Public Safety Canada | Sécurité publique Canada

Assistant Deputy Minister | Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

Seen by the DM
Vu par le SM

OCT 19 2012

DATE: SEP 25 2012

File No.: 390355
RDIMS No.: 693315

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

A JOINT PUBLIC SAFETY CANADA / COMMUNICATIONS SECURITY ESTABLISHMENT CANADA PRESENTATION TO PSMAC

(For Information)

ISSUE

Public Safety Canada (PS) and the Communications Security Establishment Canada (CSEC) will make a joint presentation to Public Service Management Advisory Committee (PSMAC) in October on the risk management approach used by PS to operationalize a secure use of iPAD in the department.

BACKGROUND

PS initiated a pilot project to use the iPAD in completing daily activities, including attending meetings, managing documents, presentations and email, with access to the department's corporate Protected B network. This pilot was initiated to demonstrate a modern government approach through the implementation of a paperless office concept that also promotes Workplace 2.0.

PS followed CSEC direction in using a risk-management approach to implement the iPAD as a secure, modern and efficient work tool. This joint presentation will explain this approach which can be used by all departments. The approach, which can be used by all departments, recognizes the mandate and priorities of each department while applying security controls that enable client and operational needs.

The presentation and PSMAC briefing note were jointly prepared by PS and CSEC staff and reviewed across both organizations.

.../2

Attached please find the presentation (TAB A) and the PSMAC Briefing Note Template (TAB B).

Should you have any questions or comments, please contact me.

Gary Robertson

Enclosure(s): (2)

Prepared by: Linda Hunter, A/CIO

Public Safety Canada | Sécurité publique Canada

SAFE RESILIENT CANADA

A Risk Management Approach to Secure Use of iPad

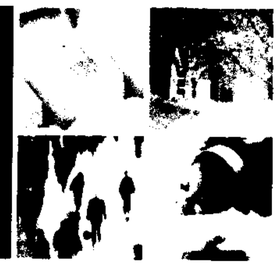
iPad Presentation to Bank of Canada

Public Safety Canada (PS)

DATE: 19 December 2012

Canada

PS Business Objectives



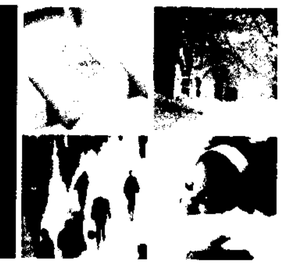
Business Objectives:

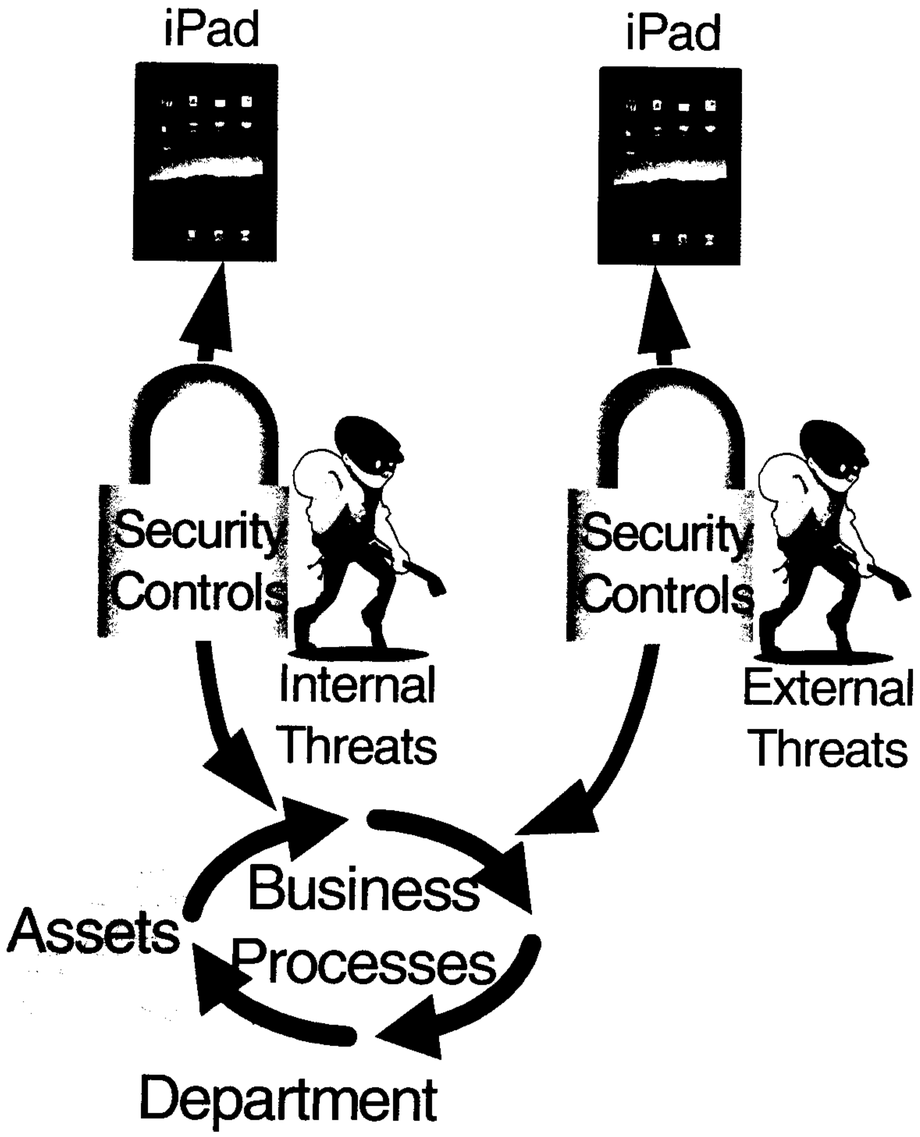
- Access to modern and efficient work tools (modern government)
- Support Greening Government (paperless)
- Move towards Workplace 2.0 including Social Media access

Requirement to enable iPad:

- Access to unclassified and Protected B corporate network
- Processing of unclassified and Protected B documents on device

CSEC - Top 5 iPad Vulnerabilities and Basic Mitigations





1. **Portable**: iPad+Data can be lost/stolen

   → *Mitigate with Encryption, Data Loss Prevention*

2. **Downloadable applications:** un-trusted apps a vehicle for malware

   → *Mitigate with Policy Enforcement and Awareness, Limited Application Library*

3. **Jailbreaking**:users can circumvent security features

   → *Mitigate with Mobile Device Monitoring Software*

4. **Un-trusted wireless network segments:**

   → *Mitigate with Secured Communication channels*

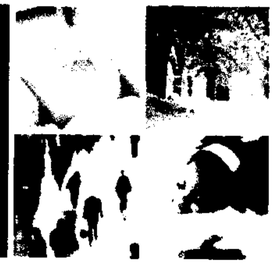
5. **Un-trusted devices**: using remote access

