s.15(1)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC FOUNDATIONAL LEARNING CURRICULUM

DAY 1: INDOCTRINATION & COMPENSATION – January 14, 2013

TIME	COURSE	PRESENTER / FACILITATOR	COURSE LOCATION
08:00-08:10	Welcome & Housekeeping	[redacted]	Edward Drake Building (EDB) [redacted]
08:10-08:40	Chief's Welcome	Chief John Forster	EDB [redacted]
08:45-09:30	Indoctrination	[redacted] (Security Briefing Officer, Security Education and Awareness – [redacted]	EDB [redacted]
09:30-10:30	Protective Security	[redacted] (Supervisor, Security & Protective Services – [redacted]	EDB [redacted]
10:30-11:00	Pass Exchange and Break	[redacted]	
11:00-12:00	Employee Compensation and Benefits	[redacted] (Corporate Compensation - HRI[redacted]	EDB [redacted]
12:00-13:15	Lunch with Executive Committee members	N/A	EDB [redacted]
13:15-14:30	Employee Compensation and Benefits…cont'd	[redacted] (Corporate Compensation - HRI[redacted]	EDB [redacted]
14:30-15:45	Closing Remarks & ID Pass Control	[redacted]	EDB [redacted]

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

s.15(1)

CSEC FOUNDATIONAL LEARNING CURRICULUM

DAY 2: THE BIG PICTURE — January 15, 2013

TIME	COURSE	PRESENTER / FACILITATOR	COURSE LOCATION
08:30-10:00	(a) Welcome & Housekeeping (b) Organization Overview		EDB
10:00-10:15	Break		
10:15-10:50	CSEC as a Separate Agency in the Public Service	(Manager, Policy & Foreign Services – HR	EDB
10:55-11:45	CSEC Legal Framework	(Directorate of Legal Services)	EDB
11:45-12:45	Lunch		
12:45-13:00	CSEC 101 Video	N/A	EDB
13:00-14:15	(1) DGPC: Supporting CSEC's Strategic Direction and Accountability (2) Office of the CSEC Commissioner (OCSEC)	(Director, Corporate & Operational Policy - (2) OCSEC	EDB
14:15-14:30	Break		
14:30-15:30	Code of Values & Ethics and Conflict of Interest	(Ethics Officer - Directorate Audit, Evaluation & Ethics) & (Labour Relations Officer – HRI	EDB

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

CSEC FOUNDATIONAL LEARNING CURRICULUM

DAY 3: ITS DAY			January 16, 2013
TIME	COURSE	PRESENTER / FACILITATOR	COURSE LOCATION
08:00-08:30	Welcome & Housekeeping		EDB
08:30-08:50	Networking Activity		EDB
08:50-09:45	Information Management	(IM Training Officer, CIO-	EDB
09:45-10:00	Break		
[redacted]			
10:00-10:45	Opening remarks & "Protect and Defend" video	Toni Moffa (Deputy Chief, ITS)	EDB
10:45-11:45	Intro to ITS	ITS Learning Centre (ITSLC) staff	EDB
11:45-12:10	COMSEC Equipment Demo	ITSLC staff	EDB
12:10-13:10	Lunch		
13:10-14:10	Wireless Demo	ATA staff	EDB
14:10-14:25	Break		
14:25-15:10	ITS Organization	ITSLC staff	EDB
15:10-16:00	Conclusion and Exercise	ITSLC staff	EDB

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC FOUNDATIONAL LEARNING CURRICULUM

DAY 4: INTEL & SIGINT — January 17, 2013

TIME	COURSE	PRESENTER/ FACILITATOR	COURSE LOCATION
08:00-08:30	Welcome & Housekeeping		EDB
	HOTEL		
08:30-09:40	Security & Intelligence Community in Canada	(Senior Mission Management	EDB
09:40-09:55	Break		
09:55-11:10	Intro to Intel	(Senior Mission Management	EDB
11:10-11:30	Networking Activity		EDB
11:30-13:00	Lunch & Group Photo		
	THE WORLD OF SIGINT		
13:00-14:15	Intro to SIGINT	(Office of SIGINT Studies)	EDB
14:15-14:30	Break		
14:30-15:30	Intro to SIGINT	(Office of SIGINT Studies)	EDB

Canada

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

CSEC FOUNDATIONAL LEARNING CURRICULUM

DAY 5: RELATIONSHIPS — January 18, 2013

TIME	COURSE	PRESENTER / FACILITATOR	COURSE LOCATION
08:00-08:30	Welcome & Housekeeping		EDB
08:30-09:20	CSEC Relationships with the Canadian Forces SIGINT: The Canadian Forces (CF) & SIGINT	and (DGI) & (DGMS)	EDB
09:25-10:00	SIGINT: Program	&	
10:00-10:15	Break		
10:15-11:10	CSEC Relationship with the Canadian Security Intelligence Service (CSIS)	CSIS)	EDB
11:15-12:00	5 Eyes Relationships: (a) The partners (b) The partnership in action	(Director General, Cyber Defence) & (Team Leader – COPCC)	EDB
12:00-12:45	Lunch		
12:45-13:45	Case Study	(Team Leader - DGI)	EDB
13:50-14:35	CSEC Internal Web / Web 2.0	(IM Training Officer, CIO-	EDB
14:45-15:30	CSEC Campus Tour (optional)		

Canada

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

CSEC FOUNDATIONAL LEARNING CURRICULUM

DAY 6: TOUR & SERVICES FAIR — January 21, 2013

LONG TERM ACCOMODATION: POD 1

The day's proceedings:

Morning:

1-Tour of CSEC's new establishment (08:45 – 09:45)

2-Services Fair: You will be assigned to a group and designated a starting kiosk. Structured rotation of 20 minutes at each kiosk where you will have the opportunity to visit and interact with 5 service / information providers.

Afternoon:

Services Fair: You will be assigned to a new group and designated a starting kiosk. Structured rotation of 20 minutes at each kiosk where you will have the opportunity to visit and interact with 6 different service / information providers.

The fair is about knowledge transfer and getting acquainted with the services, and the people behind them, that can assist you in your day-to-day work. We invite you to ask questions and share your experiences.

SERVICES FAIR STATIONS AND TIMES

Morning: 10:00 – 11:40	Afternoon: 12:50 – 15:00
1. Staffing & Recruitment (HR	1. Learning@CSEC
2. Official Languages/Employment Equity (HR)	2. Performance Planning & Review (PPR) and Learning Plans (HR
3. Counselling & Advisory Program (HRCAP)	3. Library Information Services (CIO-
4. Union	4. Multimedia & Printing Services and Linguistic Services (
5. Social Committee	5. IT Services (CIO-
	6. Young Professionals Network
Lunch: 11:40 - 12:50	Break: 13:50-14:00

Departure for return to EDB – 15:15

Canada

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

CSEC FOUNDATIONAL LEARNING CURRICULUM

DAY 7: SECURITY AWARENESS — January 22, 2013

TIME	COURSE	PRESENTER / FACILITATOR	COURSE LOCATION
08:00-08:30	Welcome & Housekeeping		EDB
08:30-09:50	The Foreign Intelligence and Terrorist Threat to CSEC	(Corporate Security)	EDB
09:50-10:05	Break		
10:05-10:55	Personnel Security	(Corporate Security)	EDB
11:00-11:50	IT Security	(Corporate Security)	EDB
11:50-12:50	Lunch		
12:50-13:35	Operations Security (OPSEC)	(Security Education & Awareness –	EDB
13:35-14:00	Emergency Management	(Emergency Management Office)	EDB
14:00-14:20	Evaluations & Break		
14:20-15:30	Closing Ceremony Activities: (a) Message from our Executive Committee (b) Certificate presentation (c) Reception		EDB

s.15(1)

TOP SECRET//SI

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Program

November 2012

Canada

Page 9

is withheld pursuant to section

est retenue en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

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

Outline

- [redacted] Program Structure
- What is the [redacted] Program?
- Current & Previous [redacted] Positions
- CSEC Afghan Contribution
- [redacted]

Page 11

is withheld pursuant to sections

est retenue en vertu des articles

15(1), 17

of the Access to Information

de la Loi sur l'accès à l'information

Page 12

is withheld pursuant to section

est retenue en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

Page 13

is withheld pursuant to sections

est retenue en vertu des articles

15(1), 17

of the Access to Information

de la Loi sur l'accès à l'information

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

What is the [redacted] Program?

Background:

[redacted]

Qualifications:

[redacted]

Training:

[redacted]

Canada

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

What is the [redacted] Program?

[redacted]

[redacted] competition process:

- In order to become a [redacted] applicants can expect to undergo a rigorous selection process involving written tests, interviews, reference checks, psychological testing, [redacted]

Things to consider:

[redacted]

Page 16

is withheld pursuant to sections

est retenue en vertu des articles

15(1), 17

of the Access to Information

de la Loi sur l'accès à l'information

Pages 17 to / à 18

are withheld pursuant to section

sont retenues en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC Afghan Contribution

[redacted]

Page 20

is withheld pursuant to section

est retenue en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1)

TOP SECRET//SI

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC Afghan Contribution

Canada

Page 22

is withheld pursuant to section

est retenue en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC Afghan Contribution

Canada

Pages 24 to / à 27

are withheld pursuant to section

sont retenues en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

Questions?

s.15(1)

UNCLASSIFIED

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Introduction to Intelligence

SIGINT Programs, [redacted]

Cerrid# 931441

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Objectives

- Identify the types of Intelligence
- Identify the sources of Intelligence
- Identify components of Intelligence Cycle model

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

What is Intelligence?

