

**Pages 208 to / à 227
are withheld pursuant to sections
sont retenues en vertu des articles**

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

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



Public Safety
Canada

Sécurité publique
Canada

BUILDING A SAFE AND RESILIENT CANADA



Working Together to Protect Sensitive Information and Critical Systems

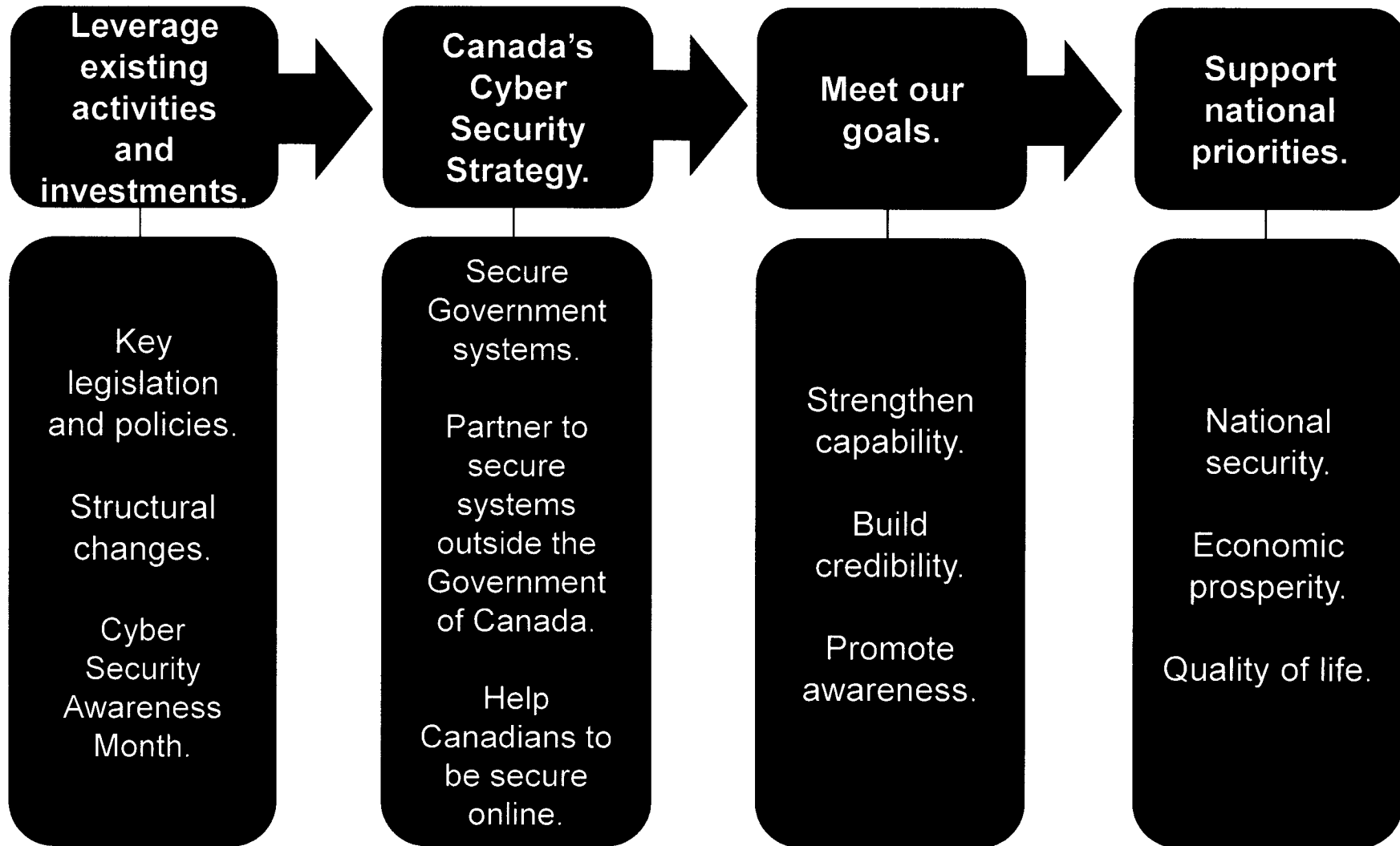
OCTOBER 31, 2012
RDIMS # 688282

Canada

Canada's Cyber Security Strategy: Describing The Approach



BUILDING A **SAFE AND RESILIENT CANADA**



How Important is Cyberspace?



BUILDING A **SAFE AND RESILIENT CANADA**

- Canadian economy relies heavily on the Internet.
 - Retail sales in 2010 - \$15.3B.
 - 93% of SMEs use the Internet (2011).
- Governments in Canada are increasingly dependent on the Internet.
 - 251 federal government organizations online.
 - All jurisdictions are increasingly leveraging online service delivery.
- Canadians are embracing cyberspace.
 - Nearly 80% of Canadian households have Internet access (2011).
 - 63% of Canadians banked online in the last year.
- Vital services, many in PT jurisdictions – banking, electricity, gas, water, transport – depend on computer control systems.

The more we depend on these systems, the greater the value of infiltrating or disrupting them.



The Cyber Environment: Who's Out There?



BUILDING A **SAFE AND RESILIENT CANADA**

State Sponsored Cyber Espionage and Military Activities

-Many nations with cyber exploitation capabilities

- Organized Crime
 - Identity theft
 - Electronic bank heists
 - Illicit trade
- Terrorist Networks
 - Recruitment / propaganda
 - Financing
 - Planning
 - Seeking cyber attack capability
- 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



What Canadian Assets are Targeted?



BUILDING A **SAFE AND RESILIENT CANADA**

- Foreign policy, national security and defence strategies, plans and capabilities.
- Trade strategies/negotiations and related information impacting our broader economic interests.
- Private sector information underpinning competitive advantage – intellectual property, pricing strategies, vulnerabilities, R&D.
- Personal information of specific Canadians based on political activities, positions of authority, potential as a source for social engineering.
- Critical infrastructure sectors - energy, financial, telecom, transport - many of which have Crown corporations.



Cyber Security and the Supply Chain



BUILDING A **SAFE AND RESILIENT CANADA**

Supply Chain Threat

- A product can be tampered with in the supply chain to later facilitate a cyber-attack against that product to exploit a network and the information the network carries.
- Dramatic globalization and significant growth in global vendors suffering from weaknesses in their supply chain means Government and industry clients are also exposed.



Public Safety
Canada

Sécurité publique
Canada

Actions Underway



BUILDING A **SAFE AND RESILIENT CANADA**

- **Creating secure capacity in Canada with trusted vendors for networks, data centres and email services through:**
 - Consolidation under Shared Services Canada.
 - Invocation of the National Security Exception.
- **Expanding efforts to collaborate and partner with provinces and territories.**
- **Building collective leverage to demand greater security from the marketplace.**



Where We Must Focus Our Efforts



BUILDING A **SAFE AND RESILIENT CANADA**

- Assess and understand the risks, within government and in our jurisdictions.
- Apply best practices when procuring goods and services:
 - Minimum security requirements.
 - Trusted vendors.
 - Data sovereignty – keeping data in Canada and under Canadian jurisdiction.
- Focus our attention on cyber security issues of shared responsibility and concern, such as public awareness and national incident response.



