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

SECRET – with attachments

DM Cyber

January 12, 2012
14:00 to 15:00

19th floor boardroom
269 Laurier Avenue West

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

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

Deputy Ministers Committee on Cyber Security

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

AGENDA

	Time	Item	Associated Documentation
1.	14:00 *5 min*	**Opening Remarks** William Baker, Deputy Minister, Public Safety	N/A
2.	14:05 *5 min*	**Deputy Ministers Committee on Cyber Security** William Baker, Deputy Minister, Public Safety *For decision: Agree upon the proposed role and scope of the Committee; and discuss Committee forward agenda.*	Draft Terms of Reference
3.	14:10 *20 min*	**Network Hygiene** Michelle D'Auray, Secretary of the Treasury Board, Treasury Board of Canada Secretariat *For information: Provide an aperçu of the challenges in protecting Government IT systems, the actions taken to date, and forward work.*	Deck: Cyber Security – the Challenge in Protecting Government Systems
4.	14:30 *10 min*	**Cyber Security Roles and Responsibilities** Lynda Clairmont, Senior Assistant Deputy Minister, National Security, Public Safety Canada *For information: Provide an overview of the roles and responsibilities of cyber security lead departments.*	Roles and responsibilities dashboard
5.	14:40 *5 min*	[redacted]	
6.	14:45 *5 min*		
7.	14:50 *10 min*	**Roundtable**	N/A

s.14(a)
s.15(1) - International

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

Sécurité publique Canada | Public Safety Canada

NON CLASSIFIÉ

Comité des sous-ministres sur la cybersécurité

Le 12 janvier 2012 – 14h00 à 15h00
Salle de conférence au 19e étage du 269, avenue Laurier ouest

ORDRE DU JOUR

	Heure	Item	Documentation connexe
	14h00	**Mot de bienvenue**	
1.	*5 min*	William Baker, sous-ministre, sécurité publique	S/O
		Comité des sous-ministres sur la cybersécurité	
		William Baker, sous-ministre, sécurité publique	
	14h05	*Pour approbation : S'accorder sur le rôle et la portée du*	
2.	*5 min*	*comité; et discuter du programme d'activités à long terme.*	Stipulations proposées
		L'hygiène des réseaux	
		Michelle D'Auray, secrétaire du Conseil du Trésor, Secrétariat du Conseil du Trésor du Canada	Présentation : Le défi quant à la protection des systèmes gouvernementaux
	14h10	*Pour information : Donner un aperçu du défi quant à la protection des systèmes gouvernementaux, des efforts actuels*	
3.	*20 min*	*et des initiatives à venir.*	
		Rôles et responsabilités en cybersécurité	
		Lynda Clairmont, sous-ministre adjointe principale, sécurité nationale, sécurité publique	
	14h30	*Pour information : Donner une vue d'ensemble des rôles et responsabilités des ministères principaux en matière de la*	Tableau de bord sur les rôles et responsabilités
4.	*10 min*	*cybersécurité.*	
	14h40		
5.	*5 min*		
	14h45		
6.	*5 min*		
	14h50		
7.	*10 min*	**Tour de table**	S/O

s.14(a)
s.15(1) - International

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

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

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

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

#3

SSE

- troops issue - of insufficient troops - no silver bullet.
- longer term - Dutch troops still in dept
  - 43 out of 100 plus

[redacted]

R&R.

- how get C10s - that were not covering everyone.
- not everything is shared as how do we engage them

[redacted]

- a future agenda item.

- Dutch - pictorial reporting all sharing information.
  - necessity of sharing information.
  - more of a consultation point - more messaging

- perhaps a future item

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

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

s.15(1) - International

[redacted]

- even worst with Las esenin
— hopefully get some drinks

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

DM Cyber.

s.16(2)(c)

1. ~~Explain~~ how & why DM Cyber was created
   - need forum to ~~explore~~ ~~navigate~~ policy issues

2 - disc ~~as-is~~ re, membership
   - ~~re~~ to having other DMs join when necessary
   - ADM Cyber supports DM Cyber; DG Cyber supports ADM Cyber

3. - Rare Boucher pres.
   - comfortable w/ deck
   - comments re, creation of SSC
      - although building of SSC will take time, there are a couple of caveats — [redacted]
   - talked about # of the apps
   [redacted]
   - one problem w/ migrating to SSC: SSC will only be looking at 45 of the 100+ gov't agencies & depts - [redacted]
      - will not solve all problems but a lot of them
   - reinforce that patching in diversified env. not useful.
   - disc. re, can we be more forceful in delivering this msg? MAF, etc
   - branding of SSC - we (Govt) need to think about branding as not only an economic benefit, but also important to ensuring security
   - comments re, how to extend knowledge to other DMs
      - part of a broader level of understanding re, threat env.

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

4. - no problems w/ IS+S piece
- comment from SSC that they are not yet an equal player - but will be
- do a digram that gives better pictoral desc of why not sharing is important
don't incl. - try to show interdependencies

[redacted]

* - need to remind DG again about this

5. + SPK proposed in ~~brief~~ ADM package

[redacted]

- managing commitments & deliver expectations

[redacted]

6. [redacted]

7. - DM spoke to Fed Agenda: can FDS
- SIN awarches products
- SSC progress
- [redacted]
- IC to come back & speak to Digital economy Strat

* DM asked that DM/ADM/DG Cyber be added to dist list for Cyber Sec. Media Scan.

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

TAB 1

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

1. OPENING REMARKS

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

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

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

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

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

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

- Finally, there are two transactional items on which it is timely that we be briefed. [redacted]

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

s.14(a)
s.15(1) - International

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

TAB 2

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

2. DEPUTY MINISTERS COMMITTEE ON CYBER SECURITY

PROPOSED TALKING POINTS

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

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

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

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

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

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

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

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

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

ISSUE

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

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

CURRENT STATUS

Terms of reference

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

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

Membership

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

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

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

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

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

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

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

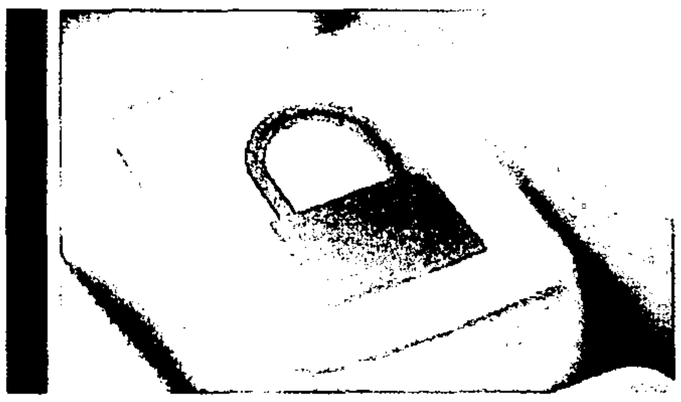
Prepared by: Melanie Mohammed
Approved by: Corey Dvorkin