- Intelligence is a PROCESS
- It is based on information that can be collected through either readily available or secret means
- It has to be analysed to be relevant to the client in order to be effective (it has to answer client's questions)
- It enables them to make **important** and **informed** decisions (eg. policy, operational, tactical, diplomatic)

Canada

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

What is Intelligence?...cont'd

Intelligence can be:

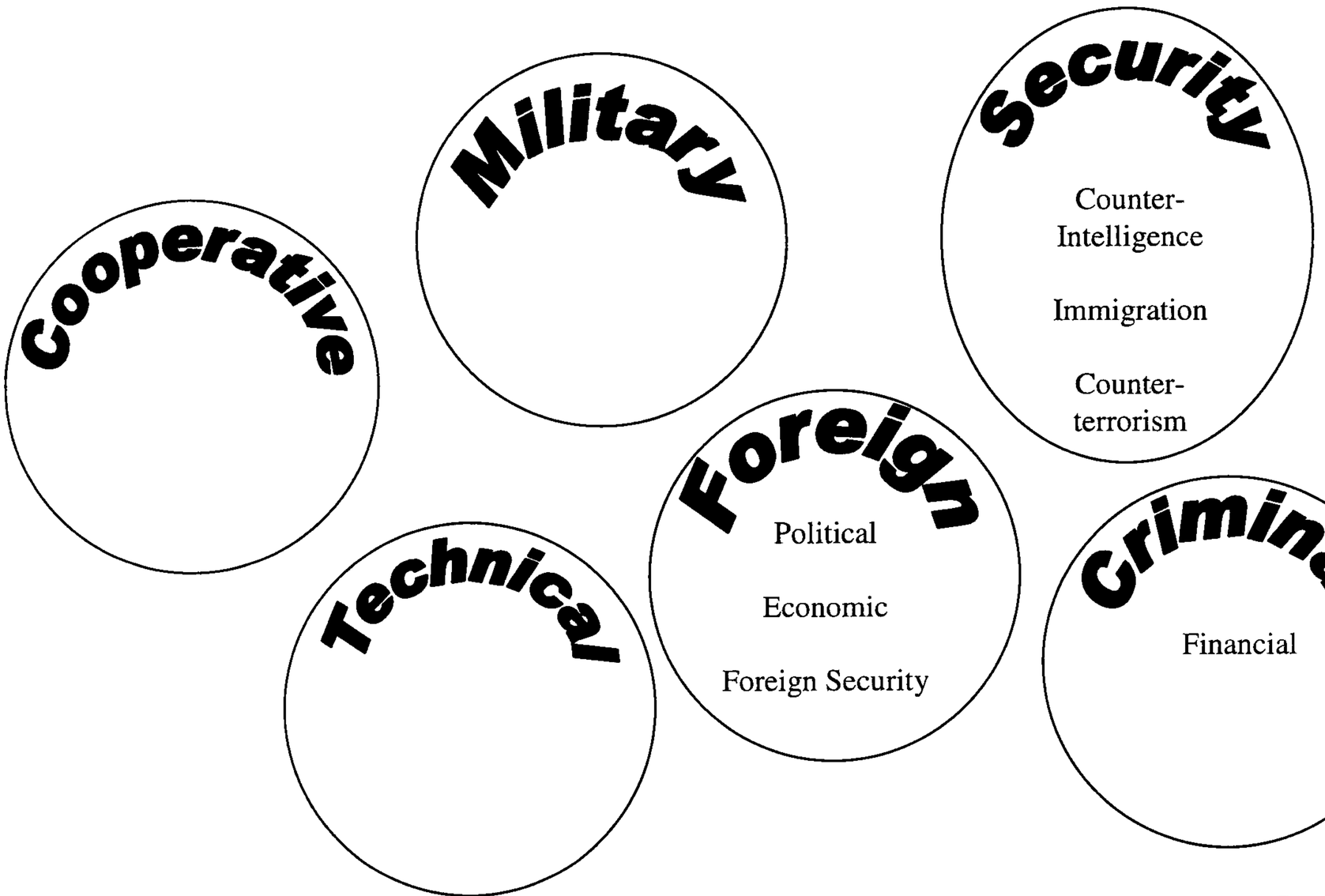
- Current
- Estimative
- Indications and Warning
- Research

What are the intelligence requirements (at a high level) that our leaders are seeking to make important and informed decisions?

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Test Your Knowledge
Types of Intelligence (6/13)



Canada

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

Test Your Knowledge
Sources of Intelligence (5/16)

SIGINT
- COMINT
- ELINT
- FISINT

IMINT
- GEOINT

OSINT

HUMINT
- RUMINT
- TRASHINT
- TECHINT

MASINT
- ACINT / ACOUSTINT
- EOINT
- RINT / NUCINT
- CBINT

Canada

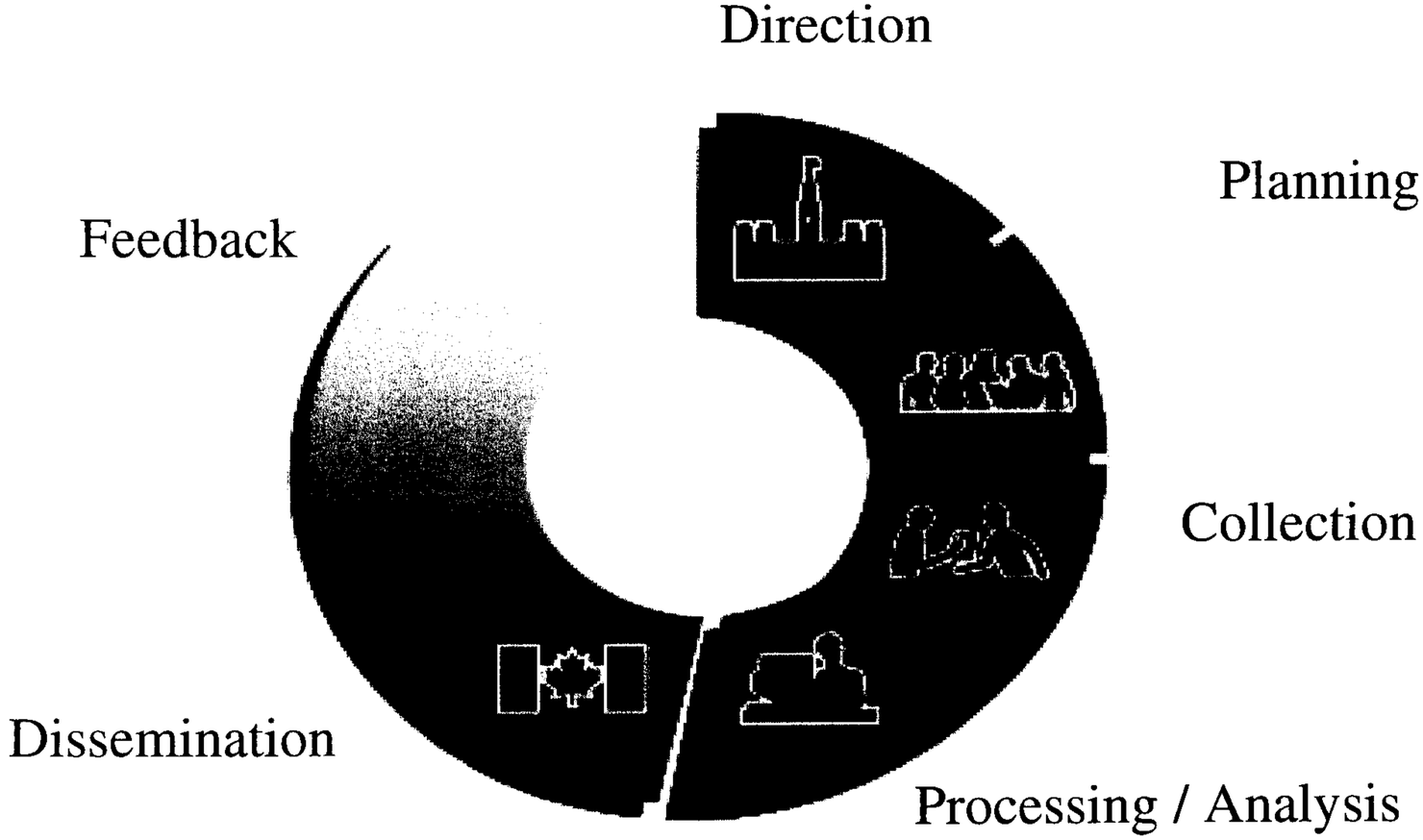
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Introducing a model
Characteristics

- Relevance
- Focused
- Acquired
- Interpreted
- Delivered
- Feedback

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

The Intelligence Cycle



Canada

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

Match the INT

- HUMINT
  - CSIS, DFAIT, DND/CF, RCMP, CBSA
- SIGINT
  - CSEC, CSIS, DND/CF, RCMP
- IMINT
  - CSIS, DND/CF, RCMP
- MASINT
  - DND/CF

AN INTRODUCTION TO CAP:

THE COUNSELLING AND ADVISORY PROGRAM

Our Mission

The CAP mission is to promote and foster resilience, wellness and good working relationships among CSEC's employees, teams, and the organization through a variety of professional and confidential services.

Our Vision

- Inspire
- Awaken
- Engage
- Empower
- Influence
- Transform
- Excel

Key Concepts of the CAP Program

- Confidentiality
- Voluntary
- Neutrality

s.15(1)

The Counselling and Advisory Program

- Individual counselling
- Support to management
- Team Performance
- [redacted]
- Wellness activities
- Resource centre
- Provision of services for employees with a disability

Contact Information

Counsellors:

[redacted]

[redacted]

Wellness Coordinator:

[redacted]

[redacted]

Office Location:

- SLT building - [redacted]

Wellness Quiz

1. Stress can instigate other health issues.

True or False?

Wellness Quiz

2. What accounts for 50% of difficulty concentrating and focusing at work?

a) Your Boss.

b) American Idol.

c) Sleep Deprivation

Wellness Quiz

3. Why is Wellness in the workplace an important concept for leaders of an organization to consider?

a) It can improve employees' performance
b) It is the right thing to do
c) It lowers health care costs
d) Wellness shmellness!
e) Answers a to c

Wellness Quiz

4. Individuals affected by mental illness are not productive members of society.

Myth or Reality?

Wellness Quiz

5. The workplace is not responsible for mental health. It is an individual concern and responsibility.

Myth or Reality?

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Policy at CSEC

Foundational Learning Curriculum
June 19, 2012

[redacted]

External Review and Policy Management

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

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

Each business line is responsible for specific areas of policy

- Director General Policy and Communications
  - Operational, Disclosure Risk Management and broad Corporate policies
- Corporate Services
  - Assets Management, Financial, and Security policies
- Chief Information Office
  - Information Management, Management of Information Technology, and Information Security policies
- SIGINT and ITS
  - Detailed Operational Instructions
  - COMSEC policy for the GC
  - SIGINT Security Management policy for the GC

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

Policies are linked to Authorities and Strategic Direction

- Authorities
  - Legislation, regulations, orders-in-council
  - Ministerial Authorizations issued in accordance with section 273.65 of the *National Defence Act*
  - Non-legislative instruments that transfer or delegate specified authorities to CSEC (e.g., *Policy on Government Security*)
- Strategic Direction
  - Ministerial Directives
  - Other directions from the Minister or Cabinet (including Cabinet Committees)
  - GC policies applicable to CSEC
  - CSEC senior management direction

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

Why Policy Matters

- Actions are consistent with legislation, central agency directives and other operating context requirements;
- Uniformity, consistency, stability and continuity in decisions, even if personnel change (corporate memory);
- Clear definition of accountability and responsibility;
- New issues can be handled quickly and effectively;
- Public accountability and CSE Commissioner review;
- Functional areas operate in an efficient and business like manner; and
- Functions are carried out in a manner that is ethical and reflect GC and CSEC values.