Conclusion



BUILDING A **SAFE AND RESILIENT CANADA**

- Safeguarding our cyber systems is key to Canada's economic and national security.
- Supply chain security and secure procurement are important aspects of cyber security.
- We must strengthen and expand our joint cyber security efforts.


www.publicsafety.gc.ca/cyber
www.publicsafety.gc.ca/ci

GETCÿBERSAFE



Public Safety
Canada

Sécurité publique
Canada

 Public Safety Canada / Sécurité publique Canada



Working Together to Protect Sensitive Information and Critical Systems

OCTOBER 31 2012
R.DIMS # 688282

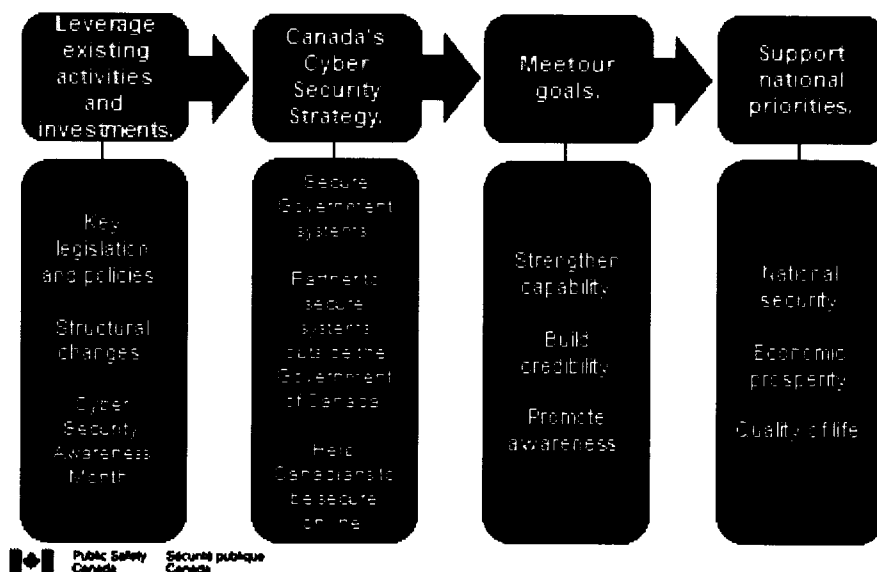
Canada

October 26, 2012 – 1pm

Canada's Cyber Security Strategy: Describing The Approach



SAFE AND RESILIENT CANADA



- Public Safety Canada is the federal government lead on the National Cyber Security Strategy, and we are working closely with government and private sector partners on its implementation.
- The Strategy is built on three pillars: securing federal government systems, partnering to secure vital cyber systems across Canada, and helping Canadians to be secure online.
- Today I want to address the security of federal, provincial and territorial systems, as well as those of the private sector.

How Important is Cyberspace?



SAFE AND RESILIENT CANADA

- Canadian economy relies heavily on the Internet.
 - Retail sales in 2010 - \$15.3B.
 - 93% of SMEs use the Internet (2011).
- Governments in Canada are increasingly dependent on the Internet.
 - 251 federal government organizations online.
 - All jurisdictions are increasingly leveraging online service delivery.
- Canadians are embracing cyberspace.
 - Nearly 80% of Canadian households have the Internet (2011).
 - 63% of Canadians banked online in the last year.
- Vital services, many in PT jurisdictions – banking, electricity, gas, water, transport – depend on computer control systems.

The more we depend on these systems, the greater the value of infiltrating or disrupting them.



2

- Canada and Canadians rely heavily on cyberspace, and most of the nation's important cyber infrastructure resides in private hands.
- The national security and economic risks associated with this infrastructure demand close partnerships between all levels of government and with the private sector to protect and defend it.
- These partnerships require sustained attention to succeed.
 - Owners and operators of critical networks often have to deal with all levels of government on security and resilience issues.
 - When information crosses national borders, competing legislation and policy from multiple states may come into play.
 - Private firms must answer to shareholders and the market, and so are often reluctant to share sensitive information on security concerns.
- Nonetheless, it is clear that the effective functioning of government, economic growth and jobs, and the safety of Canadians all rely upon a secure and reliable cyberspace.

The Cyber Environment: Who's Out There?

SAFE RESILIENT CANADA

State Sponsored Cyber Espionage and Military Activities

-Many nations with cyber exploitation capabilities

- **Organized Crime**
 - Identity theft
 - Electronic bank heists
 - Illicit trade
- **Terrorist Networks**
 - Recruitment / propaganda
 - Financing
 - Planning
 - Seeking cyber attack capability
- **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

 Public Safety Canada / Sécurité publique Canada

3

- Those interested in launching cyber attacks against us range from sophisticated state actors to criminals to hacktivists.
- For all of them, access to sophisticated cyber attack tools is proliferating, and the cost of mounting attacks is dropping.
- At the same time, the complexity of our networks and the costs to defend them are growing.
- State and state-sponsored actors are the greatest concern. They will set objectives and be very patient, disciplined and persistent in achieving them.
- We know of [REDACTED] cyber exploitation capabilities.

s.15(1) - Def

What Canadian Assets are Targeted?

SAFE AND RESILIENT CANADA

- **Foreign policy, national security and defence strategies, plans and capabilities.**
- **Trade strategies/negotiations and related information impacting our broader economic interests.**
- **Private sector information underpinning competitive advantage – intellectual property, pricing strategies, vulnerabilities, R&D.**
- **Personal information of specific Canadians based on political activities, positions of authority, potential as a source for social engineering.**
- **Critical infrastructure sectors - energy, financial, telecom, transport - many of which have Crown corporations.**

 Public Safety Canada / Sécurité publique Canada

4

- Governments in Canada and industry are targets for cyber espionage.
- Our governments hold sensitive information on trade and investment policy that is of great interest to those seeking Canada's natural resources and intellectual property.
- Our industry invests in research and development, resource extraction, and business ventures across the globe. That information is invaluable to competitors and potential acquirers of Canadian firms.
- Foreign states are active and highly effective in espionage activity against Canada. They are well-resourced with sophisticated capabilities, and have the legal authority within their jurisdictions to employ these capabilities.
- In many cases, the information obtained using state capabilities is passed to their domestic industry, including competitors of Canadian companies, creating an un-even playing field

Cyber Security and the Supply Chain



BUILDING A SAFE AND RESILIENT CANADA

Supply Chain Threat

- A product can be tampered with in the supply chain to later facilitate a cyber-attack against that product to exploit a network and the information the network carries.
- Dramatic globalization and significant growth in global vendors suffering from weaknesses in their supply chain means Government and industry clients are also exposed.

- The Government of Canada has significant concerns regarding cyber threats stemming from the supply chain, both for government and within the private sector.
- This refers to hardware or software being tampered with in the factory or when being assembled to insert what amounts to the electronic equivalent of a back door.
- Once the equipment is installed, attackers can remotely exploit these vulnerabilities to gain access to computers and networks to covertly copy or manipulate the information stored there. It is also possible for back doors to be created that would allow the remote shutdown or destruction of the equipment.
- The risk of this kind of attack has increased given the dramatic globalization of the information technology industry. Equipment vendors are dependent on dozens or hundreds of suppliers of sub-components from all over the world, often with limited control over the security of those suppliers

Actions Underway

SAFE RESILIENT CANADA


- **Creating secure capacity in Canada with trusted vendors for networks, data centres and email services through:**
 - Consolidation under Shared Services Canada.
 - Invocation of the National Security Exception.
- **Expanding efforts to collaborate and partner with provinces and territories.**
- **Building collective leverage to demand greater security from the marketplace.**

-
- The government is taking steps to mitigate the risks posed by supply chain threats to the Canadian telecommunications infrastructure but we need to work in closer partnership to succeed.
 - The consolidation of the Federal Government's network, data centre and email services under Shared Services Canada, including related procurement, will not only yield cost savings but will allow us to build security in from the beginning.
 - We have applied a National Security Exception to this procurement to ensure we have full control over the security aspects.
 - We have shared information on this and other cyber security issues with your jurisdictions through established channels, and we are appreciative of PT efforts to also share information with us regarding activity on their networks and reporting incidents.
 - We are working to further strengthen these mechanisms for exchange.