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

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

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED
DRAFT



Deputy Ministers Committee on Cyber Security

Terms of Reference

Purpose

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

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

Membership

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

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

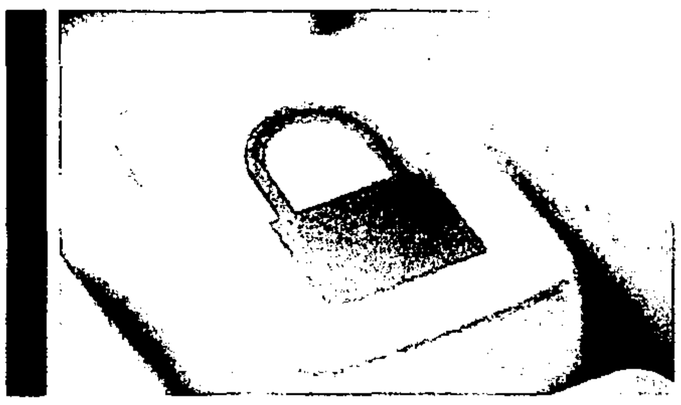
Governance / Relationship to other working groups and committees

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

Meeting frequency

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

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



Comité des sous-ministres sur la cybersécurité

Mandat

Objet

Le Comité des sous-ministres sur la cybersécurité vise à :

- orienter les politiques;
- établir les priorités;
- surveiller les progrès relatifs à la mise en œuvre de la *Stratégie de cybersécurité du Canada*;
- examiner les problèmes qui surviennent.

Membres

- Présidence et secrétariat :
  - Sous-ministre, Sécurité publique Canada

- Membres principaux :
  - Directeur, Service canadien du renseignement de sécurité
  - Commissaire, Gendarmerie royale du Canada
  - Sous-ministre, Défense nationale
  - Chef d'état-major de la Défense, Forces canadiennes
  - Chef, Centre de la sécurité des télécommunications du Canada
  - Sous-ministre, ministère des Affaires étrangères
  - Sous-ministre, Industrie Canada
  - Sous-ministre et sous-procureur général du Canada, Justice Canada
  - Conseiller national pour la sécurité auprès du premier ministre, Bureau du Conseil privé;
  - Président, Services partagés Canada
  - Secrétaire du Conseil du Trésor, Secrétariat du Conseil du Trésor

Structure de gouvernance et lien avec les autres groupes de travail et comités

Le Comité des SM est appuyé par le Comité des sous-ministres adjoints sur la cybersécurité, lui-même appuyé par le Comité des directeurs généraux sur la cybersécurité.

Fréquence des réunions

Le Comité des SM se réunira sur une base trimestrielle; le président pourra organiser des réunions au besoin.

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

TAB 3

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

3. NETWORK HYGIENE

PROPOSED TALKING POINTS

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

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

During discussion

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

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

- Can we work more collaboratively to expedite this process?

ISSUE

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

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

BACKGROUND

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

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

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

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

CURRENT STATUS

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

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

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

NEXT STEPS

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

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

CSEC has also prepared a list of the top ten mitigating actions for proper network hygiene that can provide direction and clarity to Deputy Heads.

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

CONCLUSION

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

Prepared by: Melanie Mohammed
Approved by: Adam Hatfield

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

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

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

Better government with partners for Canadians

SECRET

Cyber Security

The Challenge in Protecting Government Systems

Canada

Agenda

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

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

SECRET

Cyber Threat Landscape

Opportunistic

SIMPLE

SOPHISTICATED

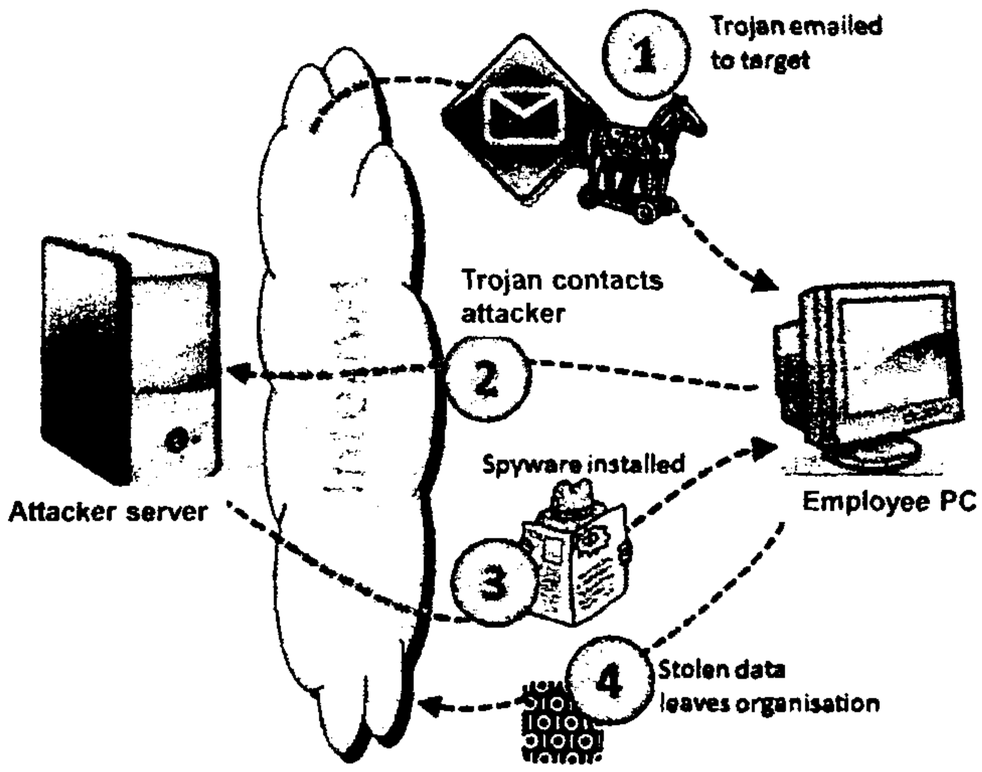
Planned

- Hackers and Hacktivists
  - Motivation: Social/political
  - Target: Organizations promoting political and/or societal positions
  - Methods: Website defacement, denial of service
  - Techniques: Exploitation of common software vulnerabilities
- Criminals
  - Motivation: Profit
  - Target: Canadian citizens, retailers, financial sector
  - Methods: Social engineering to send malicious emails to groups of people, exploitation of common software vulnerabilities, establishment of fake websites
- State Sponsored
  - Motivation: Political, military, economic advantage
  - Target: Government, academia, industry, critical infrastructure
  - [redacted]

3

SECRET

Typical Attack Scenario



4

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

s.15(1) - Subversive

s.16(2)(c)

SECRET

Cyber Defence is a Challenge

- [redacted]
- People are also targets - it can be hard for a user to detect malicious emails
  - Adversaries use social engineering techniques to trick people into believing the malicious email or attachment is valid and important to them
- Sophisticated attackers constantly probe and persist until they succeed, exploiting any weaknesses in our defences, scaling from most common and well known vulnerability to the most complex methods and non-public vulnerability.
  - Constantly harvesting data (network and human behaviour) for future exploitation.
  - [redacted]

5

need an organized network & response to the suggested solution

SECRET

[redacted]

3

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

s.15(1) - Subversive

s.16(2)(c)

s.21(1)

SECRET

What We Have Done To Date

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

7

SECRET

Moving Forward

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

- Creation of SSC
  - Game changer: significant impact on our consolidation effort
  - Consolidating and standardizing Enterprise IT Architecture
  - Increasing operational excellence at the enterprise level
  - Standing up a Gov-CIRT at SSC
- [redacted]
- Security awareness: changing behaviour

8

network
data centre
email

- partly offset in a shrinking environment.