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

CSEC Policy Framework (ORG-1)

- Lays out the rationale for and defines the policy instruments recognized at CSEC

- Establishes policy accountability and responsibility

- Policy Categories
  - Lead Security Agency policy
  - Operational policy
  - Organizational policy

- Types of Policy Instruments
  - Policies, Procedures, Standards, Guidelines, Instructions

Page 54

is withheld pursuant to sections

est retenue en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Questions about Policy at CSEC

- Contact the External Review and Policy Management team by email: [redacted]

s.15(1)

s.16(2)(c)

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

Office of the CSE Commissioner

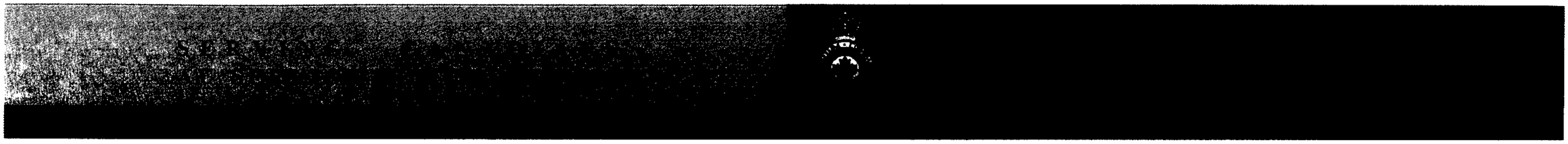
- External Review and Policy Management [redacted] is the team responsible for liaison with the Office of the CSE Commissioner

- The CSE Commissioner provides external, independent review of CSEC's activities to ensure compliance with the law and the protection of privacy of Canadians

- For questions related to the CSE Commissioner, contact [redacted] by email at [redacted]

CSE's Legal Framework and Security of Information Act

Department of Justice, CSE Legal Services



Directorate of Legal Services (DLS)

- Since 1986, CSE has had in-house legal counsel who are Department of Justice (DOJ) lawyers

- Mission of DOJ:
  - to provide client departments with legal advice; and
  - to ensure that government is administered in accordance with the law and the Constitution

Canadian Charter of Rights and Freedoms

- Applicable to all government departments, agencies and government actions but not to private entities

- CSE must consider and comply with the *Charter* in the course of its activities

- Section 8 of the *Charter* is of particular interest for CSE

  Everyone has the right to be secure against unreasonable search or seizure.

CSE's Authorities

- *National Defence Act* (NDA), Part V.1

  – CSE's Mandate and Mandate Restrictions

  – Ministerial Directives

  – Ministerial Authorizations

CSE's Mandate – section 273.64 NDA

- Threefold mandate of CSE:

  a) to acquire and provide foreign intelligence (SIGINT);

  b) to provide advice, guidance and services to help to ensure the protection of electronic information and information infrastructures of importance to the government of Canada (ITS);

  c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties (Assistance).

CSE Mandate Restrictions

General (s. 273.66)

- CSE may only undertake activities within its mandate, consistent with ministerial direction and consistent with ministerial authorization if required.

A and B Mandates – SIGINT and IT Security (ss. 273.64(2))

- shall not be directed at Canadians or persons in Canada; and
- subject to measures to protect the privacy of Canadians in the use and retention of intercepted information

C Mandate – Assistance (ss. 273.64(3))

- subject to any limitations imposed by law on the agency to whom CSE is providing assistance

Ministerial Directives

- June 2001 – Examples of Some Ministerial Directives (MDs)
  - MD on Accountability Framework (Unclassified)
  - MD on Privacy of Canadians (Unclassified)

- *NDA* now provides that the Minister may issue written directions to the Chief respecting the carrying out of the Chief's duties and functions (ss. 273.62(3))

- MDs have also been issued relating to sensitive operations, relationships and other matters

Ministerial Authorizations (MAs)

- Minister may authorize in writing the interception of private communications in relation to an activity or a class of activities (ss. 273.65(1) and (3))

  – Part VI of the *Criminal Code* does not apply to an interception of a communication under the authority of a MA (s. 273.69).

  – GoC cannot be sued in respect of the use, disclosure or disclosure of the existence of a communication intercepted under the authority of a MA (s. 273.7).

Ministerial Authorizations

Validity

- Up to one year, as specified in the Ministerial Authorization (MA) and may be renewed (s. 273.68(1))
- Minister may vary or cancel at any time (s. 273.68(2))

Conditions

- MA may contain any conditions that the Minister considers advisable to protect the privacy of Canadians (s. 273.65(5))

Support

- Minister may issue written directions to the Canadian Forces to support CSE in carrying out activities under a MA (s. 273.65(6))

Other Acts

- *Privacy Act*
- *Access to Information Act*
- *Security of Information Act*
- *Financial Administration Act*
- *Canadian Human Rights Act & Employment Equity Act*
- *Official Languages Act*

Internal Accountability and External Review

INTERNAL ACCOUNTABILITY:

- Audit and Evaluation
  - Periodic review – operational and administrative
  - Provides assurance that appropriate controls are in place to ensure compliance with law and policy
- Directorate of Legal Services

EXTERNAL REVIEW:

- Independent Review by CSE Commissioner
  - Reviews CSE activities to ensure compliance with the law
- Other External Review
  - E.g., Auditor General, Privacy and Information Commissioners

Security of Information Act

Safeguarded Information

What is Safeguarded Information?

- Information that the Government of Canada or a province is taking measures to safeguard

Pages 70 to / à 73

are withheld pursuant to section

sont retenues en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

Unauthorized Communication

- *R. v. Ratkai*
- *R. v. Delisle*

Page 75

is withheld pursuant to section

est retenue en vertu de l'article

15(1)

of the Access to Information

de la Loi sur l'accès à l'information

QUESTIONS ?

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Access to Information & Privacy (ATIP)

Manager, Communications Services

Access to Information and Privacy (ATIP) Supervisor

Access to Information and Privacy (ATIP) Senior Analyst

Access to Information and Privacy (ATIP) Analyst

Access to Information and Privacy (ATIP) Analyst

Access to Information and Privacy (ATIP) Contractor

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Agenda

- Introduction
- Access to Information Act (ATIA)
- Privacy Act (PA)
- Right of complaint
- Questions

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

INTRODUCTION

To develop an understanding of the:

- Access To Information Act (ATIA)
- Privacy Act (PA)
- Process, authorities and responsibilities under the Acts

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

The Purpose of the *Access to Information Act (ATIA)*

To provide a right of access to information under the control of the Government of Canada in accordance with the principles that:

- Information should be available to the public
- Exceptions should be limited and specific
- Decisions on disclosure should be reviewed independently. (right of complaint)

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

What does ATIP mean to CSEC?

- Subject to the *Acts*.
  - ✓ CSEC, as a federal agency, is bound to uphold the right of access to general records that government controls or to give individuals access to their personal records while protecting their privacy.
  - ✓ All personnel working under CSEC's authority including: staff, co-op students, contractors, integrees, and the Canadian Forces personnel.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Why does the Government of Canada (GOC) provide access?

- To promote a culture of openness, transparency and accessibility to government information.
- Allows Canadians to participate more fully in public policy development.
- Allows Canadians to better assess the Government of Canada's performance.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Who can access government records?

Every person who is:

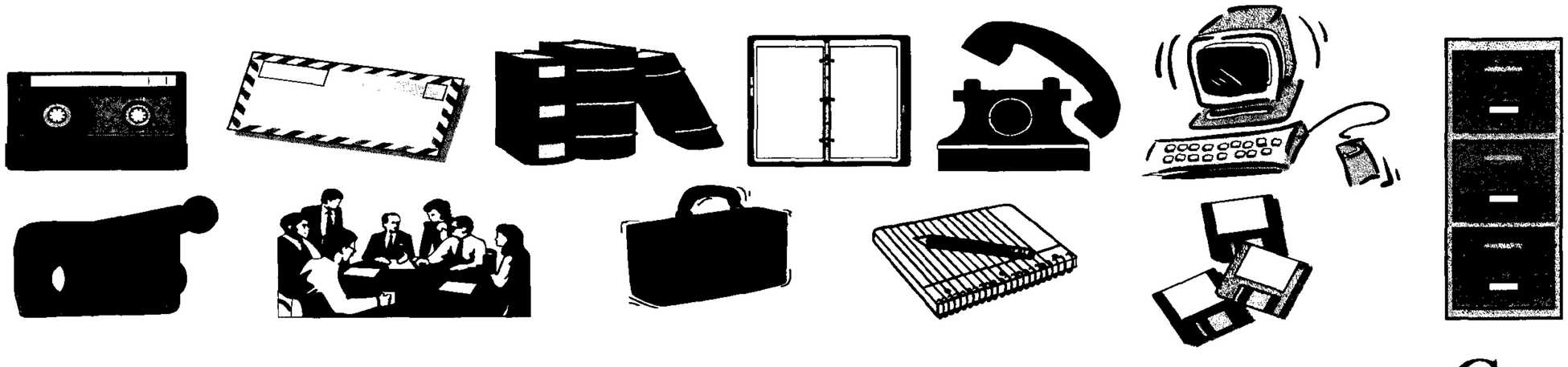
- a Canadian citizen;
- a permanent resident; or
- any individual or corporation present in Canada at the time the request is submitted.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

What is a Record According to the *Acts*?

- "Record" is defined as any documentary material, regardless of medium or form.
- Affects ALL types of records under the custody and control of a government institution, REGARDLESS of security classification level.
- Some examples:



Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

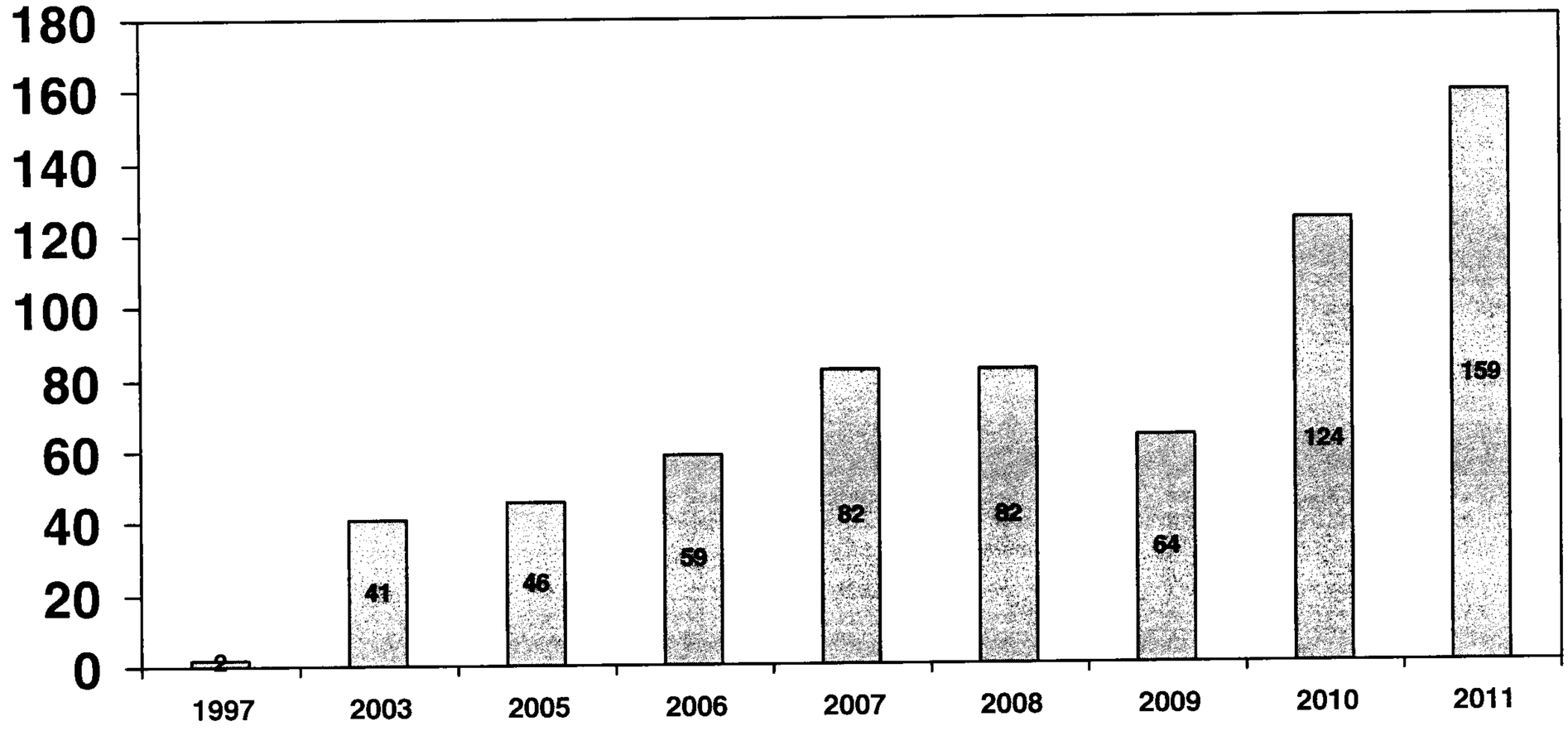
Types of Requests

- Formal: Access and Privacy
- Consultations
- Informal: Access and Privacy
- Parliamentary Inquiries

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Number of Requests



Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Examples of *ATIA* Requests

- "All briefing notes to the Minister and Deputy Minister, media lines, ministerial directives, and correspondence between the CSEC chief and CSEC Commissioner regarding the following subject: a July 28, 2011 news article published in the Globe and Mail, titled "Canadian data used to detect foreign threats", Search from 28 July 2011 to 10 March 2012."
- "The total costs, by conference, incurred by CSEC for any personnel to attend the most recent computer security conferences at:
  - -Black Hats (Las Vegas, Nevada, USA
  - -ShmooCon (Washington DC)
  - -Toorcon (Seattle, Washington/San Diego, California USA)

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

The Purpose of the *Privacy Act (PA)*

- To protect the privacy of individuals.
- To provide individuals with a right of access to personal information about themselves.
- To allow individuals a means of correcting inaccuracies in personal information held by government institutions.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

What is considered personal information?

- ★ home address, home telephone and cell numbers
- ★ age and gender
- ★ marital status
- ★ race, ethnic and national origin
- ★ religious beliefs
- ★ criminal history
- ★ educational and employment history
- ★ financial and medical history
- ★ credit card numbers, debit PINS, other on-line transaction PINS
- ★ fingerprints, blood-type or other biometric identifiers
- ★ any identifiable number including SIN/PRI number
- ★ **views or opinions of another individual about the individual**

Canada

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

Examples of Privacy Requests

- "All records (including, but not limited to, electronic messages, reports, internal and external correspondence, and formal and informal handwritten and computer-generated notes) related to ongoing participation in selection process number: XX-A(BC)2010."

- "All personal information, regardless of format, relating to {John Doe} held by CSE between Jan 2010 and today."

Canada

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

ATIP 101 Exercise

- Only the names of CSEC employees registered in the Government Electronic Directory (GEDS) can be released to the public? **T or F**
- All privacy requests must be made in writing? **T or F**
- The purpose of the *Privacy Act* is to provide individuals with a right of access to personal information about themselves and their family**?**

  T or F
- Correspondence sent to a government institution by an individual, that is of a private and confidential nature is considered personal information? **T or F**
- Personal information is protected up to a period of 10 years after an individual has been deceased? **T or F**
- The classification, salary range and responsibilities of the position held by an individual is not personal information? **T or F**

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

ATIP 101 Exercise

The following excerpts are taken from previously processed ATI and PA requests. Which portions contain personal information?

"Management had plans to meet with employee later this week but the manager, John Smith, had an accident and would not be able to meet the employee as anticipated."

"John Smith, a former employee and currently a contractor, holds a Top Secret clearance. He underwent the required security screening update, including a polygraph test… and he was subsequently cleared to begin work…"

"Good morning Marie, please be advise that Claude is away on course today. She we be back on Monday in case you need to speak to her."

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Parliamentary Inquiries

- Submitted by Members of Parliament or Senate
- Usually given less than 10 days to respond sometimes as little as 24 hours
- ATIP exemptions apply
- Use the same infrastructure as ATIP to process
- Most requests are financial in nature
- Require the Chief's signature
- Consequences of not responding:
  - Minister may be brought before a Standing Committee where he will be asked to justify the lack of or delay in responding

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Exceptions to the *Acts*

- Exclusions
- Exemptions

They exist to provide us with the means to protect classified and or personal information.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Exclusions to the *Acts*

- Published material or material available for purchase by the public.
- Confidences of the Queen's Privy Council for Canada.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Exemptions under the *ATIA*

- Information obtained in confidence (s.13)
- Federal–Provincial Affairs (s.14)
- International Affairs and Defence (s15)
- Law Enforcement and Investigations (s.16)
- Safety of Individuals (s.17)
- Economic Interest of Canada (s.18)
- Personal Information (s.19)
- Third Party Information (s.20)
- Operations of Government - Advice, Recommendations, Deliberations and Plans (s.21)
- Testing and Audits Procedures (s.22)
- Solicitor–Client Privilege (s.23)
- Statutory Prohibitions (s.24)

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Exemptions under the *PA*

- Personal Information Obtained in Confidence (s.19)
- Federal – Provincial Affairs (s.20)
- International Affairs and Defence (s.21)
- Law Enforcements and Investigations (s.22)
- Security Clearance (s.23)
- Individuals Sentenced for a Offence (s. 24)
- Safety of Individuals (s.25)
- Information about another Individual (s.26)
- Solicitor – Client Privilege (s.27)
- Medical records (s.28)

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Provision of "Reasonable Severability"

Section 25 - Severability

"The head of the institution shall disclose any part of the record that does not contain and can reasonably be severed from any part that contains, any such information or material."

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

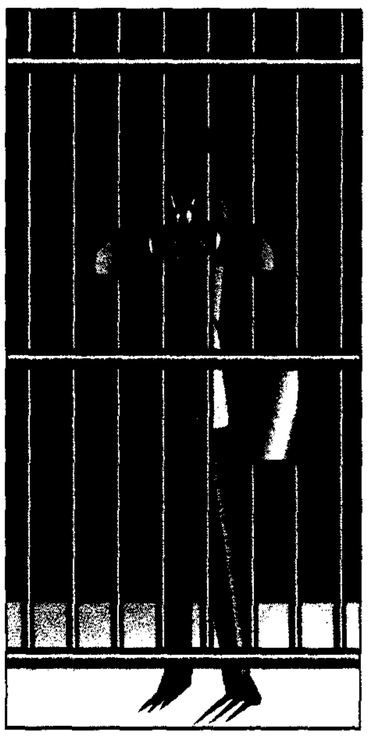
Right of Complaint

- Applicants can submit a complaint to the Office of the:
  - Information Commissioner
  - Privacy Commissioner
- Commissioner may initiate an investigation, if warranted
  - Mediation
  - Federal court

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Do you know you can go to jail because of ATIP?

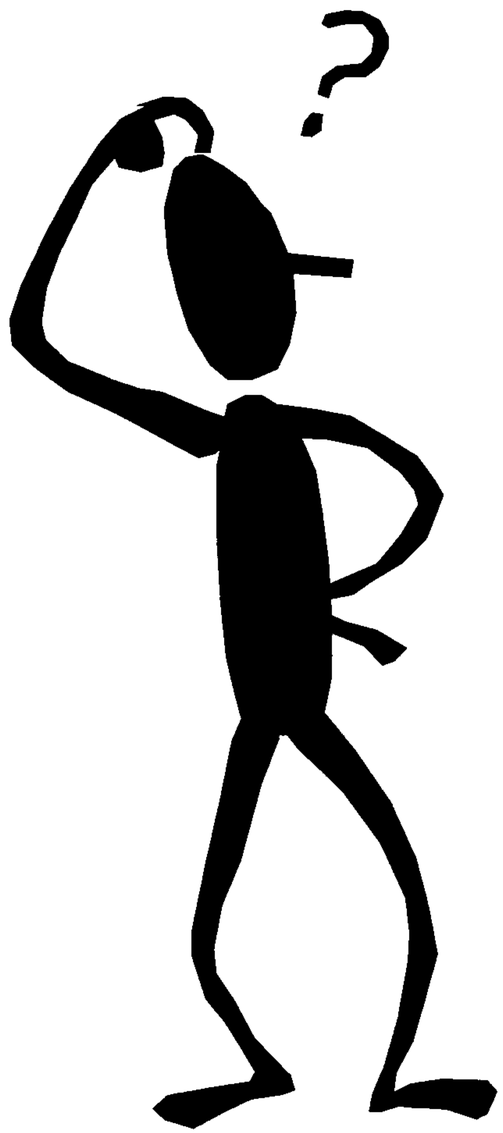


Section 67.1:

- Amended on the 25 March 1999
- To provide criminal sanctions for any person who improperly destroys, mutilates, alters, conceals or falsifies government records with intent to deny the right of access to information under the ATI Act.
- Those convicted of this **indictable offence** described above face a maximum fine of $10,000 and/or two years imprisonment.

Canada

Questions?



Email:

Via the ATIP-Unit group email account

or

[redacted]

Location:

EDB/[redacted]

Communications Security Establishment | Centre de la sécurité des télécommunications

Web 2.0 at CSEC

Web Information Management Services
Information Management Directorate

CIO-DPI

Canada

Agenda

1. What is Web 2.0
2. Our business problem
3. Our approach to Web 2.0
4. Applying Information Management
5. CSEC 2.0 Demo

1. What is Web 2.0?

Communications Security Establishment | Centre de la sécurité des télécommunications

What is Web 2.0?