Where We Must Focus Our Efforts

BUILDING A SAFE AND RESILIENT CANADA

- Assess and understand the risks, within government and in our jurisdictions.
- Apply best practices when procuring goods and services:
 - Minimum security requirements.
 - Trusted vendors.
 - Data sovereignty – keeping data in Canada and under Canadian jurisdiction.
- Focus our attention on cyber security issues of shared responsibility and concern, such as public awareness and national incident response.

- 
- We must ensure that this messaging also makes its way to and is embraced by the private sector.
- Although there can be upfront costs associated with putting necessary safeguards in place, it will cost us less in the long run. This is true from a purely financial perspective, but also in terms of maintaining confidence in government and maintaining the resiliency of critical services.
- We need to expand our current joint cyber-related activities to include aspects such as public awareness and national incident response.

s.14(a)

Conclusion

BUILDING A SAFE AND RESILIENT CANADA

- Safeguarding our cyber systems is key to Canada's economic and national security.
- Supply chain security and secure procurement are important aspects of cyber security.
- We must strengthen and expand our joint cyber security efforts.

www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

GETCYBERSAFE



9

In closing, there are three messages I would like to emphasize:

1. Safeguarding our cyber systems is key to Canada's economic and national security.
2. Supply chain security is an important part of those efforts, and can be addressed through leveraging procurement processes and working in partnership with vendors.
3. We need to strengthen and expand our joint efforts to ensure we are keeping pace with cyber security threats.

Thank you for your time and attention.\

**Pages 246 to / à 248
are withheld pursuant to section
sont retenues en vertu de l'article**

14(a)

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

**Pages 249 to / à 256
are withheld pursuant to sections
sont retenues en vertu des articles**

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

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



BRIEFING NOTE FOR THE MINISTER

MEETING WITH PRINCE MOHAMMAD BIN NAYEF, MINISTER OF THE INTERIOR, SAUDI ARABIA

Issue

You will have a bilateral meeting with Prince Mohammad on Friday January 18, 2013, from 2:30 to 3:30 p.m., at your Hill Office. Prince Mohammad will be accompanied by Dr. Saad Al Jabri, Senior Security Advisor to the Minister of the Interior, and [REDACTED]

[REDACTED] You will be supported at the meeting by your Chief of Staff, Andrew House, and Mike Theilmann, Acting Director International Affairs. Suggested key messages follow this note.

Public Safety Cooperation

Saudi Arabia is a tier one priority interest for Public Safety Canada. [REDACTED]

The **RCMP** manages a very positive bilateral operational relationship with its Saudi counterpart agencies through its liaison officer posted in Dubai, United Arab Emirates.

In October 2012, the RCMP provided the Saudi Ministry of the Interior with the Major Case Management software, "E&R III". Developed by the RCMP, the software facilitates the tracking, vetting and linking of information associated with complex and high-volume investigations. A number of Saudi law enforcement officers will attend training in the software at the Canadian Police College in February 2013.


The Saudi Ministry of the Interior has more than 500,000 employees and comprises a number of agencies and organizations, including those responsible for domestic security, counter-terrorism, police, corrections, special operations forces, and borders. The General Investigation Directorate is also part of the Ministry of the Interior, while the General Intelligence Presidency reports directly to the King.

s.19(1)

s.15(1) - Int'l



Countering Violent Extremism

 a working group (the Contact Group) on counter-radicalization, which includes Saudi Arabia. The working group meets regularly to discuss issues related to countering violent extremism and radicalization.

Saudi officials believe the most effective way to avoid recidivism in prison in convicted terrorists is to fully reintegrate extremists into society. The Saudi government's de-radicalization program, which includes rehabilitation and post-release care, has received significant international attention. Since its inception, thousands of detainees have gone through the program. Key elements of the program include:

- Religious re-education, psychological counseling and vocational training;
- Government assistance to regain former employment or find new employment; and,
- Financial aid to cover post-release costs for housing, medical and dental care.

Consistent with Saudi beliefs and traditions, which emphasize family honour, the Saudi government works closely with families of detainees in the rehabilitation process. For example, detainees are released into custody of at least three family members, who sign pledges of responsibility for the detainee. Government officials also encourage unmarried detainees to marry, and will work with family members to identify suitable spouses (e.g. those who are not considered radical).

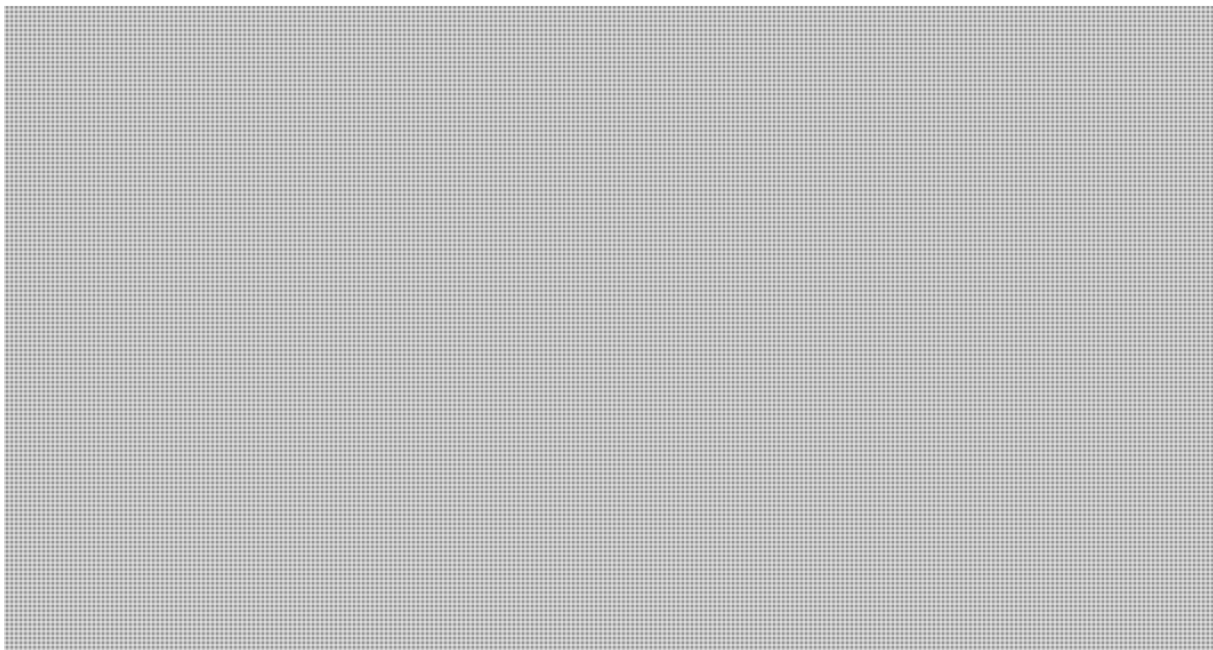
Canada's approach to countering violent extremism is situated within the *Prevent* pillar of Canada's Counter-Terrorism Strategy, launched in February 2012. The approach focuses on social cohesion and on building individual and community resilience to the threat of domestic terrorism.

Canada's approach is multi-faceted, holistic and involves a number of government departments and agencies. Activities include coordinated domestic intelligence and law enforcement, and community outreach (including through the Cross-Cultural Roundtable on Security), as well as close relationships with bilateral (e.g. the U.S., U.K. and Saudi Arabia) and multilateral partners (e.g. the Global Counter-Terrorism Forum). Public Safety Canada is also active in countering violent extremism through its funding of the Kaniska Project.

Ministry of the Interior Modernization Program



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



Regional Security

Mali. Following the March 22, 2012 coup d'état and the takeover of the northern two thirds of the country by rebels and terrorists, international efforts have focused on facilitating the restoration of democratic rule, supporting the re-establishment of government control in the north, and addressing the humanitarian crisis in the country.

On October 12, 2012, the UNSC adopted Resolution 2071 regarding the situation in northern Mali. The resolution paves the way for the creation by the UNSC of a UN stabilization mission in support of a regional African-led mission to Mali, which would authorize military deployment.

