008)
- Globally, in 2008 companies are estimated to have lost more than \$1 trillion in intellectual property (patents, research, trade secrets) due to cyber crime. (McAfee/Purdue University, 2009)



SECRET

Cyber Security – a Canadian Priority

- The National Security Policy 2004 recognized that cyber security was a major element of emergency management.

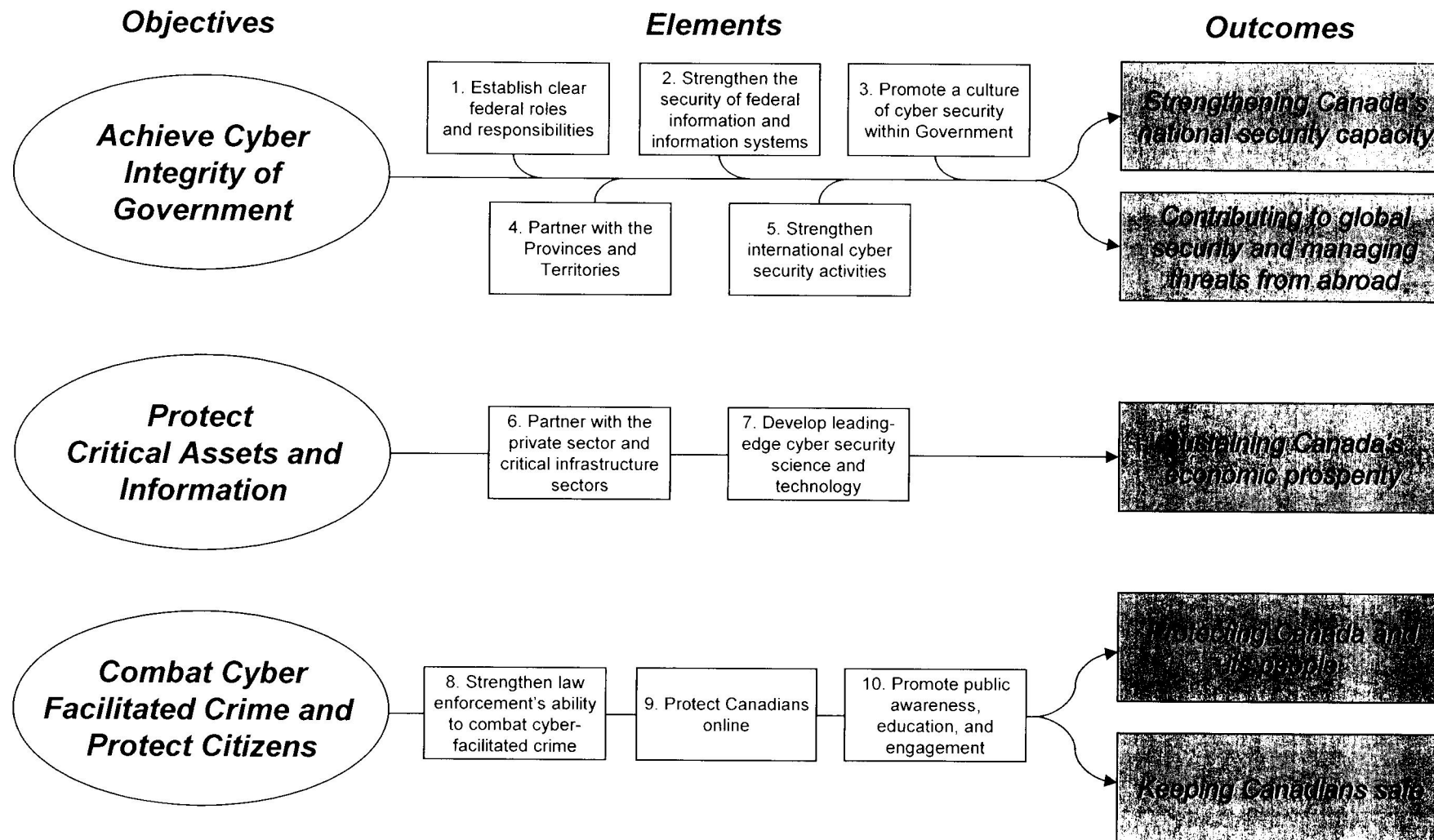
Cyber-security is at the forefront of the transborder challenge to Canada's critical infrastructure...