The **combination** of web technologies allowing users to **contribute** to the **content** of websites resulting in **social networking** and **collaboration**.

Web 2.0 in the Workplace

- Our knowledge is limited to our education, experience, and connections.
- Web 2.0 allows us **to expand our connections**
  - To find people with similar interests
  - To find experts on specific topics
  - To collaborate on content like never before
  - To get feedback from other points of views
- Web 2.0 **increases the quality of our work**.

2. Our business problem

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

CLASSIFICATION: **UNCLASSIFIED**

The numbers

In 2008:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

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

CLASSIFICATION: **UNCLASSIFIED**

Communications Security Establishment | Centre de la sécurité des télécommunications

The intangibles

Communications Security Establishment | Centre de la sécurité des télécommunications

The needs

- Collaboration
- Content integration
- Official languages solution
- Social networking
- Personalization of content
- Blogging and Tweeting
- Multimedia
- Content quality

3. Our approach to 2.0

Communications Security Establishment | Centre de la sécurité des télécommunications

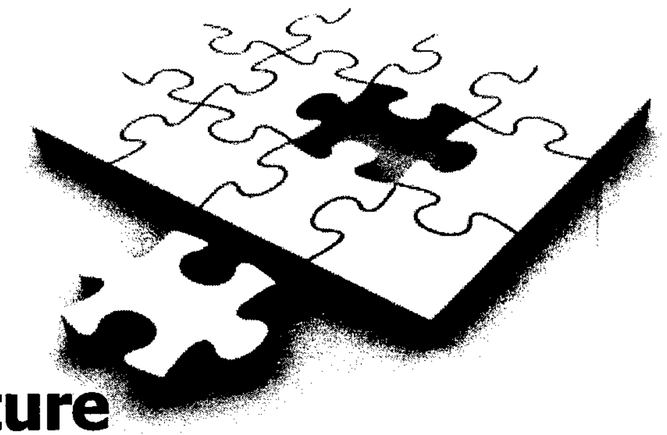
Our approach to Web 2.0

- More than any one buzz word or feature
- We are embracing the nature of Web 2.0
- Relinquishing control of content
- Connecting people
- Merging social networking with corporate web
- Building **one** integrated website as opposed to many separate websites

Communications Security Establishment | Centre de la sécurité des télécommunications

Putting the pieces together

- **Modernize** the intranet **infrastructure** using a Web Content Management System (WCMS) and Web 2.0 technologies
- **Apply Information Management** principles to create content ownership and set retention, disposition, and archival to all content.



- Build a **functional information architecture**
- Enhance **sharing** and **collaboration** within CSEC
- Apply new **CLF 2.0** from the GoC

Communications Security Establishment | Centre de la sécurité des télécommunications

Web 2.0 Technologies

Open source software helping us implement Web 2.0 capabilities **similar** to popular tools


Firefox

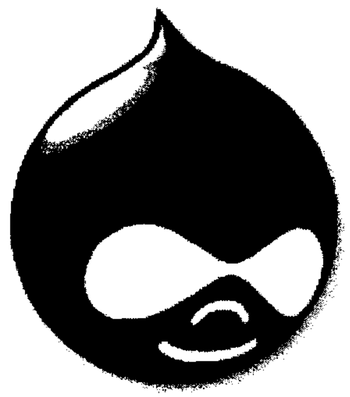

RSS


Video


Instant Messaging


Blogger


Facebook


DRUPAL


Forums


WikiMedia


Twitter


iGoogle Search

CIO-DPI

Canada

Communications Security Establishment | Centre de la sécurité des télécommunications

4. Applying Information Management

Communications Security Establishment | Centre de la sécurité des télécommunications

Applying IM to content

Content Audit

An inventory of your content (links, relationships, owners)

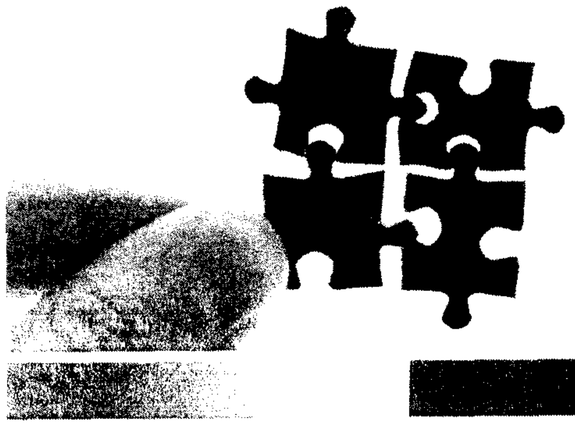
Information Audit

Validating the accuracy, purpose and worthiness of your information

RESULT

Quality Information

Information ready to be published on the web



Canada

New Roles and Responsibilities

Web Publisher ⟶ **Content Publisher**

- Profile: Computer Science ⟶ Profile: Any
- Knowledge of Web languages (i.e. html/xml) ⟶ Knowledge of IM and communication best practices for the Web
- Creates pages using web programming languages ⟶ Creates specific content types using the WCMS templates
- Ensures CLF compliancy ⟶ Automated
- Develops menu and navigation ⟶ Automated
- Reviews content upon request ⟶ Automated
- Edits content upon request ⟶ Delegates editing privileges to and assist content editors

Content Accountability

Web Consultant (WC)

Provides Training

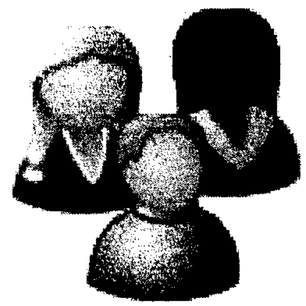
Provides Tech. Support

Content Publishers (CP)

Provides Assistance

Delegates edit permissions

Content Editors (CE)



Web Information Management Services

Anyone that has taken the Content Publisher Course

Any User

Content Stewards (CS)

Identifies

Identifies

Any User

Communications Security Establishment | Centre de la sécurité des télécommunications

Outcomes of Web Modernization

New Web CMS

- Updated web policy
- Content accountability
- Integration of corporate and social
- Automated translation requests
- Content publishers have control over content
- Content publishers can delegate edit permissions
- Email notifications to Content Publisher that have content about-to-expire
- Automatic un-publishing of expired content
- New Web 2.0 Features

5. Demo

Communications Security Establishment
Centre de la sécurité des télécommunications

Questions ?

CIO-DPI

Canada

CHIEF'S OFFICE
BUREAU DU CHEF

LTA PROJECT (DGAP)
DIRECTEUR DE PROJET, INSTALLATION À LONG TERME (ILT)

GENERAL COUNSEL, LEGAL SERVICES (DLS)
AVOCAT GÉNÉRAL, DIRECTION DES SERVICES JURIDIQUES (DSJ)

DG AUDIT, EVALUATION AND ETHICS (DGAEE)
DG, VÉRIFICATION, ÉVALUATION ET ÉTHIQUE (DGVEE)

ASSOCIATE CHIEF CORPORATE SERVICES POLICY AND COMMUNICATIONS (ACCSE)
CHEF ASSOCIÉ, SERVICES CENTRAUX, POLITIQUES ET COMMUNICATIONS (CA SCPC)

DG FINANCE (DGF)
DG, FINANCES (DGF)

DG POLICY AND COMMUNICATIONS (DGPC)
- B, C, D

DG, POLITIQUES ET COMMUNICATIONS (DGPC)
- B, C, D

DG HUMAN RESOURCES (DGHR)
DG, RESSOURCES HUMAINES (DGRH)

CHIEF INFORMATION OFFICER (CIO)
DIRIGEANT PRINCIPAL DE L'INFORMATION (DPI)

DIR INFORMATION MANAGEMENT (CIO-
DIR, GESTION DE L'INFORMATION (DPI-

DIR PROGRAM MANAGEMENT (CIO-
DIR, GESTION DES PROGRAMMES (DPI-

DG TECHNOLOGY AND ENTERPRISE SOLUTIONS (CIO-
DG, TECHNOLOGIES ET SOLUTIONS D'ENTREPRISE (DPI-

DEPUTY CHIEF IT SECURITY (ITS)
CHEF ADJOINT, SÉCURITÉ DES TI (STI)

DG CYBER DEFENCE
- Cyber Defence Operations (CDO)
- Cyber Threat Evaluation Center (CTEC)

DG, CYBERDÉFENSE
- Opérations de cyberdéfense (OCD)
- Centre d'évaluation des cybermenaces (CEC)

DIRECTOR ITS PROGRAM MANAGEMENT & OVERSIGHT
- PMO, IPOC

DIRECTEUR, GESTION ET CONFORMITÉ DU PROGRAMME
- GCP, BSAC

STRATEGIC RELATIONS OFFICE (SRO)
BUREAU DES RELATIONS STRATÉGIQUES (BRS)

DG CYBER PROTECTION
- ATA, M, T

DG, CYBERPROTECTION
- ATA, M, T

DEPUTY CHIEF SIGINT (SIGINT)
CHEF ADJOINT, SIGINT

DG MILITARY SIGINT (DGMS)
DG, SIGINT MILITAIRE (DGSM)

DG INTELLIGENCE (DGI)
DG, RENSEIGNEMENT (DGR)

DG SIGINT PROGRAMS (DGP)
DG, PROGRAMMES SIGINT (DGP)

