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

Supply Chain Threats to Canada

May 8, 2012

Director IT Securit

Canada

OVERALL CLASSIFICATION IS SECRET

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

CSEC Role in the GC

- CSEC Role in the Government of Canada
  - Mandate: (*b*) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada
  - Policy on Government Security: Lead agency and technical authority for IT Security
  - Provide cyber-defence (operational) and cyber-protection (preventative) advice, guidance and services to the Government Canada
  - Government of Canada partner of the National Security Agency (NSA) and National Institute of Standards and Technology (NIST)

Canada

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

OVERALL CLASSIFICATION IS SECRET

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

Cyber Security Overview

- Threat Actors
  - National Governments
  - Terrorists
  - Industrial Spies and Organized Crime Groups
  - Hactivists
  - Malfeasants

Canada

OVERALL CLASSIFICATION IS SECRET

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

CSEC IT Security Predictions (2006)

- "...market forces will continue to favour commercial and personal technologies over requirements for security fea

Canada

s.13(1)(a)
s.15(1)
s.16(2)(c)
s.21(1)(a)

OVERALL CLASSIFICATION IS SECRET

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

Today's Network Threats to the GC

- Sourced from GC - Cyber Threat Evaluation Centre (CTEC) Reporting

Canada

OVERALL CLASSIFICATION IS SECRET

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

The Farewell Dossier

- Soviets were pillaging large amounts of Western technology in the late 1970's/early 1980's

Canada

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

OVERALL CLASSIFICATION IS SECRET

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

The Supply Chain Threat

Canada

OVERALL CLASSIFICATION IS SECRET

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

US Military Bans Disks, USB Drives

- ***Wired Magazine*** (Nov. 19, 2008)
  - Resulting from Agent.btz virus attack
  - Applied to 'Secret' SIPR net and 'Unclassified' NIPR net
  - Includes thumb drives, CDs, flash media, and all other removable data storage devices
- ***60 Minutes*** (Nov. 8, 2009)
  - 'The most significant incident ever publicly acknowledged by the Pentagon'
  - 'Someone was able to get past the encryption devices and firewalls of the US military and sit there for days'
  - 'This was the CENTCOM network – the command that is fighting our two wars'
  - 'They could see what the traffic was, they could read documents, they could interfere with things'

- Jim Lewis, Centre for Strategic and International Studies

- 'Lewis believes it was done by foreign spies who left corrupted thumbnail drives...around...in places where...personnel were likely to pick them up. As soon as someone inserted one into a CENTCOM computer, a malicious code opened a backdoor.'

Canada

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

OVERALL CLASSIFICATION IS SECRET

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

Supply Chain Threat/Risk Conclusion

•

•

•

Canada

OVERALL CLASSIFICATION IS SECRET

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

Initial GC Trigger: Next Generation Cellular Networks

- In advance of the 2008 Wireless Spectrum Auction and to replace aging CDMA networks, Canadian telecommunications companies began planning the infrastructure for Canada-wide 4th Generation (4G) or Next Generation Cellular Networks (NGNs).

•

•

Canada

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

OVERALL CLASSIFICATION IS SECRET

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

GC Intervention:
Technology Supply Chain Working Group

-
  - Raise awareness among key stakeholders
  - Build IT Security into the procurement process
  - Mitigate
- Bottom Line:

There is no way to prevent the introduction of foreign technology in Canada. We must find the appropriate balance between IT security requirements, the threat-risk environment, and the need to efficiently process information and provide services to Canadians while allowing industry to remain competitive.

Canada

OVERALL CLASSIFICATION IS SECRET

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

-
-
-
-

Canada

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

OVERALL CLASSIFICATION IS SECRET

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

Defining 'Untrustworthiness' or

a.
b.
c.

2.
3.
4.
5.
6.
7.

Canada

OVERALL CLASSIFICATION IS SECRET

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

Canada

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

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

Huawei:

OVERALL CLASSIFICATION IS SECRET

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

Huawei: The Company

- Company growth and expansion
  - From start-up to #2 behind Ericsson in 20 years
  - Generous financing, export credits, 15-25 year loans to new markets
  - Founder: Ren Zhengfei (PLA Officer, Information Engineering Academy)
  - Board Chair: Sun Yafang, (Ministry of State Security)

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

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

Huawei:

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

GC Proposed Measures

PROACTIVE

REACTIVE

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

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

PROACTIVE

Build IT security into the procurement process

Today, IT security requirements are not routinely built into procurement processes; with unclear IT security objectives, it is difficult for the Government to protect information and services

Short-Term Actions

1. PWGSC, with the assistance of CSE, to finalize its *IT security contract clauses*
2. PWGSC with the assistance of CSE and client departments, to develop recommendations for the inclusion of some or all of the IT security clauses within these RFPs/contracts
3.
4.
5.
6.