- Public Safety Canada was tasked with the development of Canada's Cyber Security Strategy.
- The Minister of Public Safety has stated
 - (cyber security) is almost a new arms race
 - developing a cyber security strategy is a priority for the Government
 - a national cyber security strategy will be completed this Fall



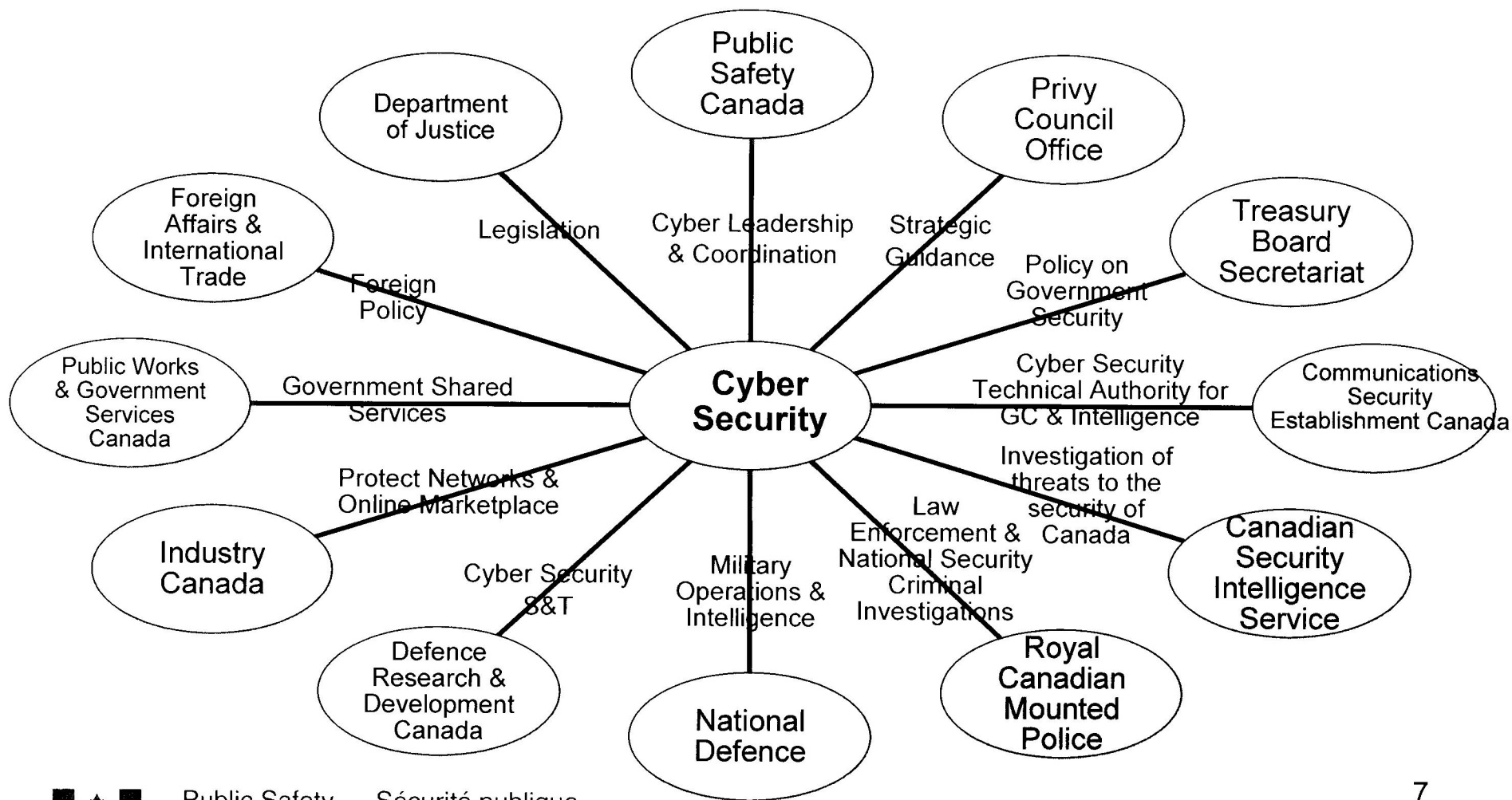
SECRET

Cyber Security for a Strong and Resilient Canada



SECRET

Cyber Security – Community

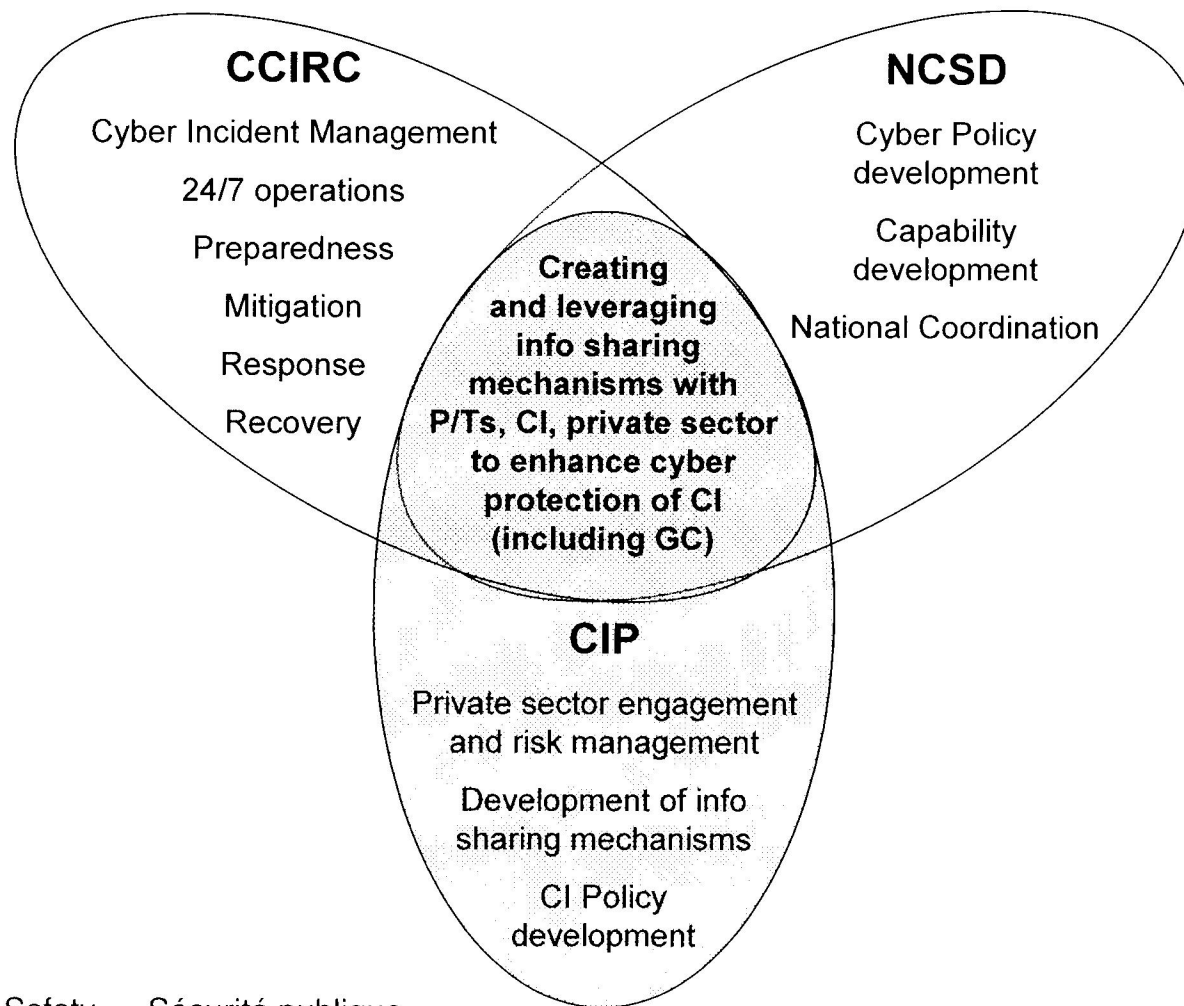


Public Safety
Canada

Sécurité publique
Canada

SECRET

Public Safety – Roles and Responsibilities



SECRET

Canadian and U.S. Cyber Security Initiatives

Notional Vision of Canadian Strategy

Achieve Cyber Integrity of Government

1. Establish National Cyber Security Leadership and Capabilities
2. Strengthen the Security of GC Information and Information Systems
3. Promote a Culture of Cyber Security within Government
4. Augment Joint Activities with the Provinces and Territories
5. Strengthen International Cyber Security Activities

Protect Critical Assets and Information

6. Assist the Private Sector and CI in Strengthening Cyber Security Practices
7. Develop Leading-Edge Cyber Security Science and Technology