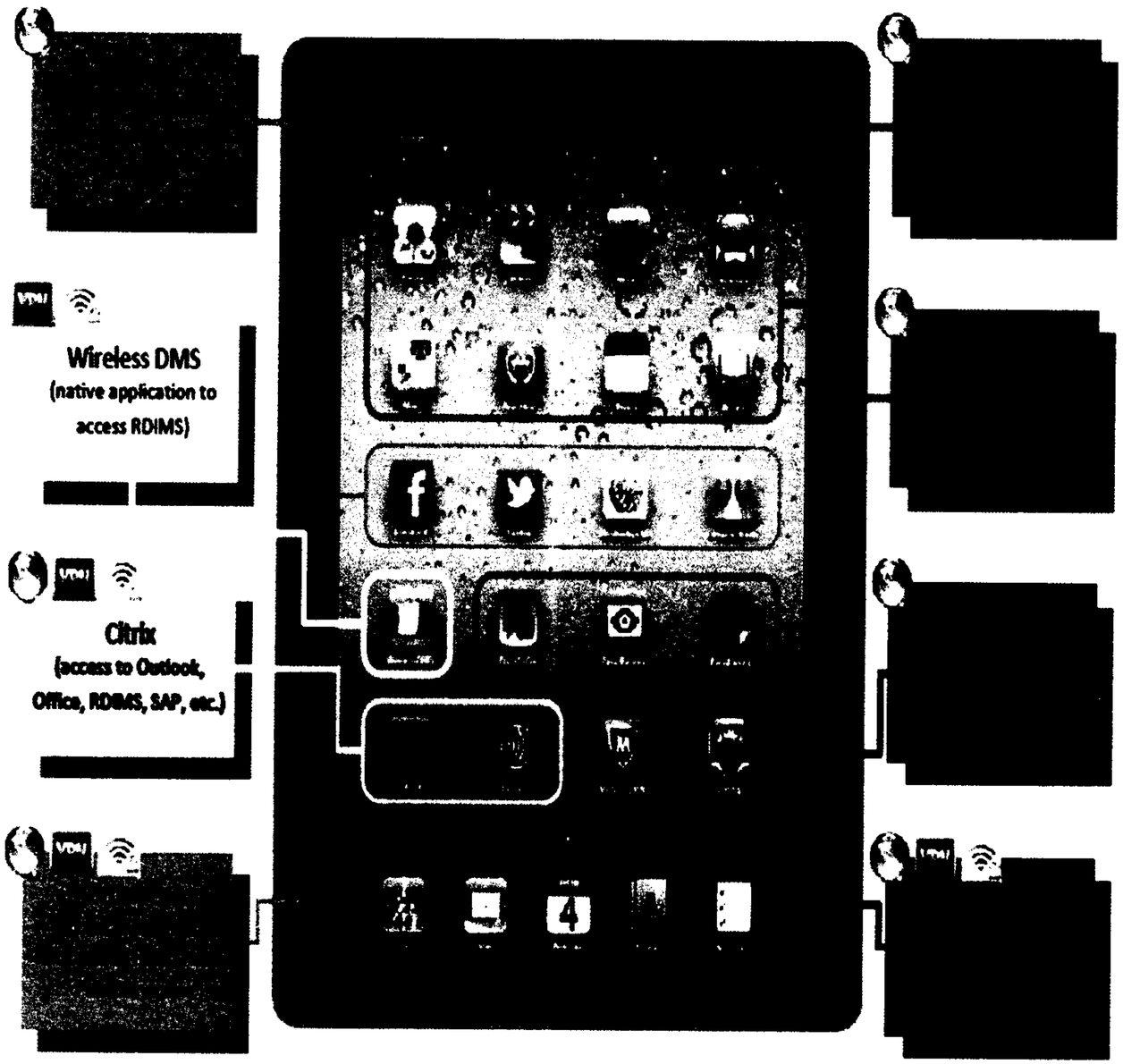
   → *Mitigate with Strong Authentication*

PS Risk Management

- Identified and mitigated security risks from the onset
- Leveraged existing, accredited PB security controls as our baseline
- Addressed CSEC Top 5 Vulnerabilities

PS iPAD - How it works securely





- **PORTABLE - Protection of data on the device with encryption where possible and physical protection (remote wipe)**
- **DOWNLOADABLE APPS – Policy enforcement and awareness/Corporate apps on deployment/signed user agreement signed/user guide**
- **JAILBREAKING - Enterprise management of security controls including Jailbreak detection with Mobile Device Management**
- **UNTRUSTED WIRELESS – Secure communications channels including WiFi connection within PS Headquarters/VPN access only to corporate network**
- **UNTRUSTED DEVICES USING REMOTE ACCESS - Secure remote access with strong authentication to access corporate* email**

PS corporate network = Protected B and below

PS Key Success Factors

- Met business objectives
  - Access to modern and efficient work tools (modern government)
  - Support Greening Government (paperless)
  - Move towards Workplace 2.0