Commonly used acronyms at CSEC / Acronymes les plus utilisés au CSTC

ENGLISH / ANGLAIS	FRENCH / FRANÇAIS
ADCS Associate Deputy Chief SIGINT	**SCA SIGINT** Sous-chef adjoint SIGINT
ADM Associate Deputy Minister	**SMA** Sous-ministre adjoint(e)
ANT Advanced Network Tradecraft	**ANT** Savoir-faire avancé en matière de réseaux
AO Administrative Officer	**AA** Agent(e) administratif (ive)
ATIP Access to Information and Privacy	**AIPRP** Accès à l'information et protection des renseignments personnels
AUSLO Australian Liaison Office (Australia)	**AUSLO** Australian Liaison Office (Australie)
BCM Briefcase Move	**DV** Déménagement valise
BCP Business Continuity Planning	**PCA** Planification de la continuité des activités
BRMO Business Relationship Management Office	**BGRA** Bureau de la gestion des relations d'affaires
BRLO British Liaison Office	**BRLO** Bureau de liaison Britannique
C2C Computer-to-computer	**C2C** Communication entre ordinateurs
CANSLO Canadian Senior Liaison Office	**CANSLO** Bureau spécial de liaison du Canada
CANUKUS Canada / UK / USA Security Agreement	**CANUKUS** Entente sur la sécurité entre le Canada, le Royaume-Uni et les États-Unis
CAP Counseling Advisory Program	**PCO** Programme de consultation et d'orientation
CAPIA Canadian Association of Professional Intelligence Analysts	**ACAPR** Association canadienne des analystes professionnels du renseignement
CBM Competency-Based Management	**GAC** Gestion axée sur les compétences
CBNRC Communications Branch, National Research Council (CSEC's predecessor)	**DTCNRC** Direction des télécommunications du Conseil national de recherches du Canada (prédécesseur du CSTC)
CBSA Canada Border Services Agency	**ASFC** Agence des services frontaliers du Canada
CCMP Canadian Cryptographic Modernization Program	**PCMPC** Programme canadien de modernisation des produits cryptographiques
CDI Chief of Defence Intelligence (DND)	**CRD** Chef du renseignement de la Défense (MDN)
CEO Canadian Eyes Only	**CEO** Réservé au Canadiens
CERT Computer Emergency Response Team	**CERT** Équipe d'action à l'urgence informatique
CF Canadian Forces	**FC** Forces canadiennes
CFCSU Canadian Forces Crypto Support Unit	**USCFC** Unité de soutien cryptographique des forces canadiennes
CFEWC Canadian Forces Electronic Warfare Centre	**CGEFC** Centre de guerre électronique des Forces canadiennes
CFIOG Canadian Forces Information Operations Group	**GOIFC** Groupes des opérations de l'information des Forces canadiennes
CFSOC Canadian Forces SIGINT Operations Centre	**COSFC** Centre des opérations SIGINT des Forces canadiennes
CI Criminal Intelligence or Counter Intelligence	**CI** Contre-ingérence ou renseignement criminel
CIO Chief Information Office	**DPI** Bureau de la dirigeante principale de l'information
CNO Computer Network Operations	**CNO** Opérations liées aux réseaux informatiques
COMINT Communications Intelligence	**COMINT** Communications de renseignements
COMPUSEC Computer Security	**COMPUSEC** Sécurité informatique
COMSAT Communications Satellite	**COMSAT** Satellite de télécommunications
COMSEC Communications Security	**COMSEC** Sécurité des télécommunications électroniques
COTS Commercial Off-the-Shelf	**COTS** Commercial sur étagère
CPP Canada Post Place	**PPC** Place Postes Canada
CRI Cryptologic Research Institute	**IRC** Institut de recherche cryptologique
CRM Client Relations Management	**GRAC** Gestion des relations avec la clientèle
CRO Customer Relations Officer	**ARC** Agent des relations avec la clientèle
CS Corporate Services	**SC** Services centraux

CSIS Canadian Security Intelligence Service	**SCRS** Service canadien du renseignement de sécurité
CT Counter Terrorism	**AT** Anti-terrorisme
CVAN CSE Visitor Access Notification	**DLVC** Demande de laissez-passer de visiteurs au CST
DFAIT Department of Foreign Affairs and International Trade	**MAECI** Ministère des Affaires étrangères et commerce international
DGPC Director General, Policy & Communications	**DGPC** Directeur général, Politiques et communications
DM Deputy Minister	**MA** Ministre adjoint(e)
DND Department of National Defence	**MDN** Ministère de la Défense nationale
DNI Digital Network Intelligence	**DNI** renseignement de réseaux numériques
DSD Defence Signals Directorate (Australia)	**DSD** Defence Signals Directorate (Australie)
EA Executive Assistant	**AE** adjoint exécutif; adjointe exécutive
EDB Edward Drake building	**EDB** Édifice Edward Drake
ELINT Electronic Intelligence	**ELINT** Renseignement électronique
EPR End-Product Report	**RPF** Rapport produit fini
EXCOM Executive Committee	**COMEX** Comité exécutif

FAMIS Financial and Asset Management Information System	**FAMIS** Système d'information de gestion financière et des biens
FI Foreign Intelligence	**FI** Renseignement étranger
FINTRAC Financial Transactions & Reports and Analysis Centre	**CANAFE** Centre d'analyse des opérations et déclarations financières du Canada
FIPS Foreign Intelligence Priorities	**PRE** Priorités en matière de renseignement étranger
FISA Foreign Intelligence Surveillance Act (US)	**FISA** Foreign Intelligence Surveillance Act (US)
FISINT Foreign Instrumentation Intelligence	**FISINT** Renseignement tiré de signaux d'instrumentation étrangers
FLIP Foreign Language Incentive Plan	**RILE** Régime d'incitation pour les langues étrangères
FOUO For Official Use Only	**FOUO** Réservé à des fins officielles
FSP Foreign Services Program	**PSE** Programme du service extérieur
FTE Full-time equivalent	**ETP** Équivalent temps plein
FTP File Transfer Protocol	**FTP** Protocole de transfert de fichier
GCHQ Government Communications Headquarters (UK)	**GCHQ** Government Communications Headquarters (UK)
GCR Government of Canada Requirement	**BGC** Besoins du gouvernement du Canada

GCSB Government Communications Security Bureau (New Zealand)	**GCSB** Government Communications Security Bureau (New Zealand)
GCWCC Government of Canada Workplace Charitable Campaign	**CCMTGC** Campagne de charité en matière de travail du gouvernement du Canada
GII Global Information Infrastructure	**IMI** Infrastructure mondiale d'information
GOC Government of Canada	**GC** Gouvernement du Canada
GOTS Government Off-the-Shelf	**GOTS** Gouvernemental sur étagère
GSA Global Security Agenda	**PSM** Programme de sécurité mondial
GSO Group Security Officer	**ASG** Agent de sécurité de groupe
GSP Government Security Policy	**PGS** Politique de gouvernement sur la sécurité
GSM Global System for Mobile communications	**GSM** Système mondial de communications mobiles
HR Human Resources	**RH** Ressources humaines
HRSR Human Resources Service Request	**DSRH** Demande de service en ressources humaines
HUMINT Human Intelligence	**HUMINT** Renseignement humain
IAC Intelligence Advisory Committee	**CCR** Comité consultative du renseignement

IB Insurance Building	**IA** Immeuble des Assurances
ICSI Interdepartmental Committee on Security and Intelligence	**CISR** Comité interministériel de la sécurité et du renseignement
IM/IT Information Management/ Information Technology	**GI/TI** Gestion de l'information/ Technologie de l'information
INFOSEC Information Security	**INFOSEC** Sécurité de l'information
INMARSAT International Maritime Satellite Organization or International Mobile Satellite Organization	**INMARSAT** Télécommunications mobiles par satellites
IPG Intelligence Policy Group	**GPR** Groupe sur la politique du renseignement
ISDN Integrated Services Digital Network	**RNIS** Réseau numérique à l'intégration de services
ISI Intelligence Source Identifier	**ISI** Indicateur de source de renseignement
ISOM Integrated SIGINT Operational Model	**MOIS** Modèle opérationnel intégré SIGINT
ISP Internet Service Provider	**FSI** Fournisseur de services internet
ITAC Integrated Threat Assessment Centre	**CIEM** Centre intégré d'évaluation des menaces
ITS Information Technology Security	**STI** Sécurité des technologies de l'information
ITSEC Information Technology Security Evaluation Criteria	**CTSRI** Comité des techniques de sécurité relatives à l'information

JCC Joint Consultation Committee	**CCM** Comité consultatif mixte
L&D Learning & Development	**A&D** Apprentissage & Développement
LDAP Lightweight Directory Access Protocol	**LDAP** Protocole allégé d'accès annuaire
LDP Leadership Development Program	**PDL** Programme de développement en Leadership
LIA Leave with income averaging	**CER** Congé avec étalement du revenu
LO Liaison Officer	**LO** Agent(e) de liaison
LTA Long-Term Accomodation	**ILT** L'installation à long terme
MA Market Allowance	**MA** Indemnité en fonction du marché
MC Memorandum to Cabinet	**MC** Mémoire au Cabinet
MFA Ministry of Foreign Affairs	**MAE** Ministère des affaires étrangères
MOD Ministry of Defence	**MDN** Ministère de la défense nationale
MOU Memorandum Of Understanding	**PE** Protocle d'entente
MTA Mid-Term Accomodation	**IMT** Installation à moyen terme
MTF Management Team Forum	**TEG** Tribube de l'équipe de gestion

NCPAT National COMSEC Procedures, Audits and Training	**PVFCN** Bureau des procédures, des vérifications et de la formation COMSEC à l'échelle nationale
NDHQ National Defence Headquarters	**QGDN** Quartier général de la Défense nationale
NSA National Security Agency (US)	**NSA** Service SIGINT américain
NSPL National SIGINT Priorities List	**LPSN** Liste des priorités SIGINT nationales
NZLOW New Zealand Liaison Office (Washington)	**NZLOW** Bureau de liaison de la Nouvelle-Zélande à Washington
OCT Office of Counter Terrorism	**BAT** Bureau de l'antiterrorisme
OHS Occupational Health & Safety	**SST** Santé et sécurité au travail
OL Official Languages	**LO** Langues officielles
OPI Office of Primary Interest	**BPR** Bureau de première responsabilité
PA Performance Agreement	**ER** Entente de rendement
PCO Privy Council Office	**BCP** Bureau de Conseil privé

PDA Personal Digital Assistant	**PDA** Agenda électronique
PID Portable Information Device	**DIP** Dispositif d'information personnel
PIQ Position Information Questionnaire	**QRP** Questionnaire de renseignements sur le poste
PKI Public Key Infrastructure	**ICP** Infrastructure à clé publique
PMO Prime Minister's Office	**CPM** Cabinet du Premier ministre
PPR Performance Planning and Review	**PER** Planification et examen du rendement
PPRC People Planning and Resources Committee	**CEPR** Comité des effectifs, de la planification et des ressources
PQP Pre-Qualified Pool	**RCP** Répertoire de candidats préqualifiés
PR Purchase Requisition	**DD** Demande d'achat
PRI Personal Record Identifier	**CIDP** Code d'identification de dossier personnel
PSAC Public Service Alliance of Canada	**AFPC** Alliance de la fonction publique du Canada
PSEPC Public Safety and Emergency Preparedness Canada	**SPPCC** Sécurité publique et Protection civile Canada
RCMP Royal Canadian Mounted Police	**GRC** Gendarmerie Royale du Canada
RDIMS Records Document Information Management System	**SGDDI** Système de gestion des dossiers, des documents et de l'information
RoD Record of Decision	**RoD** Compte rendu de décisions

RFI Request for Information	**DI** Demande d'information
RFP Request for Proposal	**RFP** Appel d'offres
S&I Security and Intelligence	**S&I** Sécurité et renseignement
SA Special Access	**AS** Accès spécial
SAFP SIGINT Adjunct Faculty Program	**PEAS** Programme d'enseignement auxiliaire SIGINT
SAGA Strength & Gap Analysis (Underfill document)	**AFE** Analyse des forces et des écarts (document de sous-classement)
SAPP Special Assignment Pay Plan	**PRAS** Programme de rémunération d'affectation spéciale
SAWUNEH Summer Analytic Workshop Up North Eh	**SAWUNEH** Summer Analytic Workshop Up North Eh
SCIP Secure Communications Interoperability Protocol	**SCIP** Protocole d'interopérabilité des communications sécurisées
SDdev SIGINT Development	**SD** Développement SIGINT
SGSM Global System for Mobile communications	**SGSM** Sécurité de système mondial de communications mobiles
SI Security Intelligence or Special Intelligence	**SI** Renseignement de sécurité ou renseignment spécial
SIGINT Signals Intelligence	**SIGINT** Renseignement électromagnétique