France, which has 6,000 citizens in Mali, was the first country to provide support to Malian forces. It launched a series of air strikes against rebel positions on January 11, 2013, and deployed 2,500 troops. On January 14, 2013, Prime Minister Harper announced that Canada will not have a direct Canadian military mission in Mali and will instead provide limited and clearly defined logistical support (deployment of a CC-177 aircraft) to assist the French government in transporting equipment and personnel to Mali. In addition to this logistical support, Prime Minister Harper added that Canada would continue to provide humanitarian aid and development assistance to the region to help alleviate the worsening humanitarian conditions in the region.



Syria. The situation in Syria is worsening and the most imminent threat is a humanitarian crisis prompted by an exodus of refugees, many of them Palestinians. It is believed that certain neighbouring countries would not welcome these refugees (e.g. Jordan). While Russia is still unwilling to support a UN Security Council on Syria,



s.15(1) - Int'l
s.18(b)
s.20(1)(b)
s.21(1)(a)



[REDACTED]

Yemen. The instability in Yemen has been a concern of the international community for some time. Political turmoil connected to the “Arab Spring” has compounded these issues, and has led to further instability. Al Qaida in the Arabian Peninsula remains the country’s most aggressive threat to international security.

[REDACTED]

Iran. AQ-inspired Sunni extremists and individual or small group acts of terror [REDACTED] are the most formidable internal threat to the Iranian regime, while Israel remains its strongest external threat. Iran continues its role as a patron to terrorist groups such as Hizballah, Hamas, the Palestinian Islamic Jihad, and the Popular Front for the Liberation of Palestine – General Command. The August 15, 2012 cyber attack against Saudi Arabia’s state oil company Aramco, which compromised more than 30,000 computers, [REDACTED]

Cyber Security Issues

Cyber Attack Against Aramco. On August 15, 2012, [REDACTED] the Saudi state-owned oil company’s computers, unleashed a computer virus to initiate what is regarded as one of the most destructive acts of computer sabotage on a company to date. The virus erased data on three-quarters of Aramco’s corporate computers – documents, spreadsheets, emails, files – replacing them with an image of a burning American flag. Media reports speculated that Iran was behind the attack, [REDACTED]

[REDACTED]

Internet Governance. The current day-to-day operations of the Internet are managed by a group of non-profit organizations, academics and engineers based primarily in the U.S. While Canada and its allies strongly support this multi-stakeholder approach, [REDACTED]

[REDACTED] want greater state control over the Internet and the information transmitted over it.

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(b)



UNCLASSIFIED

BRIEFING NOTE FOR THE MINISTER

MEETING WITH BARONESS PAULINE NEVILLE-JONES, SPECIAL REPRESENTATIVE TO BUSINESS ON CYBER SECURITY, UK CABINET OFFICE

Issue

You will be meeting with Baroness Pauline Neville-Jones, Special Representative to Business on Cyber Security, United Kingdom (UK) Cabinet Office.

There will not be a gift exchange.

Strategic Objectives

The recommended strategic objectives of your meeting are to:

- Obtain a better understanding of how the UK provides intelligence to private sector organizations, particularly in light of the UK's update to its *National Cyber Security Strategy*; and
- Convey the message that Canada and the UK face the same cyber threats

Public-Private Information Sharing

United Kingdom: the British government's engagement with the private sector is primarily driven by its intelligence agencies. The Centre for the Protection of National Infrastructure (CPNI) is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage.

Building on the work of the CPNI, in early September the UK formally launched their *Cyber Security Guidance for Business* program, which has released three tailored information products to help the CEOs of the 100 largest British companies address the cyber vulnerabilities of their organizations. Also in September, the UK government announced £3.8M in funding to create a Research Institute in the Science of Cyber Security based at University College London. This Institute is intended to bring together government, the UK signals intelligence agency and seven universities to develop new cyber security solutions, principally focused around cybercrime.

Canada:

As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to modernize Canada's frameworks for information sharing accordingly. It may be useful to learn more about the UK's new national

s.15(1) - Int'l

UNCLASSIFIED

security hub for public-private information sharing,

Global Cyber Security Threats and Trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. Intelligence services and militaries are also increasingly supporting, both directly and indirectly, espionage activities which are intended to secure an economic advantage whether through stealing of trade secrets or research, or by interfering in negotiations.

Recognizing the magnitude of the challenge, countries have started to pay more attention to cyber security issues and are taking steps to protect themselves. Since 2009, approximately 15 countries, including Australia, Canada, Germany, France, the Netherlands, South Korea, Russia, the UK, and the United States have each released a cyber security strategy.

United Kingdom: The UK updated its *National Cyber Security Strategy* in November 2011. The update included the following measures:

- A new national cyber security hub that will allow government and the private sector to exchange information on threats and responses;
- The establishment of a new Cyber Crime Unit within the National Crime Agency which is meant to be up and running by 2013;
- A new Joint Cyber Unit for the UK military;
- Have the Centre for the CPNI take a more inclusive approach to defining critical infrastructure;
- Improve the GetSafeOnline website (the UK equivalent of Canada's GetCyberSafe.ca public awareness campaign) and work with Internet service providers to develop a voluntary code of conduct to help people to determine if their computers have been compromised and what to do about it; and
- Continued emphasis on international dialogue, geared towards maintaining the momentum generated by the London Conference on Cyberspace held in November 2011 and the Budapest Conference held in October 2012.

Canada: Public Safety Canada's efforts under *Canada's Cyber Security Strategy* align well with many of the initiatives highlighted in the UK's strategy.

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the Royal Canadian Mounted Police's Integrated Cyber Crime Fusion Centre.
- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks.

s.21(1)(a)

UNCLASSIFIED

- Canada's GetCyberSafe.ca website was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.



**MEETING WITH BARONESS PAULINE NEVILLE-JONES,
SPECIAL REPRESENTATIVE TO BUSINESS ON CYBER SECURITY,
UK CABINET OFFICE**

KEY MESSAGES

Public-private information sharing

You may wish to:

- Inquire about the objectives of the “hub” for government and private sector information sharing referenced in the update to the UK’s cyber security strategy and how this “hub” would work.
- Ask about the challenges faced by the UK in their efforts to share information to enhance the security of networks and systems.

Global cyber security threats and trends

- Note that Canada and the United Kingdom have a strong history of working together to address cyber threats and improve our collective security.
- Highlight that the UK’s recently updated national cyber security strategy is very compatible with Canada’s, particularly its focus on addressing the economic dimension of cyber security.



BRIEFING NOTE FOR THE MINISTER

CYBER SECURITY

Global Cyber Security Threats and Trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. Intelligence services and militaries are also increasingly supporting, both directly and indirectly, espionage activities which are intended to secure an economic advantage whether through stealing of trade secrets or research, or by interfering in negotiations.

Recognising the magnitude of the challenge, countries have started to pay more attention to cyber security issues and are taking steps to protect themselves. Since 2009, approximately 15 countries, including Australia, Canada, Germany, France, the Netherlands, South Korea, Russia, the UK, and the United States have each released a cyber security strategy.

United Kingdom: The UK updated its *National Cyber Security Strategy* in November 2011. The update included the following measures:

- A new national cyber security hub that will allow government and the private sector to exchange information on threats and responses;
- The establishment of a new Cyber Crime Unit within the National Crime Agency which is meant to be up and running by 2013;
- A new Joint Cyber Unit for the UK military;
- Have the Centre for the Protection of National Infrastructure (CPNI) take a more inclusive approach to defining critical infrastructure;
- Improve the GetSafeOnLine website (the UK equivalent of Canada's GetCyberSafe.ca public awareness campaign) and work with Internet service providers to develop a voluntary code of conduct to help people to determine if their computers have been compromised and what to do about it; and
- Continued emphasis on international dialogue, geared towards maintaining the momentum generated by the London Conference on Cyberspace held in November 2011.