  Through

  - Enabling iPad secure access to Protected B corporate network
    - Through strong authentication, secure communications, and corporate management of security controls
  - Enabling Protected B document processing on the iPad (e.g. executive briefing binders)
    - Through corporate management of security controls for policy enforcement and user awareness

QUESTIONS

A Risk Management Approach to Secure Use of iPAD / Approche de gestion des risques pour un usage sécuritaire du iPAD

Background / Contexte

- With the growing interest in Workplace 2.0, office mobility, social media and greening of government, Public Safety Canada (PS) worked with the Communications Security Establishment Canada (CSEC) in using a risk-management approach to implementing the iPad device as a secure, modern and efficient work tool. / Avec l'intérêt grandissant envers le milieu de travail 2.0, la mobilité au bureau, les médias sociaux et l'écologisation du gouvernement, Sécurité publique Canada (SP) a travaillé avec le Centre suivi les instructions du Centre de la sécurité des télécommunications Canada (CSTC) et a adopté une approche de gestion des risques concernant la mise en place du iPad comme outil de travail sécuritaire, moderne et efficace.

- This pilot project successfully demonstrates advancement in modern government by providing a contemporary, efficient and mobile work tool that also supports greening of government through the implementation of a paperless office concept. Workplace 2.0 directions are fostered through the provision of access to social media when not connected to the departmental corporate (Protected B) network. / Le projet pilote a permis de démontrer la modernisation du gouvernement en fournissant un outil de travail contemporain, efficace et mobile qui favorise l'écologisation du gouvernement par la mise en œuvre du concept de bureau sans papier. Il permet aussi de respecter les directives sur le milieu de travail 2.0 en donnant accès aux médias sociaux en l'absence d'une connexion au réseau ministériel (Protégé B).

- The PS iPad pilot enabled access to the corporate Protected B network including processing of Protected B documents on the iPad device. / Le projet pilote de SP sur l'iPad a permis d'avoir accès au réseau Protégé B du Ministère et de traiter des documents Protégé B à partir d'un iPad.

- CSEC reviewed and supports the use by PS of a risk management approach which considered the departmental risk profile as well as recognizing departmental business priorities. This presentation shows how PS and CSEC have joined forces to advocate this risk management approach which was used in the departmental iPAD pilot. / Le CSTC a examiné et approuvé l'approche de gestion des risques de SP, qui tient compte du profil de risque et des activités prioritaires du Ministère. Cette présentation montre de quelle façon SP et le CSTC ont collaboré pour recommander l'approche de gestion des risques adoptée dans le cadre du projet pilote de SP sur l'iPad.

A Risk Management Approach to Secure Use of iPAD / Approche de gestion des risques pour un usage sécuritaire du iPAD

Considerations / Facteurs à prendre en considération

- The PS iPad pilot implementation was based on a risk management approach that balanced departmental risk tolerance with business requirements, identifying and addressing risk mitigation strategies that reduced departmental risk to an acceptable level. While the residual risk tolerance may vary between departments, the process is universal, changing only with reference to the specific departmental context. / La mise en œuvre du projet pilote de SP sur l'iPad était fondée sur une approche de gestion des risques permettant de trouver un juste équilibre entre la tolérance ministérielle au risque et les exigences opérationnelles, ainsi que de trouver et d'appliquer des stratégies d'atténuation des risques ministériels à un niveau acceptable. Même si la tolérance aux risques résiduels peut varier d'un ministère à l'autre, le processus est universel et ne change qu'en fonction du contexte particulier d'un ministère.

- Maintaining corporate control of the devices was an essential element in the pilot, supporting PS in the management of security controls, device administration and the provision of functionality that supported departmental business requirements. / Le maintien du contrôle ministériel sur les tablettes était un élément essentiel du projet pilote, car il aide SP à gérer les mesures de sécurité, à administrer les tablettes et à fournir des fonctionnalités qui appuient ses exigences opérationnelles.