SIRC Security & Intelligence Review Committee	**CSARS** Comité de surveillance des activités de renseignement de sécurité
SLA Service Level Agreement	**SLA** Accord sur les niveaux de service
SLA Support to Lawful Access	**SAL** Soutien à l'accès légal
SLLP Second Language Learning Program	**PFLS** Programme formation linguistique en langue seconde
SLT Sir Leonard Tilley (building)	**SLT** Sir Leonard Tilley (édifice)
SMART (objectives) Specific, Measurable, Attainable, Realistic & Timely	**(objectif) SMART** Spécifique, mesurable, réalisable, réaliste et limité dans le temps
SME Subject Matter Expert	**SME** Spécialiste
SMO Support to Military Operations	**SOM** Soutien aux opérations militaires
SMT Senior Management Team	**EGS** Équipe de la gestion supérieure
SOQ Statement of Qualifications	**EQ** Énoncé de qualité
SOW Statement of Work	**ET** Énoncé des travaux
STA Short-Term Accomodation	**ICT** Installation à court terme
STE Secure Terminal Equipment	**STE** Appareil terminal sécurisé
STU Secure Telephone Unit	**STU** Poste téléphonique protégé

s.15(1)

SUSLOO Special US Liaison Office Ottawa	**SUSLOO** Bureau spécial de liaison des États-Unis à Ottawa
SWE Salary Wage Envelope	**ES** Enveloppe salariale
SWOT Strengths, Weaknesses, Opportunities & Threats	**SWOT** Forces, faiblesses, possibilités et menaces
TL Team (or Task) Leader	**TL** Chef d'équipe
TSSA Top Secret SIGINT Access	**TSSA** Très secret, accès SIGINT
UNDE Union of National Defence Employees	**UEDN** Union des employés de la Défense nationale
VOIP Voice Over Internet Protocol	**VOIP** Voix sur IP

LTA PROJECT (DGAP) – Director General Accommodations Project

[redacted]

DG Policy & Communications (DGPC)

B – Strategic Policy
B1 – Strategic Policy

C – Communications

C1 – Communications Support Services
C1A – Visual Communications
C1D – Linguistic Services

C2 – Communications

D – Disclosure, Policy and Review

D1 – Disclosure Management
D1A – Legal Disclosures
D1B – Access to Information and Privacy Office (ATIP)

D2 – Corporate and Operational Policy
D2A – Privacy and Interests Protection
D2B – Policy Management

D3 – External Review

DLS – Director Legal Services

DGAEE – Director General Audit & Evaluation, & Ethics

DAE – Director Audit & Evaluation
DAE1 – Audit
DAE2 – Evaluation

DEPUTY CHIEF CORPORATE SERVICES (DCCS)

DG Corporate Services Operations (CSOPS)

DCS – Director Corporate Security & Safety

[redacted]

S2 – Personnel Security

[redacted]

S3 – Security Education & Awareness

S4 – Security Secretariat

F – Assets Management

F1 – Program Implementation
F2 – Strategic Outlook & Planning
F3 – Realty Operations
F4 – Material Management
- **F4A –** Shipping and Receiving Mail
- **F4B –** Warehouse and Shuttle Services

F5 – Facilities Service Management
F6 – Facilities Service Delivery

O – CSPC Program Management

O1 – Emergency Management Office
O2 – Business Management

DG Finance (DGF)

DFO – Financial Operations

DFO1 – Accounting Operations
- **DFO1A –** Financial Analysis
- **DFO1B –** Financial Analysis

DFO1B1 – Accounts Payable / Travel and Relocation
DFO2 – Financial Systems
DFO2A – Financial Analysis
W3 – Contracting & Procurement

DRM – Resource Management
DRM3 – Costing, Budgeting & Reporting
W1B – External Financial Services

DSPMM (W5) – Strategic Planning & Modern Management
W5A – Integrated Management and Reporting
W5B – Integrated Planning and Coordination

DG Human Resources (DGHR)

HRCAP – Counselling & Advisory Program

HRCS – Client Services
HRCS1
HRCS2
HRCS3
HRCS4
HRCS5

HRP – Programs
HRP1 – Labour Relations, Occupational Health & Safety and Compensation
HRP2 – Staffing Programs
HRP3 – Organizational Design and Classification
HRP4 – Policy and Foreign Services

CHIEF INFORMATION OFFICER (CIO)

Information Management (CIO-

CIO-

CIO-
CIO-
CIO-

s.15(1)

SECRET

CIO-[redacted]
CIO-[redacted]
CIO-[redacted]

CIO-[redacted]
CIO-[redacted]
CIO-[redacted]

[redacted] *(CIO-*[redacted]

CIO-[redacted]
CIO-[redacted]
CIO-[redacted]
CIO-[redacted]

CIO-[redacted]
CIO-[redacted]
CIO-[redacted]
CIO-[redacted]

CIO-[redacted]

[redacted] *(CIO-*[redacted]

CIO-[redacted]
CIO-[redacted]
CIO-[redacted]
CIO-[redacted]

CIO-[redacted]
CIO-[redacted]
CIO-[redacted]

[redacted] *(CIO-*[redacted]

CIO-[redacted]
CIO-[redacted]

Program Management (CIO-[redacted]

CIO-[redacted]
CIO-[redacted]
CIO-[redacted]

CIO-
CIO-
CIO-
CIO-

CIO-

CIO-
CIO-
CIO-

CIO-
CIO-
CIO-

CIO-
CIO-
CIO-

DG Technology & Enterprise Solutions (CIO

CIO
CIO-
CIO-

DEPUTY CHIEF IT SECURITY (ITS)

DG Cyber Defence

CDO – Cyber Defence Operations

CDO
CDO
CDO
CDO
CDO

CDO
CDO2
CDO2
CDO2

CDO
CDO
CDO

s.15(1)

SECRET

CDO [redacted]

CTEC – Cyber Threat Evaluation Centre

CTEC [redacted]

CTEC [redacted]

CTEC [redacted]

CTEC [redacted]

CTEC [redacted]

CTEC [redacted]

CTEC [redacted]

CTEC [redacted]

DG Cyber Protection

ATA – Architecture & Technology Assurance

ATA [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

AT [redacted]

AT [redacted]

AT [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

ATA [redacted]

AT [redacted]

AT [redacted]

AT [redacted]

[redacted] - Crypto Material Systems & Services

[redacted]

[redacted]

[redacted] - Canadian Cryptographic Modernization Program (CCMP)

Director ITS Program Management & Oversight (PMO)

PMO – Program Management & Oversight

PMO[redacted]
PMO[redacted]
PMO[redacted]

PMO[redacted]
PMO[redacted]

[redacted]

Strategic Relations Office (SRO)

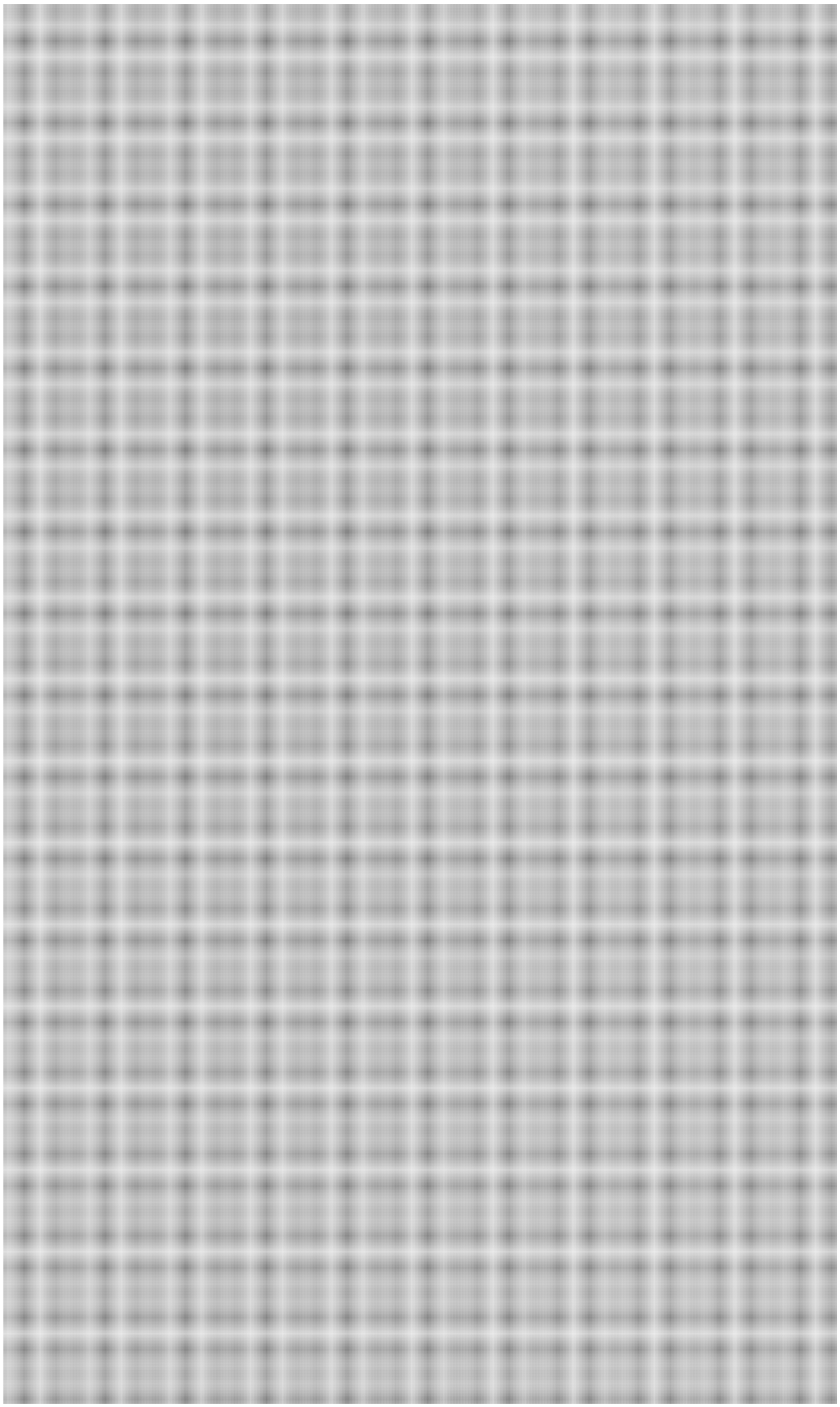
DEPUTY CHIEF SIGINT (SIGINT)