Canada: Public Safety Canada's efforts under *Canada's Cyber Security Strategy* align well with many of the initiatives highlighted in the UK's strategy.

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the Royal Canadian Mounted Police's Integrated Cyber Crime Fusion Centre.

UNCLASSIFIED

- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks.
- Canada's GetCyberSafe.ca website was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.

Public-Private Information Sharing

United Kingdom: the British government's engagement with the private sector is primarily driven by its intelligence agencies. The CPNI is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage.

Building on the work of the CPNI, in early September the UK formally launched their *Cyber Security Guidance for Business* program, which has released three tailored information products to help the CEOs of the 100 largest British companies address the cyber vulnerabilities of their organizations. Also in September, the UK government announced £3.8M in funding to create a Research Institute in the Science of Cyber Security based at University College London. This Institute is intended to bring together government, the UK signals intelligence agency and seven universities to develop new cyber security solutions, principally focused around cybercrime.

Canada: [REDACTED]

[REDACTED] As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to modernize Canada's frameworks for information sharing accordingly. It may be useful to learn more about the UK's new national security hub for public-private information sharing, [REDACTED]

Canada-UK Cooperation [REDACTED]

United Kingdom: The UK with the support of like-minded countries, [REDACTED] launched the London Conference on Cyberspace on November 1–2, 2011. This process is intended to specifically highlight the linkages between the various aspects of cybersecurity, namely that:

s.15(1) - Int'l

s.21(1)(a)

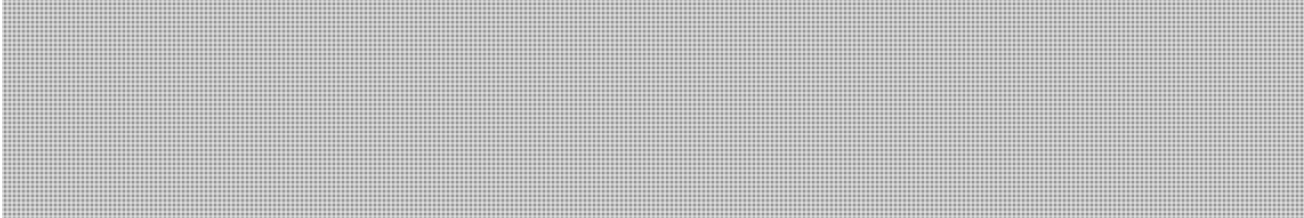
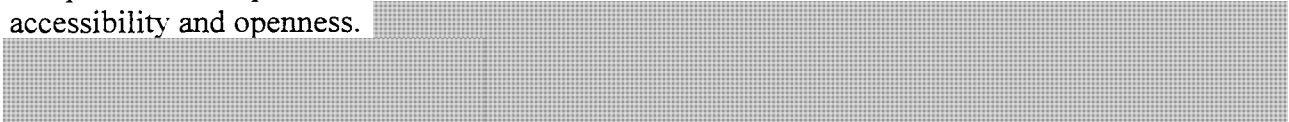
UNCLASSIFIED

- the current governance of the Internet, with a multi-stakeholder model that includes the private sector, has enabled incredible innovations and economic growth;
- going forward, the international community should focus on non-binding norms, which would set out the broad “rules of the road” for cyberspace; and
- existing international law, such as human rights law and the law of armed conflict, apply equally in cyberspace.

Underpinning this normative approach to cyberspace is the idea that no major structural changes to Internet governance or the international system are required to address new cyber issues.

The London Conference on Cyberspace was the first time that these issues were considered in a comprehensive way. It was hosted by the UK Foreign Minister William Hague, featured high-level participation (including from U.S. Vice President Joseph Biden), and brought together representatives from over 60 countries, the private sector and civil society. Hungary is hosting the next Conference in Budapest in October 2012, and it will likely feature similar prominent political engagement.

Canada: Canada has actively supported the UK in its efforts to sponsor norms for cyberspace that promote safe, predictable and consistent interactions while ensuring the Internet’s accessibility and openness.



s.15(1) - Int'l

s.21(1)(b)



CYBER SECURITY

KEY MESSAGES

Global cyber security threats and trends

- Note that Canada and the United Kingdom have a strong history of working together to address cyber threats and improve our collective security.
- Highlight that the UK's recently updated national cyber security strategy is very compatible with Canada's, particularly its focus on addressing the economic dimension of cyber security.

Public-private information sharing

You may wish to:

- Inquire about the objectives of the “hub” for government and private sector information sharing referenced in the update to the UK's cyber security strategy and how this “hub” would work.
- Ask about the challenges faced by the UK in their efforts to share information to enhance the security of networks and systems.

Canada-UK cooperation

- Note that the Canadian Cyber Incident Response Centre (CCIRC) and its UK counterpart, the Protection for National Infrastructure (CPNI), have an excellent working relationship and routinely share information on malicious websites and computer viruses.
- Express your understanding that Canada strongly supports the UK at the policy level in promoting common interests and policy positions on cyber security.

s.15(1) - Int'l



BRIEFING NOTE FOR THE MINISTER

CYBER SECURITY ISSUES

Background

Global Cyber Security Threats and Trends

Cyber threats remain a significant concern to Canada and the UK, due to both countries' dependencies on computers and networked systems for their respective prosperity and security. The range of threats is growing, encompassing hacker activists as well as criminal groups and state sponsored espionage. The ease of use of modern hacking tools makes it simple for activists to temporarily disrupt websites or cause other damage to networks. Hacking techniques are also becoming more sophisticated: for example, so-called "social engineering" techniques entail extensive research on potential victims that allow hackers to pose as trusted individuals. The hackers then craft emails or other messages that have been fabricated to trick the victim into downloading viruses or divulging details that would allow access to valuable information, such as intellectual property or credit card information. Foreign intelligence services and militaries are also capitalizing on states' dependence on networked infrastructure to conduct espionage activities or to support military operations.

Recognizing the magnitude of the challenge, countries have started to pay more attention to cyber security issues and are taking steps to protect themselves. Since 2009, approximately 15 countries, including Australia, Canada, Germany, France, the Netherlands, the Republic of Korea, Russia, the UK, and the US have each released a cyber security strategy.

United Kingdom: The UK updated its *National Cyber Security Strategy* in November 2011. The update included the following measures:

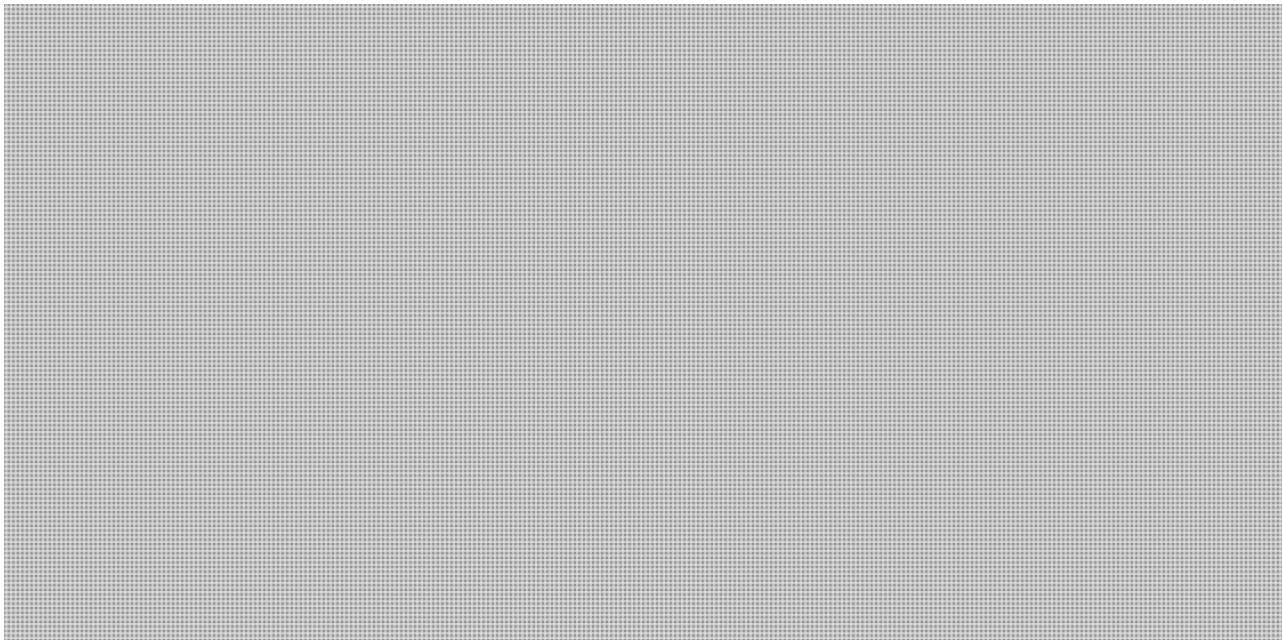
- A new national cyber security hub that will allow government and the private sector to exchange information on threats and responses;
- The establishment of a new Cyber Crime Unit within the National Crime Agency which is meant to be up and running by 2013;
- A new Joint Cyber Unit which will develop military capabilities to give the UK comparative advantage in cyber space;
- An expanded role for the Centre for the Protection of National Infrastructure (CPNI) so that it will conduct outreach to sectors beyond what has been traditionally considered part of the national critical infrastructure;
- Improve the GetSafeOnLine website (the UK equivalent of Canada's GetCyberSafe.ca public awareness campaign) and work with Internet service providers to develop a voluntary code of conduct to help people to determine if their computers have been compromised and what to do about it; and,
- Continued emphasis on international dialogue, principally maintaining momentum generated by the London Conference on Cyberspace held in November 2011.

SECRET

Canada: Public Safety Canada's efforts under *Canada's Cyber Security Strategy's* align well with many of the initiatives highlighted in the UK's strategy:

- The UK's dedicated cybercrime unit within the National Crime Agency would be similar to the RCMP's Integrated Cyber Crime Fusion Centre which was established per *Canada's Cyber Security Strategy*.
- The Canadian Cyber Incident Response Centre (CCIRC), the Canadian equivalent of the CPNI, already provides mitigation advice on cyber incidents to both critical infrastructure and other private and public sector organizations outside of federal government networks; and,
- Canada's GetCyberSafe.ca website (equivalent to the UK's GetSafeOnline.org website) was established under *Canada's Cyber Security Strategy*, and Public Safety Canada also leads activities through Cyber Security Awareness Month each October in a manner similar to the UK's public outreach campaigns.

Beyond similarities with the UK approach, Canada has also recently passed robust anti-spam legislation that levy administrative fines for sending spam, as well as establishing the Spam Reporting Centre. Further, bringing a number of government department networks under the management of new Shared Services Canada will render Government of Canada systems more secure.



Clearer Understanding of Public-Private Information Sharing

United Kingdom: The UK has a unique interface with the private sector that is primarily driven by its intelligence agencies. The CPNI is the UK authority that provides protective security advice to businesses and organizations across the national infrastructure. CPNI's protective security advice is aimed at reducing the vulnerability of the critical national infrastructure to national security threats such as terrorism and espionage. The advice under which these threats are addressed covers physical, personnel and information security, and includes cyber security.

s.13(1)(a)

s.15(1) - Int'l

SECRET

Canada: [REDACTED]

[REDACTED] As the implementation of *Canada's Cyber Security Strategy* moves forward, it will be important to identify any gaps and modernize Canada's frameworks for information sharing accordingly. In this regard, it may be useful to learn more about the UK's new national security hub to facilitate public-private information sharing.

Canada-UK Cooperation [REDACTED]

Cyber security is gaining sustained and high-level attention globally. As an indication of the importance placed on the issue by [REDACTED]

The Internet has historically been managed through a public-private model that is coordinated by a non-profit corporation based in the US, namely the Internet Corporation for Assigned Names and Numbers (ICANN). However, there is a concerted international effort, [REDACTED] to place governance of the Internet under United Nations control, as they see this as a venue that will be more amenable to their interests in increasing state power over the regulation and control of information. Further, these countries are advocating for international treaties to govern key aspects of cyberspace, such as cyber arms control and regulation over cyber security measures.

United Kingdom: The UK with the support of like-minded countries, [REDACTED] launched a counter-narrative with the London Conference on Cyberspace on November 1–2, 2011. This narrative emphasizes that:

- the current governance of the Internet, with a multi-stakeholder model that includes the private sector, has worked well by enabling incredible innovations and economic growth;
- going forward, the international community should focus on non-binding norms, which would set out the broad “rules of the road” for interactions in cyberspace; and,
- existing principles of international law, such as human rights law and the law of armed conflict, apply equally in cyberspace.

Underpinning this normative approach to cyberspace is the idea that no major structural changes to Internet governance or the international system are required to address new cyber issues.


The London Conference on Cyberspace represented a major initiative: it was hosted by the UK Foreign Minister William Hague, featured high-level participation (including from US Vice President Joseph Biden), and brought together representatives from over 60 countries, the private sector and civil society. Hungary will host the next Conference in Budapest in October 2012, and will likely feature similar prominent political engagement.

s.13(1)(a)

s.15(1) - Int'l

SECRET

Canada: Canada has actively supported the UK in its efforts to sponsor norms for cyberspace that promote safe, predictable and consistent interactions while ensuring the Internet's accessibility and openness.



Canada is a signatory to, and has committed publicly to ratifying, the Council of Europe Convention on Cybercrime, also known as the "Budapest Convention." Key allies, including the UK and the US, view this as a key international agreement and are eager for Canada to complete its ratification process. The recently tabled Bill C-30 contains measures, including provision for data preservation orders, which would enable Canada to ratify the Budapest Convention.

s.15(1) - Int'l

s.21(1)(b)

**Pages 273 to / à 275
are not relevant
sont non pertinentes**



SCENARIO NOTE FOR THE MINISTER

LUNCH WITH SIR FRANCIS MAUDE, MINISTER FOR THE CABINET OFFICE, CYBER SECURITY

Issue

You will attend lunch with Sir Francis Maude, Minister for the Cabinet Office, Cyber Security. The expected topics of conversation will include:

- International cyber governance, and approaches to global cyber security threats and trends;
- Canada-UK cooperation and common narrative on cyber security; and,
- Emergency management, community resilience, and civil contingencies.

A biography of Sir Francis Maude and key messages for the meeting follow this note.

There will not be a gift exchange.

Strategic Objectives

The suggested objectives of your meeting are to:

- Convey the message that Canada and the UK face the same cyber threats [REDACTED]
- Obtain a clearer understanding of how the UK provides intelligence to private sector organizations, particularly in light of the UK's November 2011 update to its *National Cyber Security Strategy*;
- [REDACTED]
- Exchange best practices on and gain an understanding of the UK's National Risk Register of Civil Emergencies the UK's support for prevention/mitigation and resilience; and,
- [REDACTED]

Role of Sir Francis Maude

As Minister for Cabinet Office, Sir Francis is responsible for the following issues:

- Public Sector Efficiency and Reform;
- UK Statistics;
- Civil Service issue;
- Government transparency;
- Civil Contingencies;
- Cyber security; and,
- Overall responsibility for Cabinet Office policy and the Department

UNCLASSIFIED

With respect to his cyber security and civil contingencies responsibilities, Sir Francis is supported by the Office of Cyber Security and Information Assurance (OCSIA) and Civil Contingencies Secretariat (CCS), both located in the Cabinet Office.