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

SECRET

Consolidation is a Prerequisite for Sustainable Network Hygiene

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

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

9

SECRET

ANNEX

10

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

SECRET

Network Hygiene – Top 10 Mitigating Actions*

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

** Extracted from CSEC Top 35 Mitigation Actions*

11

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

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

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

Un meilleur gouvernement avec nos partenaires, pour les Canadiens

SECRET

Cybersécurité

Le défi associé à la protection des systèmes gouvernementaux

Canada

Ordre du jour

- Disposition des menaces
- Ce que nous faisons
- La voie de l'avenir
- Conclusions

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

s.15(1) - Subversive

SECRET

Disposition des cybermenaces

Opportuniste

SIMPLE

SOPHISTIQUÉ

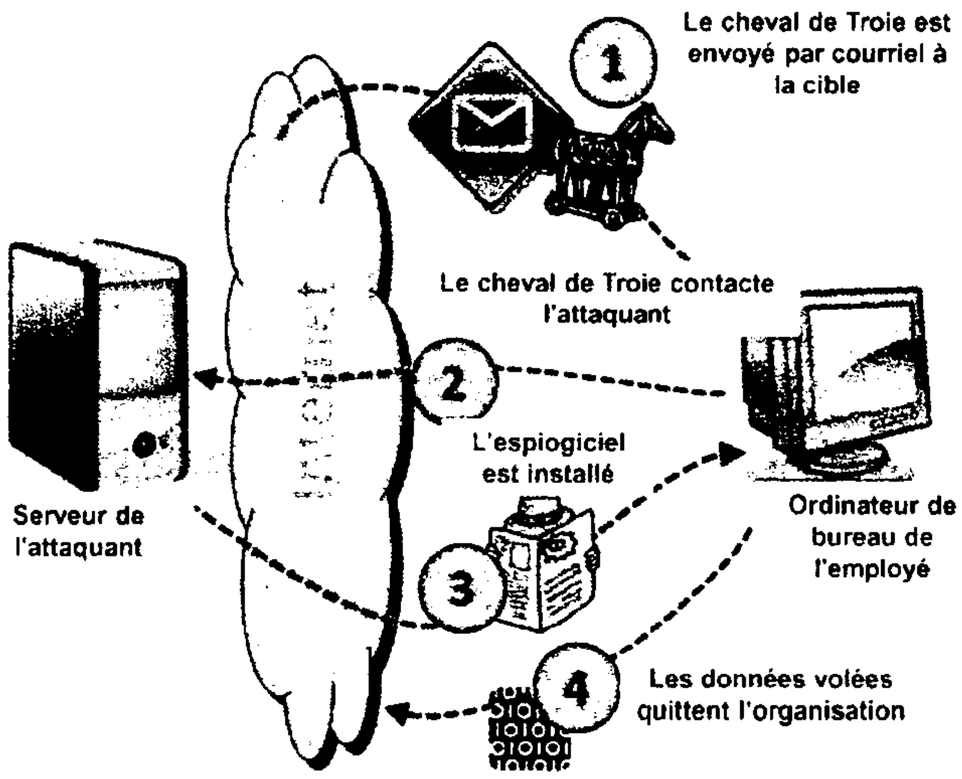
- Pirates informatiques et hacktivistes
  - Motivation : De nature sociale ou politique
  - Cibles : Organisations faisant la promotion des positions politiques ou sociales
  - Méthodes : Altération des sites Web, refus de service
  - Techniques : Exploitation des vulnérabilités communes des logiciels
- Criminels
  - Motivation : Profit
  - Cibles : Citoyens canadiens, détaillants, secteur financier
  - Méthodes : Ingénierie sociale envoyant des courriels malveillants aux groupes de personnes, exploitation des vulnérabilités communes des logiciels, création de faux sites Web
- Appuyé par l'État
  - Motivation : Avantage politique, militaire ou économique
  - Cibles : Gouvernement, milieu universitaire, industrie, infrastructure essentielle
  - [redacted]

Prévu

3

SECRET

Scénario type d'attaques



4

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

s.15(1) - Subversive

s.16(2)(c)

SECRET

La cyberdéfense représente un défi

- [redacted]
- Les personnes sont également des cibles; il peut être difficile pour un utilisateur de détecter des courriels malveillants
  - Les adversaires emploient des techniques d'ingénierie sociale pour amener des personnes par la ruse à croire que le courriel ou la pièce jointe malveillant est valide et qu'il est important
- Les attaquants subtils examinent et persistent constamment jusqu'à ce qu'ils réussissent, en exploitant toute faiblesse dans nos défenses, allant des vulnérabilités les plus communes et les plus connues jusqu'aux méthodes les plus complexes et profitant des vulnérabilités non publiques.
  - Récolte constante des données (réseau et comportement humain) aux fins d'exploitation future
  - [redacted]

5

[redacted]

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

s.15(1) - Subversive

s.16(2)(c)

s.21(1)

SECRET

Ce que nous avons fait à ce jour

- Évaluation de la conformité à la sécurité de la TI par l'entremise du CRG (2006)
  - Amélioration de la conformité
  - Sensibilisation incluant les pratiques de base d'hygiène de réseau
- Le SCT menant la consolidation des points d'accès Internet
  - Réduction d'un tiers depuis 2009
  - Le SCT a défini clairement les configurations acceptables et inacceptables (2011 montre que 80 % des configurations sont acceptables)
  - .Permet le déploiement rentable des solutions de défense

[redacted]

7

SECRET

Aller de l'avant

Le SCT continue de défendre les initiatives qui soutiennent la consolidation et la rationalisation de l'infrastructure de la TI

- Création du SPC
  - Point tournant : une grande incidence sur nos efforts de regroupement
  - Regroupement et normalisation de l'architecture de TI d'entreprise
  - Hausse de l'excellence opérationnelle à l'échelle de l'entreprise
  - Création d'une équipe de réaction aux cyberincidents du gouvernement au SSC
- [redacted]
- Sensibilisation à la sécurité : Modifier le comportement

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

SECRET

Le regroupement est un prérequis au bien-être durable de réseau

- Le gouvernement du Canada doit lutter contre tous les aspects de la cybermenace, y compris la menace la plus ingénieuse
- L'infrastructure de TI du gouvernement est complexe, massive et hétérogène et les anciens systèmes y abondent toujours
- La mise en œuvre de la mesure la plus simple représente un défi opérationnel et technique. Un effort global en matière de sécurité dans un tel environnement est complexe, risqué et coûteux
- Afin que le bien-être de réseau soit efficace, nous avons besoin d'une infrastructure de réseau simplifiée et plus cohérente
- Nous nous attaquons au problème par le truchement d'initiatives qui réduiront la complexité, augmenteront l'homogénéité de TI et réduiront l'empreinte de notre infrastructure
- Même avec un réseau simple et cohérent, il est nécessaire de déployer un effort soutenu afin de veiller à ce que les gens assument un comportement sécuritaire conscient, tant à l'échelle des employés que de la gestion