- Security controls to the Protected B level included strong authentication and secure communications protocols. However, the controls are not considered robust enough for the processing of classified information. / Au niveau Protégé B, les mesures de sécurité comprenaient des protocoles rigoureux d'authentification et de communication sécurisée. Toutefois, ces mesures ne sont pas jugées suffisamment rigoureuses pour le traitement de renseignements classifiés.

Key Messages / Messages clés

- PS followed the risk management approach advocated by CSEC to deliver a solution that meets departmental risk tolerance while providing functionality to our client community that advances the priorities for modern government. / SP a appliqué l'approche de gestion des risques recommandée par le CSTC afin de proposer une solution qui respecte le niveau de tolérance ministérielle aux risques tout en fournissant à ses clients une fonctionnalité qui contribue aux priorités liées à la modernisation du gouvernement.

- Other departments may wish to benefit from this work in improving the security of their iPAD deployments while enabling client business and operational needs. / D'autres ministères voudront peut-être bénéficier de ce travail en améliorant la sécurité du déploiement de leurs iPads toute en rencontrant les besoins d'affaires et opérationnels des clients.

Contact / Personne-ressource : Rosanna Di Paola
Name, Telephone number / nom, numéro de téléphone : 613-944-4878

Notes for Opening Remarks by

Graham Flack
Acting Deputy Minister of Public Safety

For a Study on

Chapter 3 of the Fall 2012 Report of the Office of the Auditor General of Canada Protecting Canadian Critical Infrastructure Against Cyber Threats

Senate Standing Committee on

National Security and Defence

Ottawa, Ontario

October 29, 2012

Check against delivery

- Thank you, Madame Chair.

- I would like to introduce my two colleagues from Public Safety Canada
    - Bob Gordon (Special Advisor for Cyber Security)
    - Windy Anderson (Director of the Canadian Cyber Incident Response Centre).

- I'd like to make three introductory points.

- First, cyber security threats faced by Canada and other countries have grown significantly in the last few years.

- The Government of Canada has made significant progress in identifying evolving threats and strengthening our capacity to better protect critical infrastructure.

- But we will need to continually adapt our systems to respond to the growing and changing cyber-threat environment.

- Second, I'd like to explain the role of the Canadian Cyber Incident Response Centre, or CCIRC.

- CCIRC's primary role is to monitor the cyber threat environment and provide technical and strategic advice on cyber threats, as well as to coordinate the national response against cyber attacks on systems outside the federal government.

- For instance, CCIRC has an ongoing project to evaluate weaknesses in the industrial control systems that critical infrastructure uses. This work helps all companies protect their own networks.

- CCIRC IS **NOT** responsible for monitoring or protecting federal government networks.

- This is the responsibility of all federal departments who have their own IT systems to protect sensitive information.

- Shared Services Canada was recently created to streamline our federal IT systems, and make them more secure and reliable.

- They are assisted by the Communications Security Establishment, or CSEC, who plays a role in detecting, analyzing and mitigating the impact of high level cyber security incidents that affect the integrity and availability of our federal networks.

- The Communications Security Establishment and CCIRC collaborate on risks that cross over between public and private sector systems but I wanted to clarify that CCIRC is not mandated to address threats to Government of Canada systems.

- My final point is in regard to the hours of operation of CCIRC which will be expanding to have staff on site 15 hours a day seven days a week in order to cover the core operating hours of its clients from coast to coast.

- It is important to note that CCIRC has always provided 24- hour service to its clients to deal with emergency situations.

- This is done through an on call system similar to that used in its equivalent organization in the United Kingdom. This approach has been effective in addressing client demands to date.

- Thank you; I welcome your questions.

Notes pour le mot d'ouverture de

Graham Flack
Sous-ministre par intérim de Sécurité publique Canada

Dans le cadre d'une étude sur

Le chapitre 3 du rapport d'automne 2012 du Bureau du vérificateur général du Canada – Protéger l'infrastructure canadienne essentielle contre les cybermenaces

Comité sénatorial permanent de la sécurité nationale et de la défense

Ottawa (Ontario)

Le 29 octobre 2012

Priorité au discours prononcé

- Merci, madame la Présidente.