Sir Francis chaired the panel on “Social Benefits of the Internet” at the London Conference on Cyberspace, November 1-2, 2011.

The Office of Cyber Security and Information Assurance

The OCSIA supports the Minister for the Cabinet Office, Francis Maude and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK.

The OCSIA, alongside the Cyber Security Operations Centre, works with lead government departments and agencies such as the Home Office, Ministry of Defence (MoD), the Government Communications Headquarters (GCHQ), the Communications-Electronics Security Group (CESG), the Centre for the Protection of National Infrastructure (CPNI) and the Department for Business, Innovation and Skills (BIS) in driving forward the cyber security program for the UK government and giving the UK the balance of advantage in cyberspace.

The Civil Contingencies Secretariat

The UK’s lead agency for emergency management and resiliency issues is the Civil Contingencies Secretariat (CCS) located in the UK Cabinet Office. The CCS is responsible for all program management and policy development related to building resilience working in close cooperation with the devolved administrations of Scotland, Wales and Northern Ireland. The CCS is also responsible for coordinating the UK response to non-terrorist emergencies affecting the national interest. In a terrorist emergency with large-scale consequence management issues, the CCS is responsible for coordinating the recovery in concert, if necessary, with a lead department. The secretariat is led by a director, Christina Scott, who reports to the UK National Security Advisor to the Prime Minister. The director is supported by four deputy directors each of whom is responsible for one of the four divisions that comprise the CCS: Horizon Scanning and Response, Capabilities, Local Response Capability, and the Emergency Planning College

Controversy Regarding Sir Francis Maude and Emergency Preparedness

Critics of the UK government are accusing Sir Francis of sparking nation-wide panic over gasoline shortages because of his comments regarding a potential fuel-truck driver strike. In a television interview on March 27, 2012, Sir Francis suggested that “a bit of extra fuel in a jerry can in the garage is a sensible precaution to take”, which is twice the official limit that can be safely stored in one container at a private home in the UK. Several Labour Members of Parliament have called for Sir Francis’ resignation as Minister.

Canada’s “72 Hour Be Prepared” approach does not recommend securing a reserve of gasoline.

UNCLASSIFIED

Briefing notes on cyber security (**TAB 4L**) and emergency management (**TAB 4M**) are enclosed.

Sir Francis Maude
Minister for the Cabinet Office, Cyber Security



Francis was born in 1953. He was educated at Abingdon School, Corpus Christi College, Cambridge and the College of Law. He's married with five children; and lives at Dial Post.

Francis was elected as Member of Parliament for North Warwickshire in 1983 until 1992, during which time he was a PPS (1984-85); Government Whip (1985-87); Minister for Corporate and Consumer Affairs at the Department of Trade and Industry (1987-89); Minister of State at Foreign and Commonwealth Office (1989-90); and Financial Secretary to the Treasury (1990-92).

He lost his seat at the 1992 election, and in June that year was made a Privy Counsellor.

Francis was appointed a non-executive Director of ASDA Group Plc in July 1992. He was a Director of Salomon Brothers from 1992-93; a Managing Director of Morgan Stanley & Co Ltd 1993-97. Francis was Chairman of the Government's Deregulation Task Force from 1994-97.

In May 1997 Francis was elected to serve as Member of Parliament for Horsham.

In June 1997, he was appointed Shadow Secretary of State for Culture, Media and Sport. Francis was Shadow Chancellor of the Exchequer from June 1998 until February 2000 and from February 2000 to September 2001, he was Shadow Foreign Secretary. Francis then decided to spend a few years as backbencher, during which time he became Vice-Chairman of the All Party Parliamentary Group on AIDS.

In May 2005, Francis returned to the Front Bench when he was appointed Chairman of the Conservative Party. In July 2007, he was appointed Shadow Minister for the Cabinet Office and Shadow Chancellor of the Duchy of Lancaster.

Following the formation of the Coalition Government, Francis was appointed Minister for the Cabinet Office and Paymaster General.



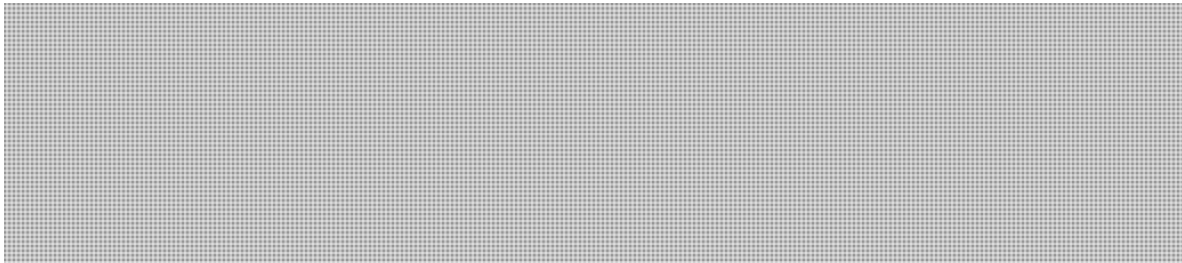
LUNCH WITH SIR FRANCIS MAUDE

KEY MESSAGES

Cyber Security

Global Cyber Security Threats and Trends

- Note that cyber threats remain a significant concern to Canada. The range of threats is growing, encompassing hacker activities as well as criminal groups and state sponsored espionage.



- Highlight Canada's initiative to bring a large portion of our government departmental networks under the management of a single new organization called Shared Services Canada. This initiative is meant to reduce the contact points of our network to the internet, allow for better monitoring of what goes in and out, and improve security measures to protect Government of Canada systems.

Canada-UK Cooperation



- Emphasize that Canada appreciates the international leadership and resolve shown by the UK in advancing a high level dialogue on norms and principles of behaviour for all stakeholders in cyberspace.
- Highlight that Canada strongly supports the UK in promoting common interests and policy positions on cyber security.
- Emphasize the importance of the October conference in Budapest, as the follow on from the London Conference on Cyberspace, as another key opportunity to influence the international discussion on cyber security and cyberspace generally.
- Note that our work on cyber security is one of the action items of the Canada-UK Joint Declaration, signed by our Prime Ministers on September 22, 2011.
- Underline that both Canada and the UK are working closely at the strategic level



SECRET

Clearer Understanding of Public-Private Information Sharing

- Inquire about the creation of a UK “hub” for government and private sector information sharing, the objectives for this hub, and how it would work.
- Inquire about the needs identified by the UK private sector and how the UK plans to respond to these needs.
- Inquire about the kinds of challenges the UK faces in sharing information with the private sector to enhance the security of networks and systems.

Emergency Management: Prevention/Mitigation

- Convey Canada’s recognition of the importance of prevention/mitigation and resilience as key principles of effective emergency management. Building resilience and a culture of prevention at all levels helps maintain and enhance the safety and security of Canadians.
- Note that in response to the increasing intensity and diversity of severe weather events, Public Safety is working with other federal departments, provincial and territorial governments, and international colleagues to address the impacts on emergency management.
- Mention that the Government of Canada, in partnership with provincial and territorial governments is developing a new National Disaster Mitigation Program that aims to strengthen community resiliency.
- Convey our willingness to share information on the work on Canada’s Platform for Disaster Risk Reduction, and extend an invitation to the U.K. to attend the next Annual National Roundtable of Canada’s Platform, which will take place in Vancouver in October 2012.



BRIEFING NOTE FOR THE MINISTER

CANADA-UNITED ARAB EMIRATES RESPONSIVE ISSUES

Visa Requirement

United Arab Emirates (UAE) nationals require a visa to enter Canada. As of October 24, 2012, processing times for UAE nationals' temporary residence visa applications were 12 days for a visitor visa, seven weeks for a study permit and five months for a temporary work permit.