Combat Cyber Facilitated Crime and Protect Citizen Safety Online

8. Strengthen Law Enforcement's Ability to Combat Cyber-Facilitated Crime
9. Enhance Privacy Protection for Canadians
10. Promote Public Awareness, Education, and Engagement

* Note: 8, 9, 10 have no U.S. equivalent

U.S. Comprehensive National Cybersecurity Initiatives

1. Trusted Internet connections (Relates to Cdn 2)
2. Deploy intrusion detection system (Cdn 2)
3. Deployment of automated defence sensors across Executive Branch federal systems (Cdn 2)
4. Coordinate and redirect research and development efforts (Cdn 2)
5. Connect current cyber Centers to enhance cyber situational awareness (Cdn 1)
6. Develop a government-wide cyber counterintelligence plan (Cdn 1)
7. Increase the security of classified networks (Cdn 2)
8. Expand cyber education (Cdn 3)
9. Define and develop enduring 'leap-ahead' technology, strategies and programs (Cdn 7)
10. Define and develop enduring deterrence strategies and programs (Cdn 5)
11. Develop a Multi-pronged approach for global supply chain risk management (Cdn 2)
12. Develop the federal role for extending cybersecurity into critical infrastructure domains (Cdn 6)



Public Safety
Canada

Sécurité publique
Canada

SECRET

United States Addresses Cyber Security

- 60-day Cyber Security Review released on May 29
- The President emphasized the importance of cyber security
 - "...the cyber threat is one of the most serious economic and national security challenges we face as a nation...in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few keystrokes on the computer -- a weapon of mass disruption"
- The President announced that the White House will develop a new comprehensive strategy to secure America's information and communications networks.
- Establishment of U.S. Cyber Command



SECRET

Cyber Challenges for Canada and United States

- The global cyber threat and threat actors are essentially the same for both countries
- Our societies are dependent upon information and information systems
- Electrons don't recognize borders
- Our critical infrastructure sectors are interconnected and interdependent
- Attacks on one CI sector risk bleeding into other sectors and across borders
- No one jurisdiction can fully address the issue
- Conclusion: The cyber threat is different than traditional threats – a new approach is required.



SECRET

What's different about the cyber threat compared with traditional threats?

- Attribution of who's attacking is difficult
- The threat only manifests itself on the device you are trying to defend
- Scale becomes an issue – millions of devices to be defended
- Geography is a foreign concept in cyber space
- Much of what needs to be defended is owned and operated by the private sector

s.21(1)(a)

-
-

- Is a technical solution possible? People engineered the Internet and its infrastructure and some say we now know how to fix it
 - Should we influence the evolution of the structure?
 - There appears to be no venue for this discussion.



Public Safety
Canada

Sécurité publique
Canada

SECRET

What's different about the cyber threat compared with traditional threats? (cont'd)

- The ease of attacks is increasing.
- How do we take account of non-state actors?



- NORAD has been a success – Why?
 - The focus has been very restricted
 - The geography and air space (the Border) to be defended is well defined and generally accepted internationally
 - General acceptance of traditional risks and responses domestically and internationally
 - Well known adversaries and potential attackers are usually easy to identify
 - Generally involves only state actors and response



**Pages 171 to / à 172
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

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

s.15(1) - Int'l

SECRET



Discussion



Public Safety
Canada

Sécurité publique
Canada

SECRET



Public Safety
Canada

Sécurité publique
Canada



Public Safety
Canada

Sécurité publique
Canada

SECRET



Cyber Security

**Visit of Robert Butler, Deputy Assistant
Secretary of Defense for Cyber and Space
Policy, and**

s.19(1)

 **and** 



DECEMBER 10, 2009

Canada

SECRET

Public Safety Canada

- Created in 2003 to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians.
- Works with five agencies and three review bodies
- Delivers programs and develops policy for:
 - Emergency management
 - National security
 - Law enforcement
 - Corrections
 - Crime prevention
- Annual budget exceeds \$9 billion with approx. 63,000 employees