Nous tirerons profit des initiatives de regroupement actuelles afin de créer une infrastructure de TI d'entreprise cohérente, résiliente et sécuritaire

9

SECRET

ANNEXE

10

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

SECRET

Hygiène de réseau – 10 principales mesures d'atténuation*

1. Rapiécer rapidement les systèmes d'exploitation
2. Rapiécer les applications (visualiseur PDF, navigateur, applications bureautiques)
3. Minimiser l'utilisation des privilèges de l'administrateur
4. Application « liste blanche » pour prévenir les programmes malveillants
5. Système de détection et de prévention d'intrusion géré par le système central
6. Inspection du poste de travail des fichiers Microsoft Office
7. Filtrage du contenu des courriels de la liste blanche pour bloquer les pièces jointes malveillantes
8. Éducation des utilisateurs sur les risques de l'Internet, ingénierie social
9. Vérifier que l'acheminement de l'achalandage interne ne sort pas du réseau
10. Outils pour prévenir l'exécution du code malveillant

* *Extrait des 35 principales mesures d'atténuation du CSTC*

11

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

TAB 4

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

4. CYBER SECURITY ROLES AND RESPONSIBILITIES

PROPOSED TALKING POINTS

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

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

ISSUE

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

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

BACKGROUND

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

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

CONSIDERATIONS

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

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

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

A series of tabletop exercises beginning January 13, 2012, will help to provide the necessary clarity, and identify policy and operational barriers to information sharing. Additionally, these exercises will contribute to Public Safety Canada's initiative to establish a national cyber incident response framework. This framework would clarify the roles and responsibilities of Government, provincial and territorial partners, and private sector entities. s.16(2)(c)

CONCLUSION

It is expected that the current dashboard, along with the exercises, will provide a better understanding of cyber security roles and responsibilities.

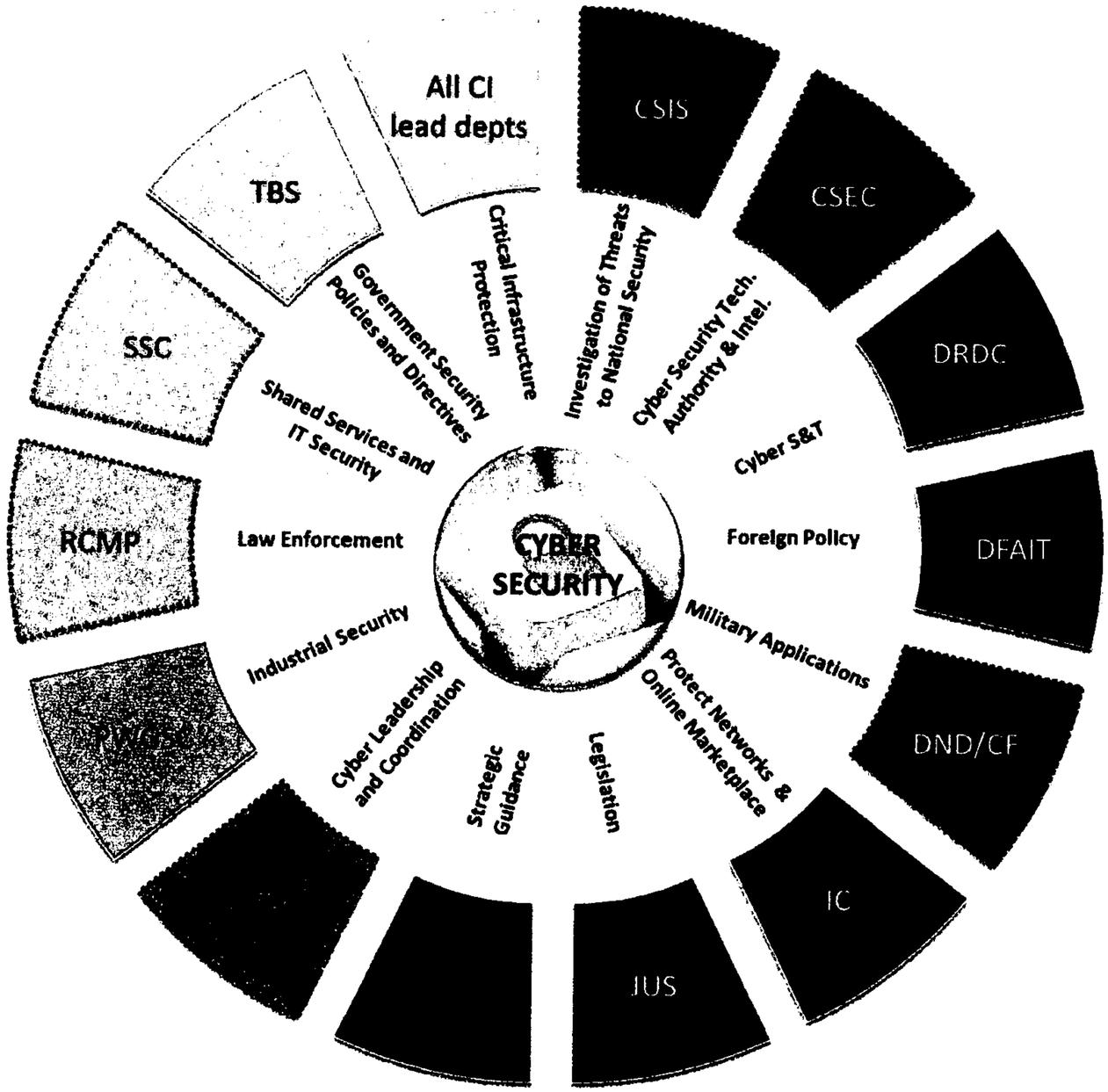
There is potential for synergy between Public Safety Canada efforts, and ongoing efforts by the Treasury Board of Canada Secretariat (TBS) to revise the GC IT IMP. We are open to coordinating with TBS so that one set of exercises could help inform our respective efforts.

Prepared by: Melanie Mohammed
Approved by: Corey Dvorkin and Adam Hatfield

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

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

Roles and responsibilities with respect to cyber security



Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

#534168

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

All critical infrastructure lead departments
Includes Finance Canada, Environment Canada, Health Canada, Transport Canada, Natural Resources Canada, Agriculture and Agri-Food Canada, and Public Safety Canada.

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

Shared Services Canada
Streamlines and consolidates ICTs in the areas of email, data centres and networks, and for ensuring the confidentiality, integrity and availability of common IT services provided to departments.
Provides common information technology (IT) security services and other solutions to enable departments to exchange information with citizens, businesses and employees.
Gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to common IT services and Government IT critical infrastructure managed by Shared Services Canada, and communicates the information to the Canadian Cyber Incident Response Centre and, as authorized, to departments and cyber security partners.

Royal Canadian Mounted Police
Leads the criminal investigative response to suspected criminal cyber incidents involving critical information infrastructure (i.e., unauthorized use of computer and mischief in relation to data). Leads the investigative response to suspected criminal national security cyber incidents.
Assists domestic and international partners with advice and guidance on cyber crime threats.