In 2009-2010, the UAE decided to pursue visa impositions on countries that had visa requirements for UAE nationals, including Canada. Based on a country visa review led by Citizenship and Immigration Canada in consultation with partners, including the Public Safety Portfolio, Canada decided to maintain its visa requirement due to safety and security issues.

Since late 2009, Canadians require a travel visa to transit through or visit the UAE (ranging from \$165 for a short term single entry visa to \$660 for a multiple entry visa),

Over 40,000 Canadians are living and working in the UAE, and over 135 Canadian businesses are located there, serving the region and beyond.

In 2012, to enhance the relationship between both countries, Ministers of Foreign Affairs John Baird and Sheikh Abdullah agreed on three actions:

- launch a Canada-UAE Business Council, which has been delivered;
- conclude a Nuclear Cooperation Agreement, which has been announced; and
- address the visa issues, which are still the subject of discussions between Canadian and UAE officials.

Citizenship Fraud

As of September 2012, approximately 150 Canadian citizens that have UAE as their place of birth were being investigated for citizenship fraud,

Cyber Security Issues

The UAE has actively advocated against Canadian positions in international venues on cyber security issues. Most recently, as chair of the World Conference on International Telecommunications (WCIT), the UAE led negotiations on the recently revised International Telecommunications Regulations, which Canada did not sign.

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

s.21(1)(b)

s.21(1)(b)

s.15(1) - Int'l



[REDACTED]

Canada's operating environment for cyber security varies significantly from the UAE. In the UAE critical infrastructure is largely under state control. [REDACTED]

[REDACTED] Canada views the current multi stakeholder model of Internet governance and an open Internet as being essential.

Public Safety Canada, through the Canadian Cyber Incident Response Centre, works on an incident by incident basis with international computer emergency response teams. This can include cooperation with regional incident response organizations or directly with the UAE Computer Emergency Response Team.

Budapest Convention. The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the first and only international treaty to specifically deal with cybercrime. Some countries (Russia, China and many developing countries) have been reluctant to join the treaty, arguing that aspects of its core elements violate national sovereignty and are instead calling for a new United Nations (UN) cybercrime treaty.

Canada is an observer at the Council of Europe and contributed to the development of the treaty. The treaty was signed by Canada and its ratification is pending the enactment of legislative amendments contained in Bill C-30, the *Protecting Children from Online Predators Act*.

Internet Governance. The current day-to-day operations of the Internet are managed by a group of non-profit organizations, academics and engineers based primarily in the United States. While Canada and its allies strongly support this multi-stakeholder approach, [REDACTED] want greater state control over the Internet and the information transmitted over it.

This governance debate was front and centre at the recent World Conference on International Telecommunications (WCIT), organized by the International Telecommunications Union (ITU). The ITU is a UN body originally founded in 1865 to regulate telegrams and which today governs telephone communications between countries. At the WCIT, Russia, China and certain Arab states, including the UAE, put forward modifications to the International Telecommunication Regulations (ITRs), some of which made reference to the Internet [REDACTED]

[REDACTED] Prior to the conference, Canada and its allies made it clear that such modifications were unacceptable and therefore refused to sign the revised treaty.



CANADA-UAE RESPONSIVE ISSUES

KEY MESSAGES

Visas

- Note that the Minister of Citizenship and Immigration Canada is responsible for visa, immigration and citizenship-related matters and that you will convey the UAE government message to him.
- Convey that the Government of Canada continues to welcome visitors, students, and temporary workers from the UAE.
- Convey that Canada continues to seek ways to improve its visa application process and to facilitate contact between our countries' officials.

Cyber Security Issues

- Note that in 2010, the Government of Canada released a cyber security strategy that focuses our efforts on securing Government systems, partnering to secure vital systems outside of the federal Government and helping to keep Canadians secure online.
- Convey that Canada is confident that supporting a safe and open Internet is in all of our interests.



UNCLASSIFIED

BRIEFING NOTE FOR THE MINISTER

RESPONSIVE ISSUES

International Cyber Issues

Two of the key cyber issues currently being debated internationally concern Internet governance and the Budapest Convention.

Internet Governance

[REDACTED]
This was highlighted at the recent World Conference on International Telecommunications (WCIT), a two-week conference to update an international telecommunications treaty. [REDACTED]

Canada is opposed to such efforts as they undermine the current Internet governance model where states, the private sector and civil society contribute to decision making.

A resolution [REDACTED] annexed to the final text could be interpreted as giving the UN a greater role in managing the Internet. This was one of the many reasons Canada declined to sign the updated treaty [REDACTED]

[REDACTED] In Canada and developed countries, most critical infrastructure is owned and operated by the private sector.

In late 2010, Jordanian legislative efforts culminated with the passage of the *Information Systems Crimes Law*. This legislation addresses serious criminal activity conducted via the Internet but also includes law enforcement oversight provisions such as warrants and maintenance of law enforcement records.

Budapest Convention

The *Council of Europe Convention on Cybercrime* (Budapest Convention) is the first and only international treaty to specifically deal with cybercrime. Some countries (Russia, China, Jordan and many developing countries) are reluctant to join the treaty, arguing that aspects of its core elements violate national sovereignty and are instead calling for a new UN cybercrime treaty.

Canada is an observer at the Council of Europe and contributed to the development of the treaty. The treaty was signed by Canada and its ratification is pending the enactment of legislative amendments contained in Bill C-30, the *Protecting Children from Online Predators Act*.

Public Safety Canada, through the Canadian Cyber Incident Response Centre, works on an incident by incident basis with international computer emergency readiness teams. This can include cooperation with regional incident response organizations.



UNCLASSIFIED

Canadian Funding to United Nations Relief and Works Agency for Palestine Refugee in the Near East (UNRWA)

Canadian funding to the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA). As home to nearly two million Palestinian refugees, Jordan relies on UNRWA funding to support this population.

In 2009, CIDA stopped providing funds to UNRWA's general fund, which finances education, health and social services to Palestinian refugees in Jordan, Lebanon, Syria and the West Bank and Gaza. Since then, funding has been provided to food security programming in West Bank and Gaza, in line with Government of Canada development priorities. The announcement of this shift in funding provoked reactions from a number of countries, including Jordan. UNRWA's support to Palestinian refugees in Jordan is derived from the UNRWA's core services budget.

Canada recognizes the important role of UNRWA. Canada's contribution is determined annually based on a variety of factors, including alignment with current aid priorities and availability of resources. While Canada no longer provides funding to the general fund, we contributed \$15 million to UNRWA's 2011 Emergency Appeal for West Bank and Gaza.

This funding helped deliver food aid to about 650,000 refugees in Gaza, helped support a school feeding program benefiting more than 200,000 children, and assisted with the creation of more than 82,000 jobs for almost 33,000 refugee families in the West Bank.



UNCLASSIFIED

RESPONSIVE ISSUES

Key Messages

Cyber

- In 2010, the Government of Canada released a cyber security strategy which focuses our efforts on securing Government systems, partnering to secure vital systems outside of the federal Government and helping to keep Canadians secure online.
- Canada is confident that supporting a safe and open Internet is in all of our interests.

United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA) Funding

- UNRWA is a key humanitarian assistance partner. Canada recognizes the important role of UNRWA in meeting the humanitarian needs of Palestinian refugees.
- Canada's contribution is determined on a yearly basis on a variety of factors, including alignment with current aid priorities and availability of resources.
- In 2011, Canada contributed \$15 million to UNRWA's 2011 Emergency Appeal for the West Bank and Gaza.
- That contribution helped deliver food aid to refugees in Gaza, supported a school feeding programme, and assisted with the creation of jobs for thousands of refugee families in the West Bank.

**Pages 302 to / à 305
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(a), 15(1) - Int'l, 21(1)(a)

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

Page 306

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

15(1) - Int'l

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

**Pages 307 to / à 314
are withheld pursuant to section
sont retenues en vertu de l'article**

16(2)(c)

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