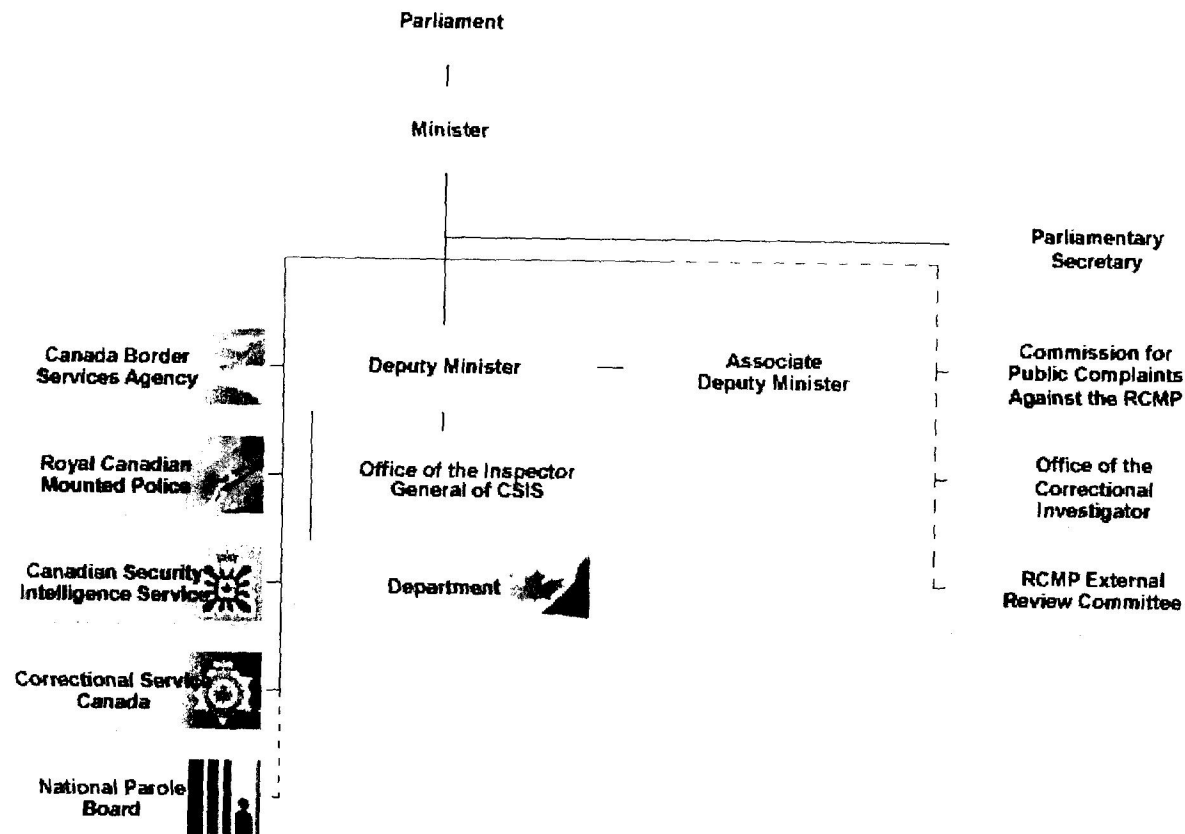


Public Safety
Canada

Sécurité publique
Canada

SECRET

Public Safety Portfolio



Public Safety
Canada

Sécurité publique
Canada

SECRET

Cyber Security – a Canadian Priority

- The National Security Policy 2004 recognized that cyber security was a major element of emergency management.

Cyber-security is at the forefront of the transborder challenge to Canada's critical infrastructure...

- Public Safety Canada was tasked with the development of Canada's Cyber Security Strategy.
- The Minister of Public Safety has stated
 - (cyber security) is almost a new arms race
 - developing a cyber security strategy is a priority for the Government
 - a national cyber security strategy will be completed this Fall