Public Works and Government Services Canada
Provider of shared and common services. As part of its Industrial Security Program activity, ensures security in contracts awarded by the Department or when requested by other Government departments.
Ensures the protection of foreign and NATO classified information within the private sector in Canada.
The Industrial Security Sector maintains relationships with allies and negotiates Memoranda of Understanding on industrial security matters, including cyber security, in contracting.

Public Safety Canada
Leads and coordinates the implementation of *Canada's Cyber Security Strategy*, including the design of a whole-of-Government approach to performance measurement and reporting; engagement with provinces and territories, critical infrastructure, and international allies on strategic cyber security policy issues and national cyber incident management; and public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace.
The Canadian Cyber Incident Response Centre acts as Canada's national CERT (Computer Emergency Response Team) in providing assistance and mitigation advice to domestic partners and coordinating the national response to any cyber security incident.

Privy Council Office
Houses and provides support to the National Security Advisor to the Prime Minister.
Coordinates activities among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to national security issues.

Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

Communications Security Establishment Canada
Monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government through its sensor network, and provides mitigation and/or recovery advice and/or guidance to Government departments to help them recover from cyber incidents.
Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the Five Eyes cryptologic community. Undertakes classified research and development for cyber security.

Canadian Security Intelligence Service
Conducts national security investigations, reports to and advising the Government of Canada of activities constituting a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act*.
Provides analysis that will assist the Government of Canada in understanding cyber threats, the actors behind those threats, and overall situational awareness enabling the Government of Canada to better identify cyber vulnerabilities and take action to secure critical infrastructure, prevent cyber espionage or other related cyber threat activity.

Defence Research and Development Canada
Leads the development of military cyber security S&T in support of the Canadian Forces.
Leads domestic Public Safety Canada cyber security S&T efforts not specifically assigned to another department or agency through the Centre for Security Science and with domestic security partners in the Public Security Technical Program. This is delivered in partnership between Government, industry, academia and allies.

Department of Foreign Affairs and International Trade
Supports international bodies in mitigating cyber threats and assisting foreign governments in improving their cyber security profile and capabilities.
Contributes to diplomatic engagement in order to help shape the multilateral regulatory space that is emerging with respect to cyber security. Enables the Government to better position Canada on the international stage to defend and promote its foreign policy and cyber security-related interests.

Department of National Defence / Canadian Forces
Responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process.
Contributes to Government situational awareness during the monitoring and analysis, mitigation, and response phases of the *GC IT IMP* by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

Industry Canada
Responsible for spectrum management in Canada and for fostering a robust and reliable telecommunications system. Develops policies to ensure a safe and secure online marketplace. Helps to ensure the continuity of telecommunications during an emergency.

Department of Justice Canada
Supports initiatives of client departments and agencies through the provision of legal advice on matters relating to cyber policy and law.
In respect of certain matters, especially those relating to criminal law policy and information sharing, Justice plays a leading role. Departmental Legal Services within the Communications Security Establishment Canada had been designated as the centre of excellence on cyber-related legislation.

#534168

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

TAB 5

Pages 46 to / à 47

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - International

of the Access to Information

de la Loi sur l'accès à l'information

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

Pages 49 to / à 50

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - International

of the Access to Information

de la Loi sur l'accès à l'information

Pages 85 to / à 95

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - International, 16(2)(c), 21(1)(a), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

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

PUBLIC SAFETY – CSEC MEMORANDUM OF UNDERSTANDING SUMMARY OF PROPOSED ROLES AND RESPONSIBILITIES

A great deal of the protocol and procedure for responding to a significant event with broad government implications already exists within the Federal Emergency Response Plan (FERP) and the Government's Information Technology Incident Management Plan (IT IMP). Transitioning to CSEC the responsibility for cyber incident response on GC networks and systems will require a review and changes to the IT IMP to ensure that CSEC's role in cyber incident management is well coordinated with broader Government response mechanisms identified in the FERP.

The Memorandum of Understanding will propose the following:

- CSEC would be responsible for cyber incident response for Government networks and systems, including the provision of mitigation advice and the issuance of alerts and notifications to the Government community. CSEC would develop Government-wide cyber situational awareness for the use of the Government clients, in particular PS. As defined in the IT IMP, CSEC would escalate cyber incidents that meet established trigger criteria to the multi-agency Cyber Triage Unit chaired by PS for further evaluation, escalation, and federal response and coordination as needed.

- PS would have three roles.
  - Per the FERP and the IT IMP, PS would continue to be responsible for ensuring a cohesive whole-of-government response to a cyber incident, including managing the escalation process from the Cyber Triage Unit to senior management. The IT IMP provides for interdepartmental engagement at the Director General and Assistant Deputy Minister levels prior to advising Deputy Ministers to ensure that a whole-of-government perspective is reflected. This includes an assessment of the impact, communications issues, possible diplomatic consequences, and law enforcement, military, and national security implications.
  - PS would be the <u>national</u> cyber incident management centre and responsible for cyber incident management for non-Government networks and systems (e.g. provincial and territorial governments, critical infrastructure, the public, industry, non-government organizations, other cyber emergency response organizations, and academia) and developing cyber situational awareness for the nation, taking into account the CSEC Government cyber situational awareness. This is a role that is technically PS' today but would be strengthened following the transition.
  - PS Communications would be the Government lead for messaging to the media and the public on cyber security issues to ensure the federal and national messages are aligned. This role is defined in the FERP, the IT IMP, and in *Canada's Cyber Security Strategy*.

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

Completing the MOU and obtaining agreement that these processes will be used will clarify roles and responsibilities and ensure that future events are handled with more clarity.

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

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Communications Security Establishment Canada

Cyber Threats and Cyber Security

Federal, Provincial, Territorial Clerks

January 23, 2012

SECRET

Canada

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

Overview

- About CSEC and our Mandates
- Overview of the Cyber Threat Environment
- CSEC Cyber Defence Capabilities & Programs
- Cyber Best Practices
- Discussion

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

CSEC's Mandate

National Defence Act

- **Part A:** Provide foreign intelligence in accordance with government priorities
- **Part B:** Provide advice, guidance and services to protect information and information systems of importance to the GC
- **Part C:** Provide technical assistance to law enforcement and national security agencies

Cyber is our core mission and core competency; developed over 65 years

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

CSEC's Cyber Role

- Our Focus
  - [redacted]
  - The federal government
    - GC Cyber Threat Evaluation Center
  - Key partners: CSIS, RCMP, Public Safety Canada, International Partners (US, UK, Aus, NZ)

- Other Government Departments
  - [redacted]
  - Public awareness

[redacted]