- J'aimerais présenter mes deux collègues de Sécurité publique Canada :
    - Bob Gordon (conseiller spécial en matière de cybersécurité);
    - Windy Anderson (directrice du Centre canadien de réponse aux incidents cybernétiques).

- J'aimerais présenter trois points en guise d'introduction.

- Premièrement, les menaces liées à la cybersécurité auxquelles font face le Canada et d'autres pays se sont accrues de façon importante au cours des dernières années.

- Le gouvernement du Canada a fait d'importants progrès en ce qui a trait à l'identification des menaces en évolution et au renforcement de notre capacité de mieux protéger nos infrastructures essentielles.

- Néanmoins, nous devons adapter continuellement nos systèmes pour pouvoir répondre au milieu variable et grandissant des cybermenaces.

- Deuxièmement, j'aimerais expliquer le rôle du Centre canadien de réponse aux incidents cybernétiques.

- Le rôle principal du Centre est de surveiller l'environnement de cybermenaces et de fournir des conseils techniques et stratégiques à ce sujet, en plus de coordonner l'intervention nationale en cas d'attaque cybernétique sur des systèmes à l'extérieur du gouvernement fédéral.

- Par exemple, le Centre canadien de réponse aux incidents cybernétiques mène actuellement un projet visant à évaluer les faiblesses des systèmes industriels de commande qu'utilisent les infrastructures essentielles. Ce projet aide toutes les entreprises à protéger leurs propres réseaux.

- Le Centre N'EST **PAS** responsable de surveiller ou de protéger les réseaux du gouvernement fédéral.

- Cette responsabilité revient aux ministères eux-mêmes, qui possèdent leurs propres systèmes informatiques pour protéger les renseignements de nature délicate.

- Services partagés Canada a récemment été créé pour réunir les systèmes de technologies de l'information du gouvernement fédéral et les rendre plus sécuritaires et plus fiables.

- Le Centre de la sécurité des télécommunications Canada apporte également son aide en participant à la détection, à l'analyse et à l'atténuation des répercussions des incidents d'importance relatifs à la cybersécurité qui touchent l'intégrité et la disponibilité de nos réseaux fédéraux.

- Le Centre de la sécurité des télécommunications Canada et le Centre canadien de réponse aux incidents cybernétiques collaborent effectivement en ce qui concerne les risques qui touchent aussi bien les systèmes du secteur public que ceux du secteur privé, mais je tiens à rappeler que le Centre canadien de réponse aux incidents cybernétiques n'a pas le mandat de s'occuper des menaces visant les systèmes du gouvernement du Canada.

- Troisièmement, j'aimerais dire quelques mots sur les heures d'exploitation du Centre canadien de réponse aux incidents cybernétiques, qui seront prolongées afin que le Centre puisse mener ses activités 15 heures par jour, sept jours par semaine, et puisse offrir ses services pendant les principales heures de fonctionnement de ses clients d'un bout à l'autre du pays.

- Il est toutefois important de noter que le Centre canadien de réponse aux incidents cybernétiques a toujours offert à ses clients un service 24 heures sur 24 pour faire face aux situations d'urgence.

- Ce service est offert grâce à un système d'appel semblable à celui utilisé par l'organisme qui joue le même rôle au Royaume-Uni. Cette approche a permis de répondre de façon efficace aux demandes des clients jusqu'à maintenant.

- Merci. C'est avec plaisir que je répondrai à vos questions.

Notes for Opening Remarks by

Graham Flack
Acting Deputy Minister of Public Safety

For a Study on

Chapter 3 of the Fall 2012 Report of the Office of the Auditor General of Canada Protecting Canadian Critical Infrastructure Against Cyber Threats

Senate Standing Committee on

National Security and Defence

Ottawa, Ontario

October 29, 2012

Check against delivery

- Merci, madame la Présidente.