Public Safety
Canada

Sécurité publique
Canada

SECRET

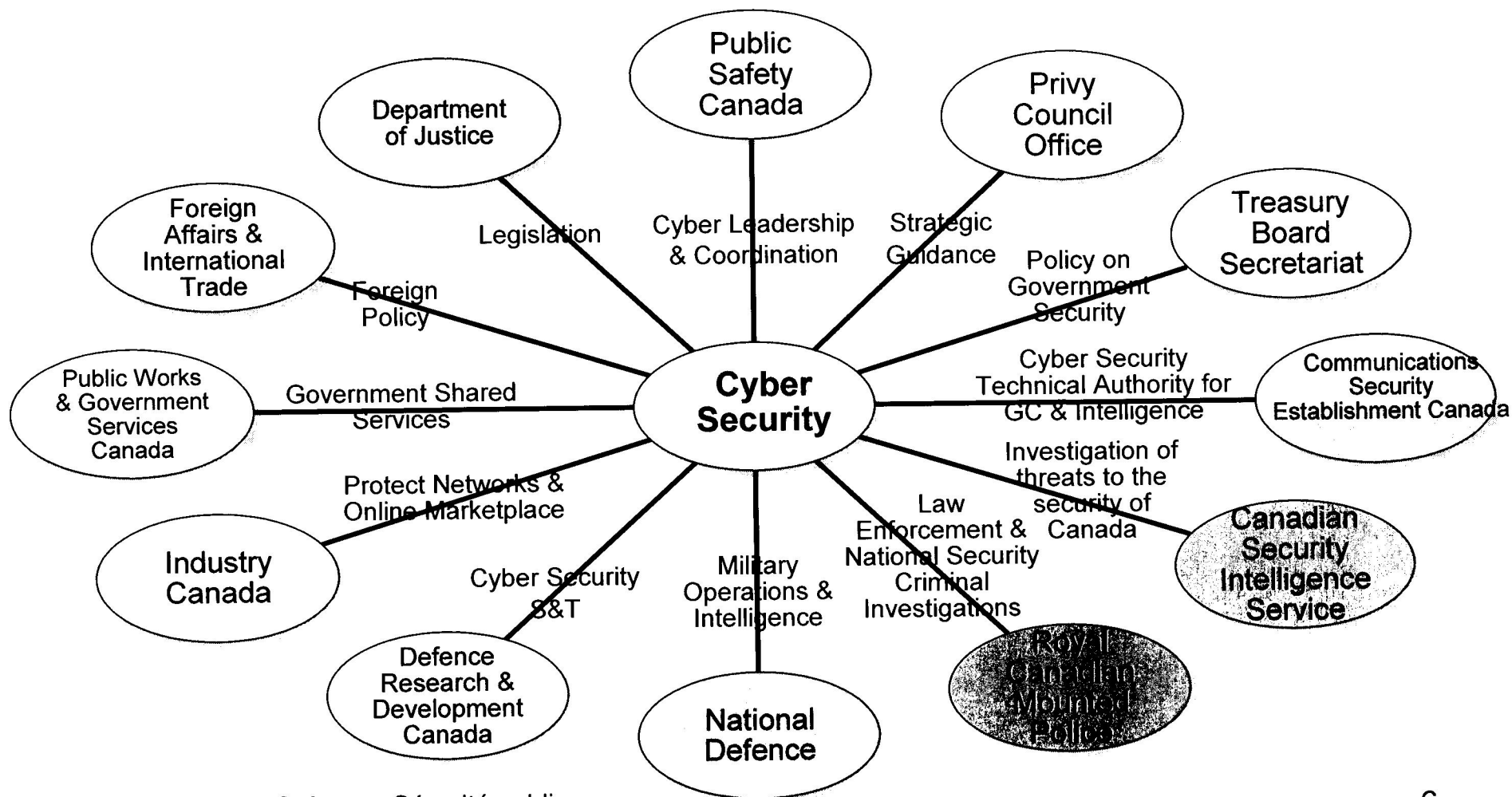
Progress to date

- Public Safety is leading inter-departmental efforts to develop a National Cyber Security Strategy.
- Work completed or underway includes
 - assessment of state of readiness in Canada's ten critical infrastructure sectors
 - development of a business case model for use by private sector to justify increased investment in cyber security
 - development of options for a made-in-Canada approach to information exchange between the government and the private sector
 - consultations and workshops with key private and public sector stakeholders
 - U.S., U.K., and Australian officials have been briefed on Canadian activities and are sharing their approaches