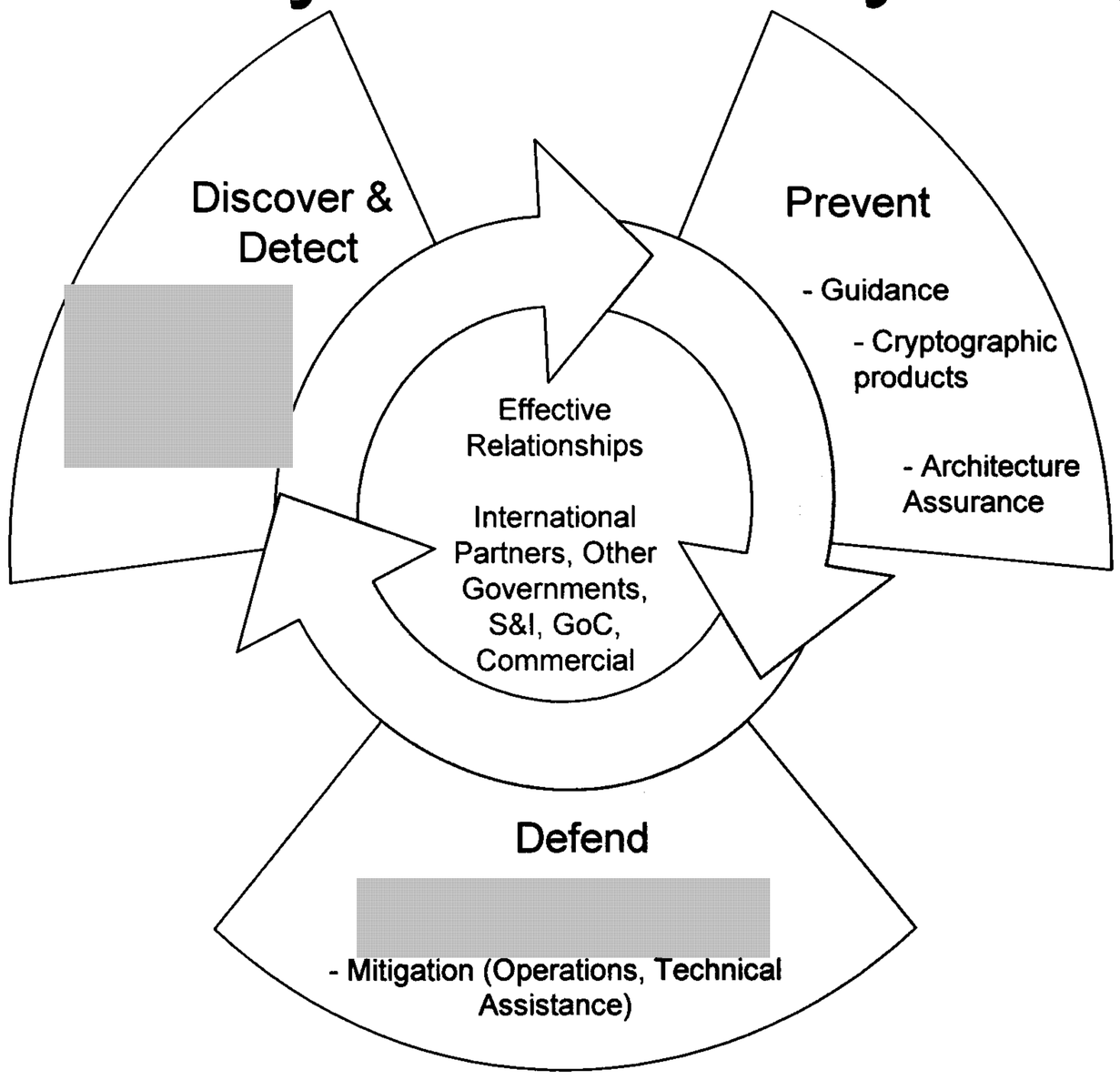
CSEC information and expertise is leveraged for above initiatives

Canada

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

CSEC Cyber Security Programs

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



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

The Cyber Environment

Where we work and play
Where we store our wealth and treasure

- 2 Billion Internet users (est. 10 to 15 B by 2015)
  - 107 Trillion emails daily
  - 300 Billion web sites
  - 700 Million on Facebook

- Heavy reliance on IT by citizens, business and government
  - >130 GC services on-line
  - >85% Canadians on-line
  - $16 Billion on-line sales in Canada in 2010; doubled by 2015; $412 Billion global sales
  - 3 Trillion records transfers daily – Bank of NY

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

The Cyber Environment

s.15(1) - Defence

Where information and wealth is exploited

- IT systems and networks are lucrative targets
  - 86% of large commercial organizations self-reported attacks
  - Cybercrime losses, globally $100 Billion est.
  - In Canada $2.5 B est. expenditure by companies suffering IT security breaches
  - Intellectual property: US estimate $1 Trillion loss
    - [redacted]

A new piece of malware is created every 1.5 seconds*

**Source – Trend Micro, Trend Micro Annual Report: Future of Threats and Threat Technologies, 2009*

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

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

The Cyber Environment

Where information and wealth is exploited

- 1 in every 284 emails contains malware
- 1 in every 192 emails contains a phishing attempt
- 95 Billion phishing emails in 2010
- Legitimate web sites hosting malware: 3200 identified daily
- Botnets can deliver 3-4 million new infections per month

Phishing Defined...

An email sent to broad audience to allow for the delivery of malware

Messages contain socially engineered text designed to appear legitimate and trustworthy.

Symantec Reports:

2008: 1.6M new threat signatures

2010: 6M new threat signatures

McAfee Reports:

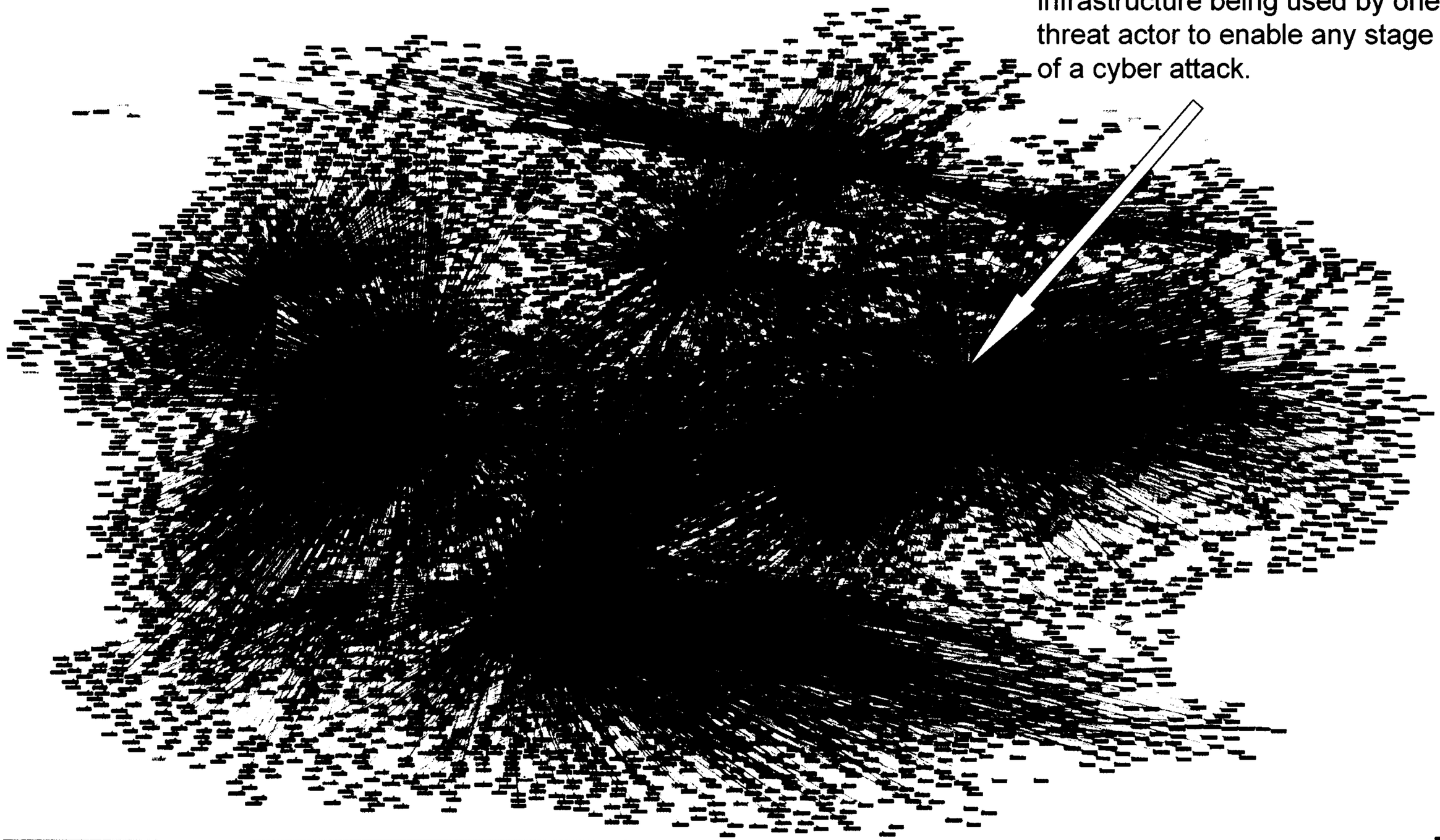
>60 million pieces of malware

Canada

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

BOTNET

Each one of these blue areas is the node of an attack network infrastructure being used by one threat actor to enable any stage of a cyber attack.



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

Who's Out There?

- **State espionage and warfare**
  - 100 Nations with cyber exploitation capabilities
- Organized Crime
  - Identity theft
  - Electronic bank heists
  - Illicit trade
- Terrorist Networks
  - Recruitment / propaganda
  - Financing
  - Planning
- Low level Actors
  - Thrill seekers
  - Hacktivists

Cyber Threat Attributes

- Inexpensive
- Basic skills can cause much damage
- Attack detection and attribution difficulty increases as attack sophistication increases

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

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

GC Response to Threat Environment

Canadian Cyber Security Strategy (CCSS)