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

Procurement Solutions to Cyber Threats

- In parallel to the recommendations of the [illegible] government and industry experts [illegible] necessary measure to combat cyber threats.
- "Use Acquisitions Rules to Improve Security
  - 13. The president should direct the National Office for Cyberspace (NOC) and the federal Chief Information Officer Council, working with industry, to develop and implement security guidelines for the procurement of IT products (with software as a priority).
  - 14. The president should task the National Security Agency and NIST, working with international partners, to reform the National Information Assurance Partnership (NIAP).
  - 15. The president should take steps to increase the use of secure Internet protocols. The president should direct the OMB and NOC to develop mandatory requirements for agencies to contract only with telecommunications carriers that use secure Internet protocols…."

- Commission on Cyber-Security for the 44th Presidency

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

OVERALL CLASSIFICATION IS SECRET

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

Accomplishments: Awareness

- CSEC
  telecor
- CSEC
- The GC
- GC Awareness
  -
  -
  -
  -
  -

Canada

OVERALL CLASSIFICATION IS SECRET

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

Accomplishments: Procurement

- Technology Supply Chain Guidance: ***Contracting Clauses for Telecommunications Equipment and Services***
- CSEC &
  th
  -
  -
  -
  -
  -
- Challenge:

ıdä

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

OVERALL CLASSIFICATION IS SECRET

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

What CSEC Can Offer

- CSEC's cryptologic programs, our relationships within the GC
- CSEC's industry relationships
  - a unique vantage point to understand threats & vulnerability to high technologies and their supporting critical infrastructures which can be translated into GC procurement advice & guidance
- Deep experience in cyber-protection / information assurance
  - the development and use of standards, auditing, compliance and evaluation as a means to provide confidence in the protection of GC information

Canada

OVERALL CLASSIFICATION IS SECRET

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

On-going Work & Next Steps

-
-
-

Canada

TOP SECRET SI//CEO
May 17, 2012
CERRID # 970077

Overview of Huawei Activities in Canada

For information

Summary

- This briefing note summarizes CSEC's perspective of Huawei's commercial activities in Canada and discusses some risk mitigation activities

Background

- Huawei entered the Canadian market in 2008. company was incorporated in the United States as Huawei North America. In 2011, Huawei Canada split from the North American office and incorporated in Canada with headquarters in Markham, Ontario.
- Huawei currently supplies commercial grade telecommunications equipment to Bell, Telus, Wind Mobile & Sasktel.
    - The company's first major success in Canada was the sale of 3rd generation (3G) radio access network equipment to Bell and Telus in 2009.
    - Huawei subsequently sold both 3G core and radio access network equipment to Wind Mobile and 3G radio access network equipment to Sasktel.
    - In 2011, Bell and Telus purchased 4th generation (4G) or Long-Term-Evolution (LTE) radio access network equipment from Huawei.
    - Huawei also sells a variety of consumer grade technologies in Canada including to some of Canada's new wireless entrants (Videotron, Wind Mobile, etc.)

s.15(1)
s.21(1)(b)
s.21(1)(c)

Considerations

- [redacted]
- [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
- [redacted]
- [redacted]
- [redacted]
- To date, [redacted] ry [redacted] it is [redacted]
- [redacted]

[redacted]

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

TOP SECRET COMINT//CEO
February 24, 2012
CERRID # 915845

GC Policy & Engagement Options for Huawei

For information

Summary

- CSEC is drafting a paper to consider GC policy & engagement options pertaining to Huawei
-
-

Background

- Huawei is increasingly active in pursuing foreign direct investment, equipment sales and services provisioning in the Canadian market.
- To some extent, Huawei initiatives are supported by strong market imperatives. Huawei invests significant financial resources in R&D and offers its equipment & services at a significant cost advantage to its competitors. These factors translate into strong economic incentives for Canadian companies to accept investment or to purchase equipment & services from Huawei.
-
-

year.

Considerations

-

s.15(1)
s.16(2)(c)
s.21(1)(c)

- In a recent meeting between CSEC
- CSEC
- CSEC's ideas
  -
  -

Recommendation

s.15(1)
s.21(1)(a)
s.21(1)(b)
s.21(1)(c)

Options

•

•

•

•

Recommendation

- CSEC will c
- CSEC also

ıne

ıeed

al

of

y