SECRET

Cyber Security – Community

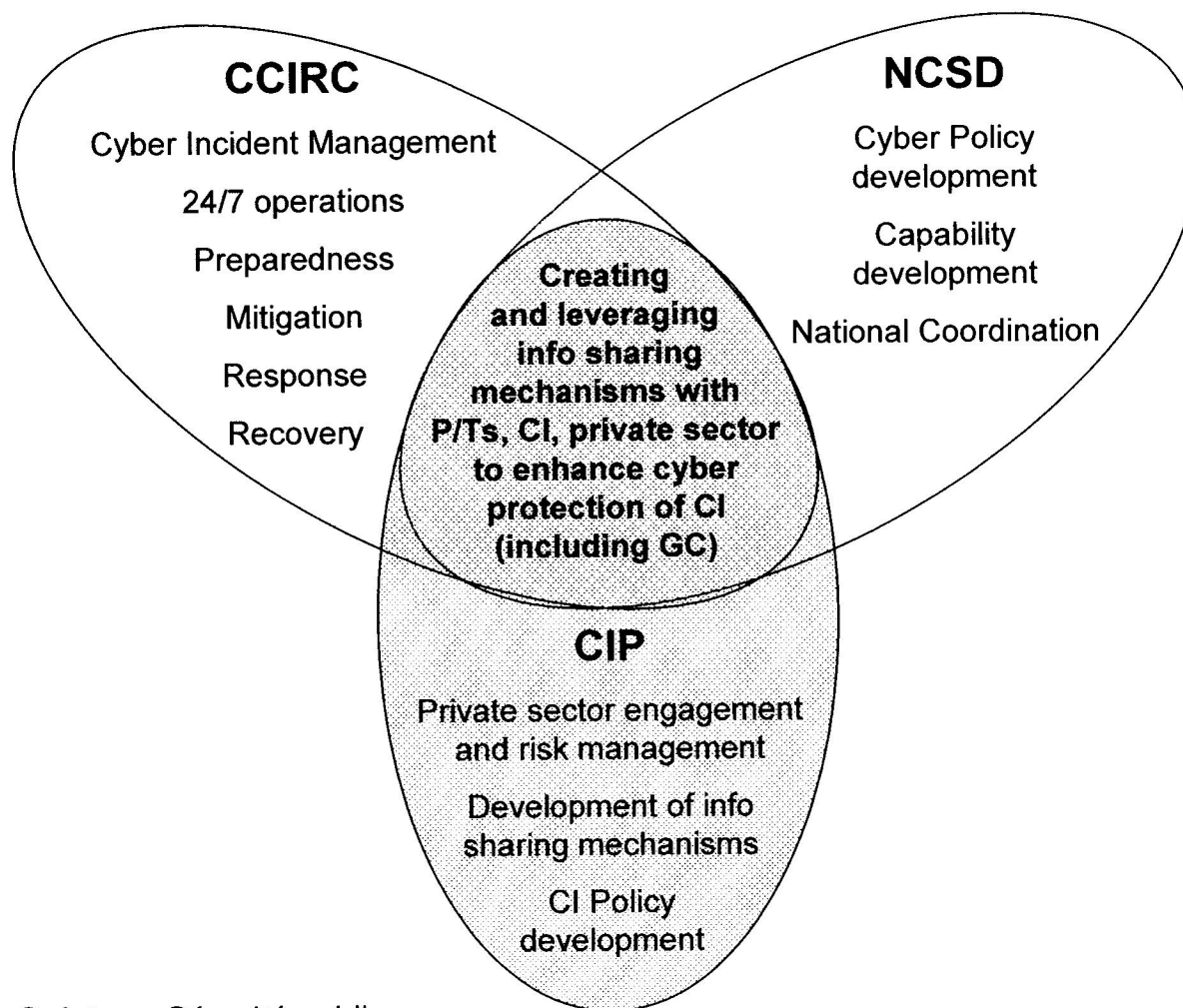


Public Safety
Canada

Sécurité publique
Canada

SECRET

Public Safety – Roles and Responsibilities

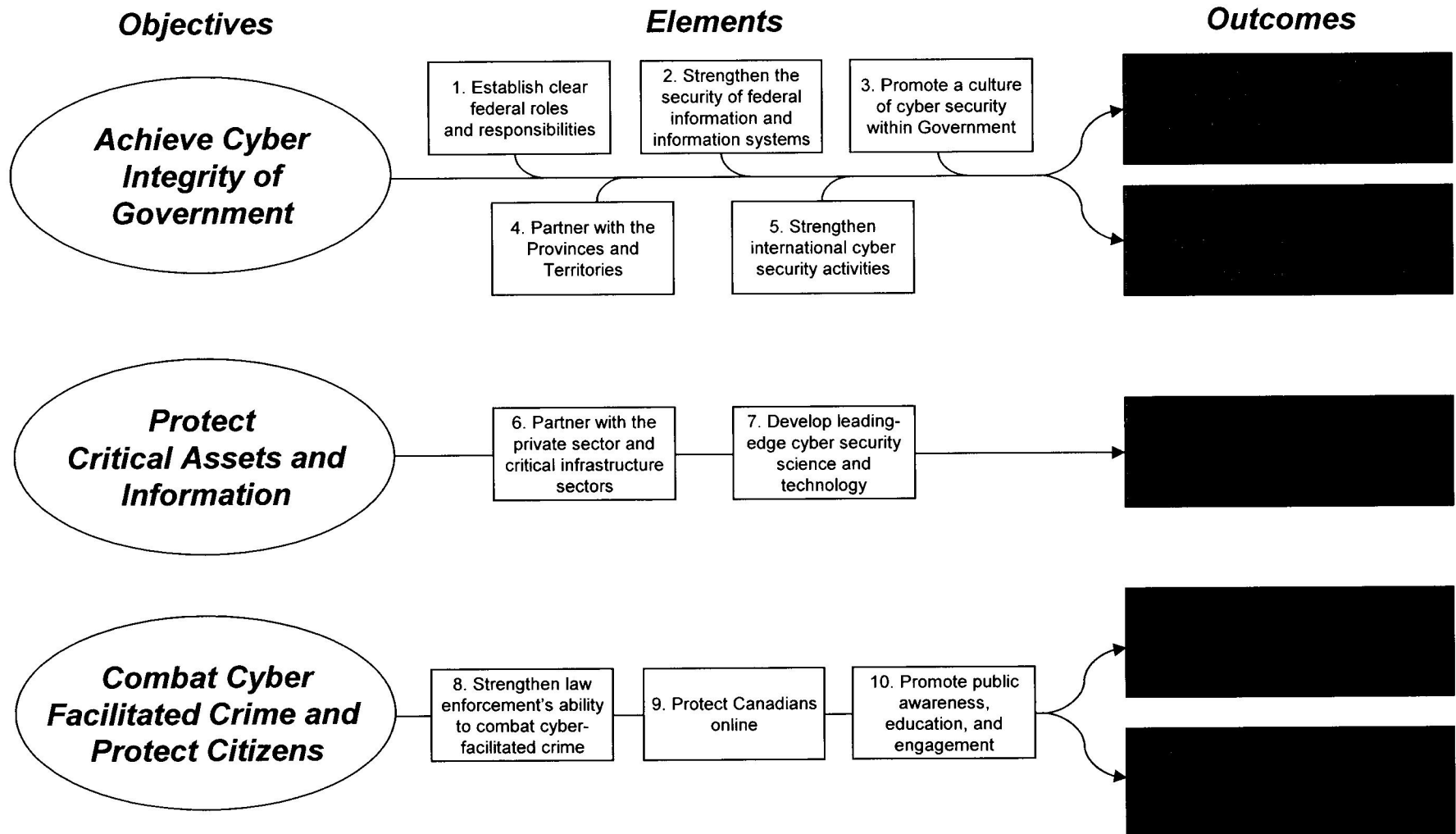


Public Safety
Canada

Sécurité publique
Canada

SECRET

Cyber Security For A Strong and Resilient Canada



SECRET

Cyber Challenges for Canada and United States

- The global cyber threat and threat actors are essentially the same for both countries
- Our societies are dependent upon information and information systems
- Electrons don't recognize borders
- Our critical infrastructure sectors are interconnected and interdependent
- Attacks on one CI sector risk bleeding into other sectors and across borders
- No one jurisdiction can fully address the issue
- Conclusion: The cyber threat is different than traditional threats – a new approach is required.



SECRET

What's different about the cyber threat compared with traditional threats?

- Attribution of who's attacking is difficult at best and most likely impossible
- The threat only manifests itself on the device you are trying to defend
- Scale becomes an issue – millions of devices to be defended
- Geography is a foreign concept in cyber space
- Much of what needs to be defended is owned and operated by the private sector

-
-

s.21(1)(a)

- Is a technical solution possible? People engineered the Internet and its infrastructure and some say we now know how to fix it
 - Should we influence the evolution of the structure?
 - There appears to be no venue for this discussion.



SECRET

What's different about the cyber threat compared with traditional threats? (cont'd)

- The ease of attacks is increasing.
- How do we take account of non-state actors?



SECRET

- NORAD has been a success – Why?
 - The focus has been very restricted
 - The geography and air space (the Border) to be defended is well defined and generally accepted internationally
 - General acceptance of traditional risks and responses domestically and internationally
 - Well known adversaries and potential attackers are usually easy to identify
 - Generally involves only state actors and response



**Pages 187 to / à 188
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

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