Achieve cyber integrity of government

Protect Critical Assets and Information

Combat cyber facilitated crime and promote public awareness

To strengthen Canada's national security and contribute to global security

To sustain Canada's economic prosperity

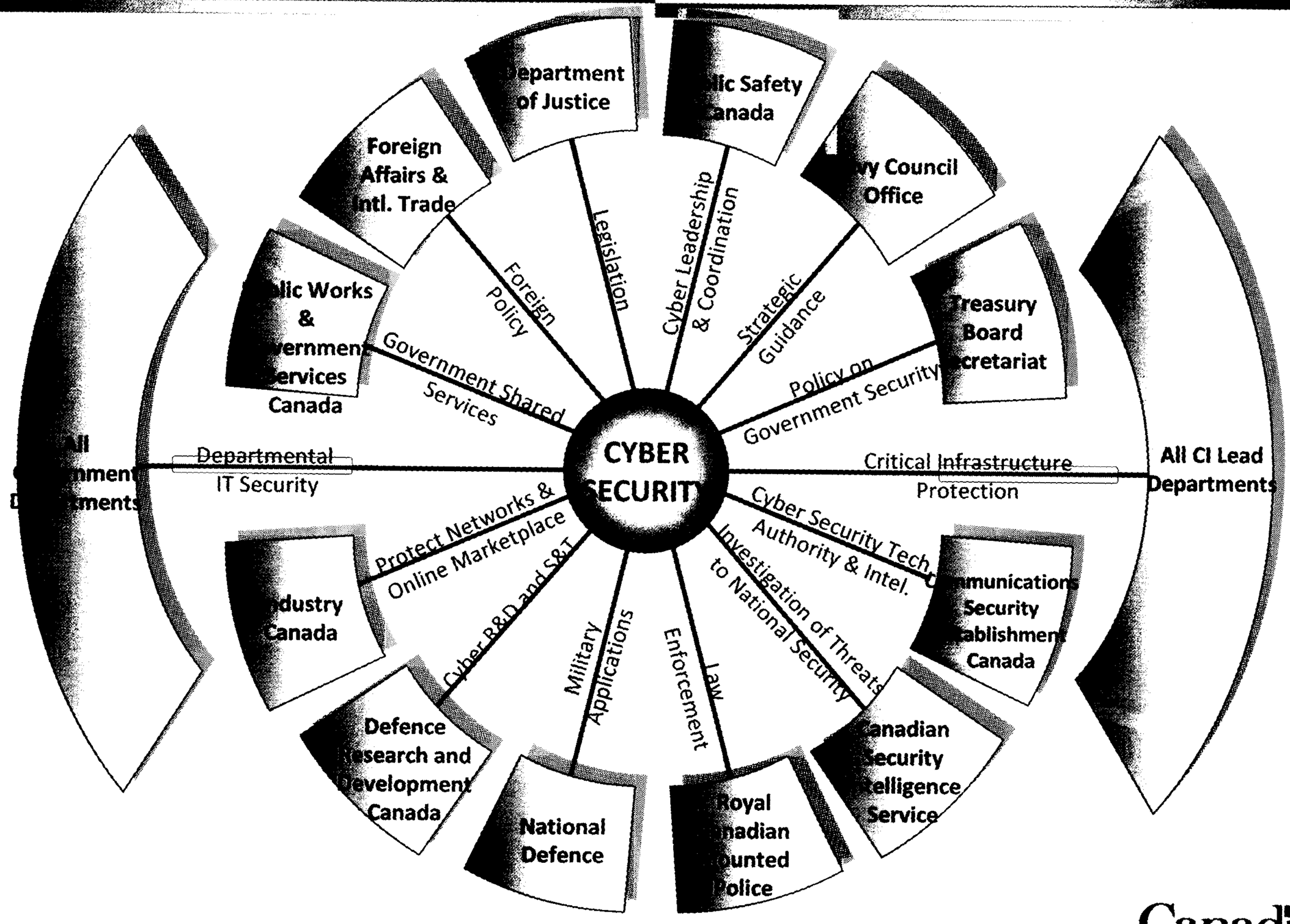
To protect Canadian citizens on line

October 2010

Canada

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

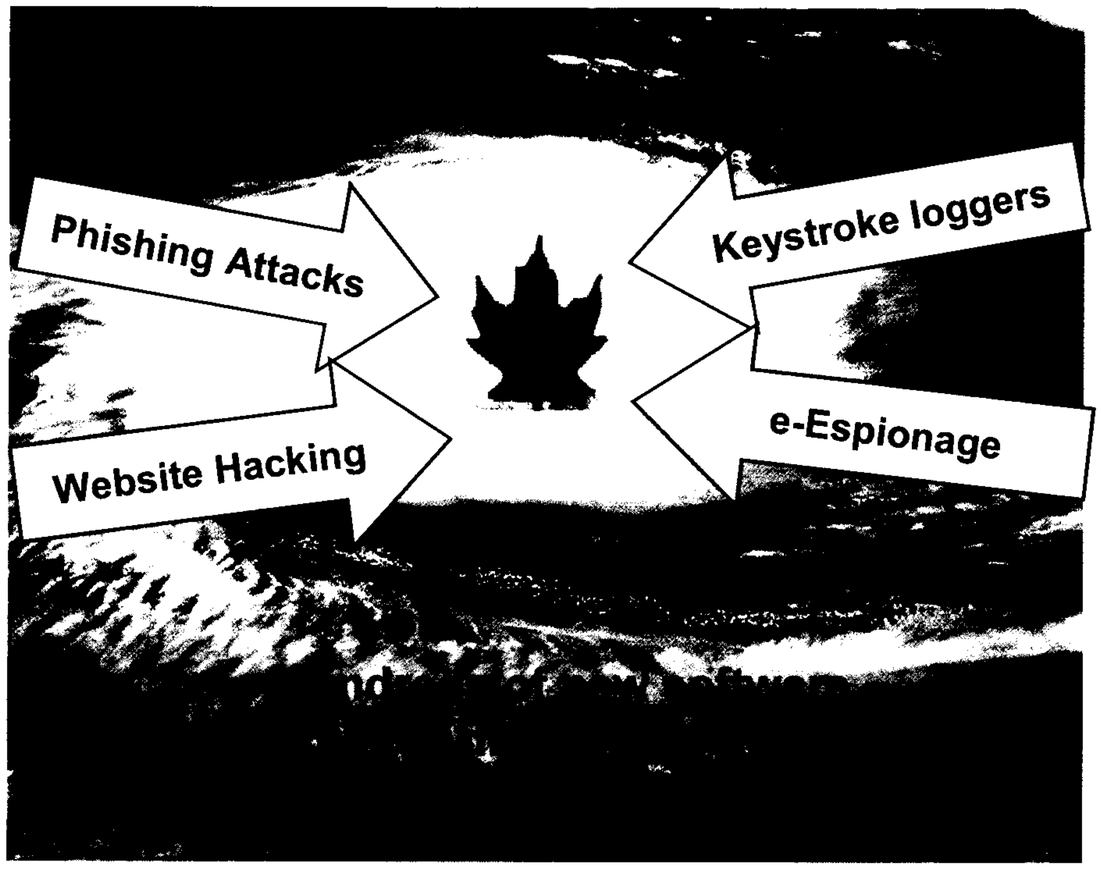
Shared Responsibility



Canada

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

How Vulnerable is the GC?



TBS/CIOB Survey Report:

- [redacted] unique Internet access points, and counting
- Driving the need for Internet Access Point Consolidation (SCNET)

GC Example:

- Cyber Response: TBS-FIN

Canada

Page 151

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - Defence, 16(2)(c)

of the Access to Information

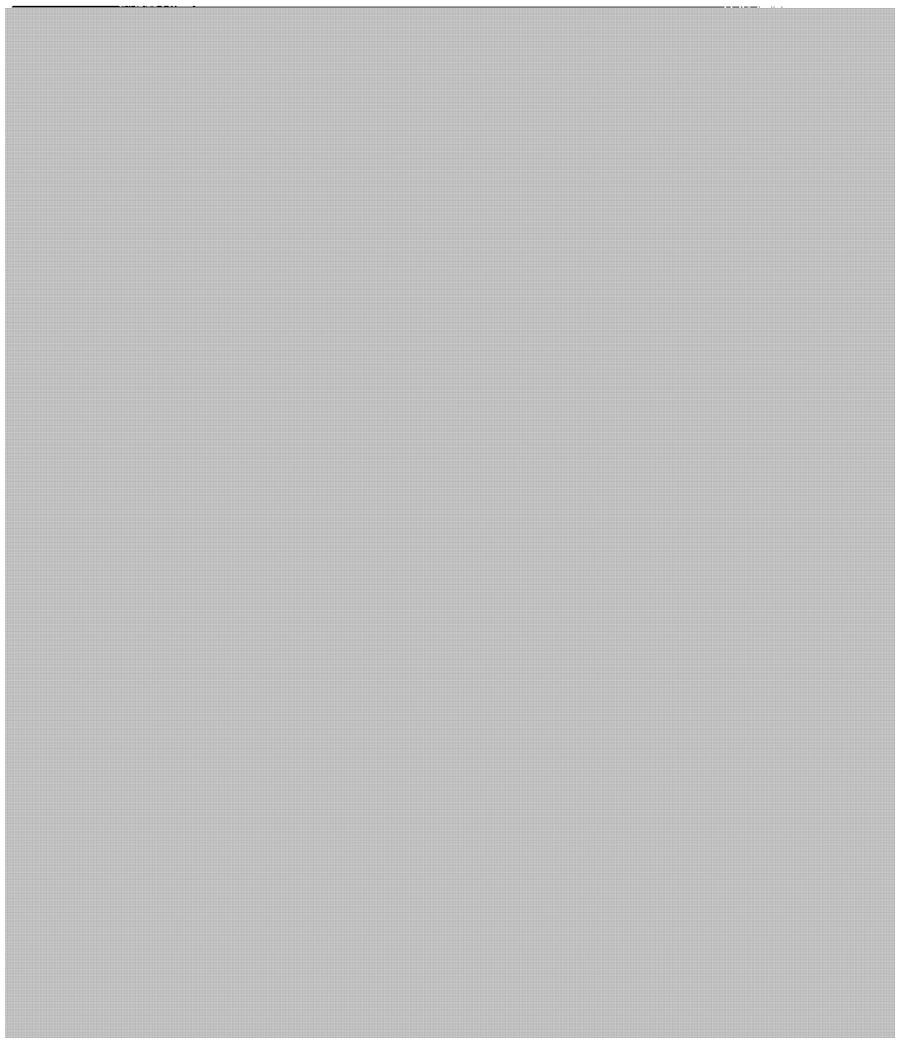
de la Loi sur l'accès à l'information

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

s.15(1) - Defence
s.16(2)(c)
s.21(1)(a)

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Steps to Increasing IT Security



Cyber Security Best Practices

1. Consolidate internet traffic
2. Patch IT systems to combat vulnerabilities
3. Whitelist safe internet browsing
4. Limit local administration privileges
5. Increase user awareness of current cyber threats

Canada

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

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Will that make them go away? - NO

Cyber Realities

- [redacted]
-
-

Addressing the Challenge

- [redacted]
-
-

There is no Silver Bullet

Advanced persistent threats, such as state-sponsored cyber espionage, will continue

Need persistent vigilance and monitoring

Invest in continuous collaboration with key stakeholders across all levels of government

Canada

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

Cyber Security Collaboration

Federal, Provincial and Territorial

- Continuous collaboration is essential for the advancement of cyber security
- Public Safety Canada / CCIRC is the cyber incident reporting gateway for Provinces, Territories and Critical Infrastructure stakeholders
- CCIRC coordinates and shares pertinent cyber threat information from multiple departments including CSEC/CTEC
- Timely reporting of incidents is a key component of Canada-wide response efforts from a cyber perspective

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

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Discussion

Canada