- J'aimerais présenter mes deux collègues de Sécurité publique Canada :
    - Bob Gordon (conseiller spécial en matière de cybersécurité);
    - Windy Anderson (directrice du Centre canadien de réponse aux incidents cybernétiques).

- J'aimerais présenter trois points en guise d'introduction.

- Premièrement, les menaces liées à la cybersécurité auxquelles font face le Canada et d'autres pays se sont accrues de façon importante au cours des dernières années.

- Le gouvernement du Canada a fait d'importants progrès en ce qui a trait à l'identification des menaces en évolution et au renforcement de notre capacité de mieux protéger nos infrastructures essentielles.

- Néanmoins, nous devons adapter continuellement nos systèmes pour pouvoir répondre au milieu variable et grandissant des cybermenaces.

- Second, I'd like to explain the role of the Canadian Cyber Incident Response Centre, or CCIRC.

- CCIRC's primary role is to monitor the cyber threat environment and provide technical and strategic advice on cyber threats, as well as to coordinate the national response against cyber attacks on systems outside the federal government.

- For instance, CCIRC has an ongoing project to evaluate weaknesses in the industrial control systems that critical infrastructure uses. This work helps all companies protect their own networks.

- CCIRC IS **NOT** responsible for monitoring or protecting federal government networks.

- This is the responsibility of all federal departments who have their own IT systems to protect sensitive information.

- Shared Services Canada was recently created to streamline our federal IT systems, and make them more secure and reliable.

- They are assisted by the Communications Security Establishment, or CSEC, who plays a role in detecting, analyzing and mitigating the impact of high level cyber security incidents that affect the integrity and availability of our federal networks.

- The Communications Security Establishment and CCIRC collaborate on risks that cross over between public and private sector systems but I wanted to clarify that CCIRC is not mandated to address threats to Government of Canada systems.

- My final point is in regard to the hours of operation of CCIRC which will be expanding to have staff on site 15 hours a day seven days a week in order to cover the core operating hours of its clients from coast to coast.

- It is important to note that CCIRC has always provided 24 hour service to its clients to deal with emergency situations.

- This is done through an on call system similar to that used in its equivalent organization in the United Kingdom. This approach has been effective in addressing client demands to date.

- Thank you; I welcome your questions.

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:

File No. : 393791
RDIMS No. : 784586

MEMORANDUM FOR THE DEPUTY MINISTER

APPEARANCE BEFORE THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

(Information only)

ISSUE

The Standing Committee on Public Accounts (PACP) will extend an invitation for you to appear regarding the Chapter 3 of the Fall 2012 Report of the Auditor General – Protecting Canadian Critical Infrastructure Against Cyber Threats. The meeting could occur as early as March 21, but we anticipate the invitation will be for March 26.

BACKGROUND

The Committee meetings take place on Tuesdays and Thursdays, from 3:30 to 5:30 pm, normally in Room C-237, commonly known as the Reading Room, of the Centre Block. It is very likely the meeting will be video recorded for future airing on the Cable Public Affairs Channel (or CPAC). You have requested to be accompanied by the Associate Deputy Minister, Assistant Deputy Minister Lynda Clairmont and Mr. Robert Gordon, Special Advisor, Cyber Security. Officials from the Office of the Auditor General and the Treasury Board Secretariat will almost certainly be invited by the Committee to appear with you.

The Committee has indicated they will allow each organization no more than five minutes to deliver an opening statement. The lead official from the Office of the Auditor General is often invited to proceed before other officials.

.../2

Canada

A handbook (attached) has been prepared to assist you in preparing for your appearance. It was developed in conjunction with the National Security Branch and Communications Services.

A Departmental Action Plan was developed following the report of the Auditor General. It is recommended that it be provided to the Committee at least 24 hours in advance of the meeting. Consistent with past practice, the action plan should be shared with the Minister's office for review before it is made public.

Should you require additional information, please do not hesitate to contact me at 613-949-0477 or Mr. Jean Cintrat, Director, Parliamentary Affairs, at 613-991-2942.

Randall Koops

Enclosure: (1)

Prepared by: Julien Clavel