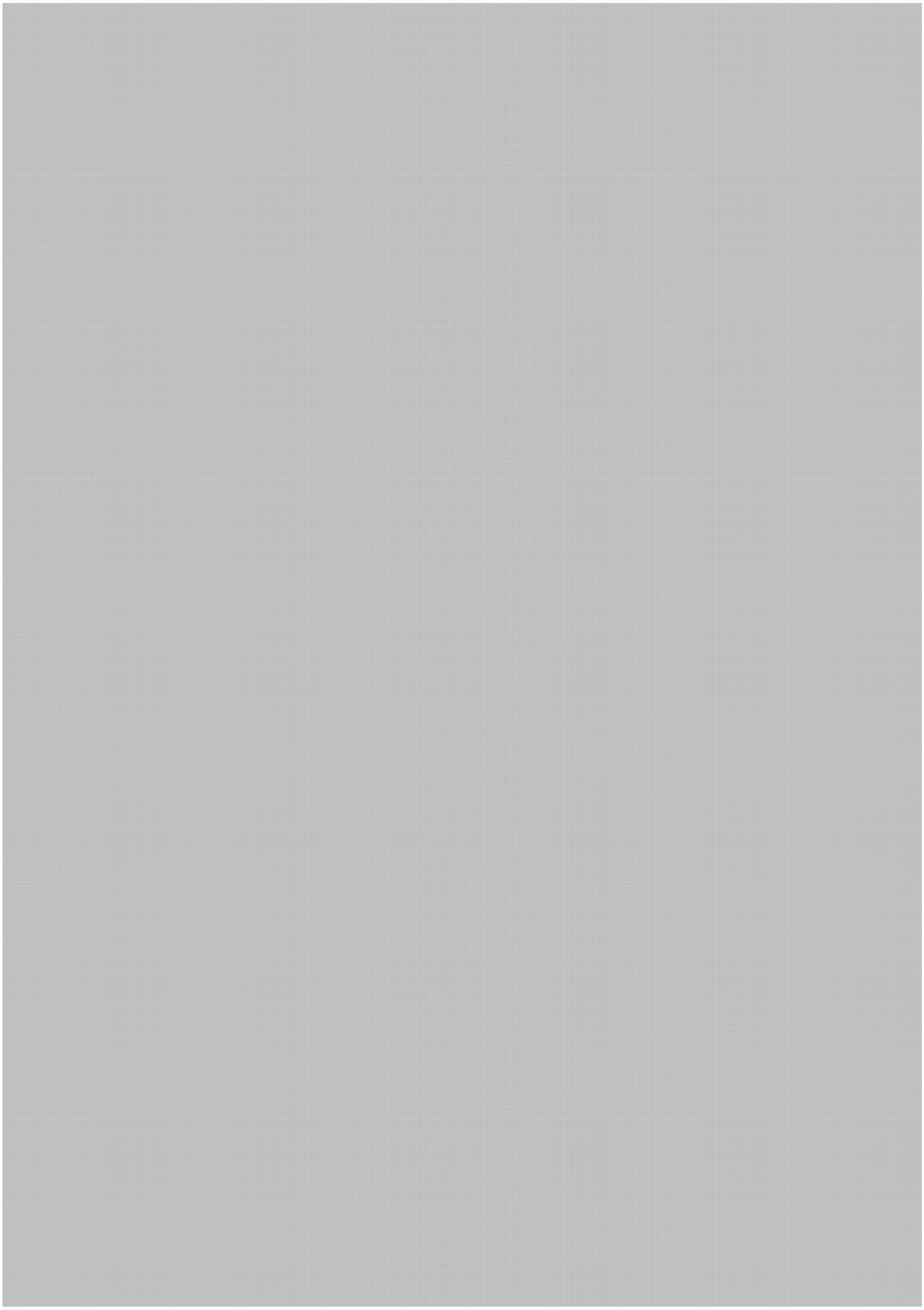
DG [redacted]

[redacted]

s.15(1)

SECRET





[redacted]

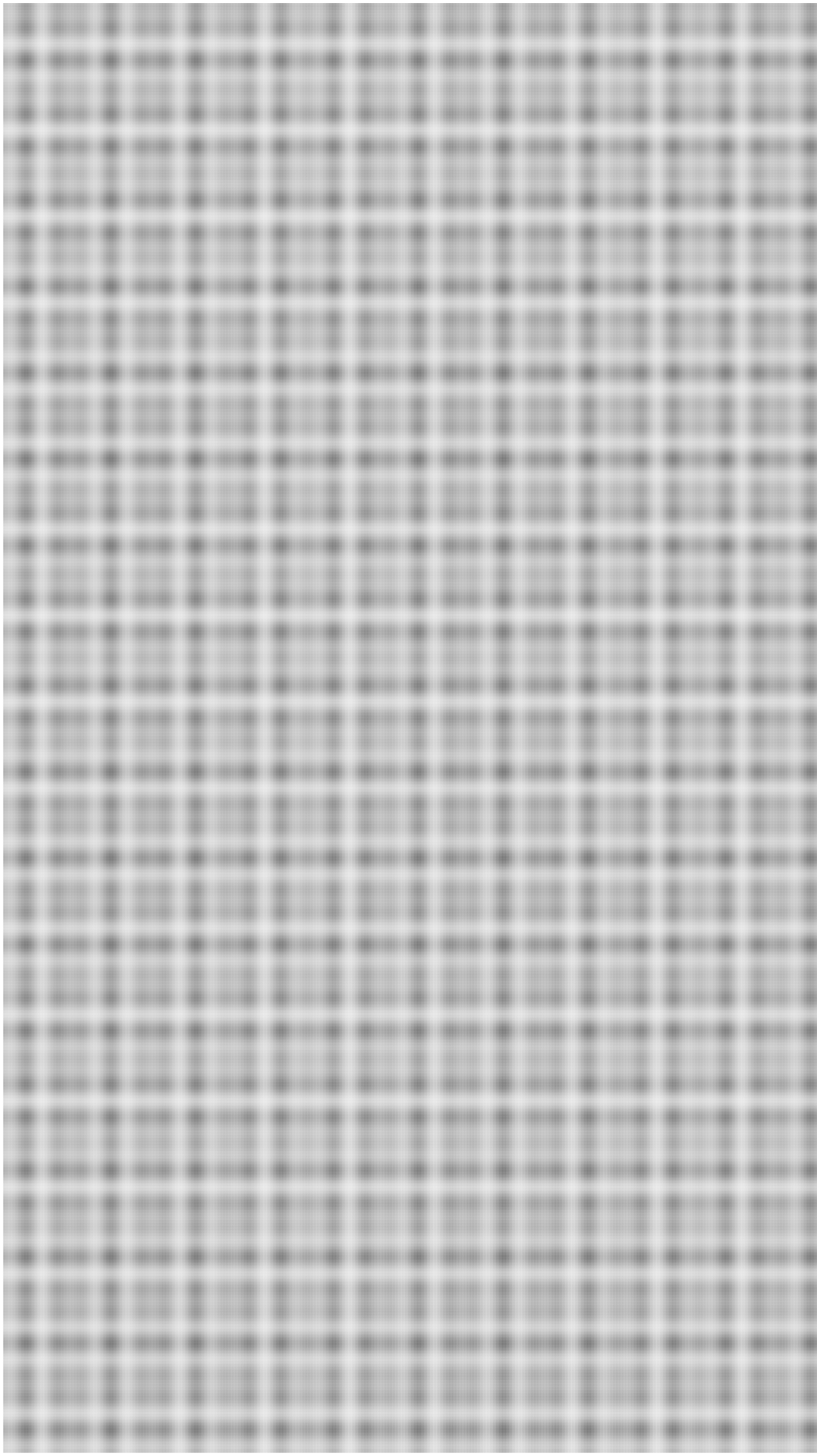
TIMC – Tutte Institute for Mathematics and Computing

DGMS – DG Military SIGINT

DG Intelligence (DGI)

[redacted]

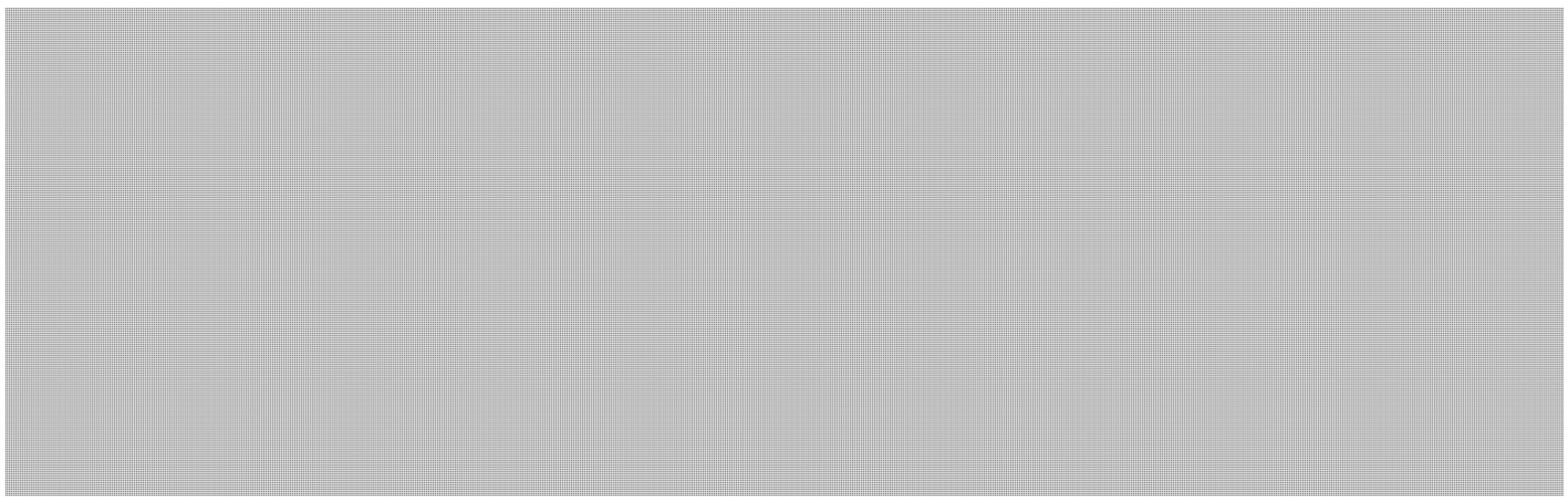
SECRET



[redacted]

DG SIGINT Programs (DGP)

[redacted]



CTEC

CYBER THREAT EVALUATION CENTRE

A world-class workplace for a world-class workforce
Un milieu moderne à l'appui d'un effectif moderne

[redacted]

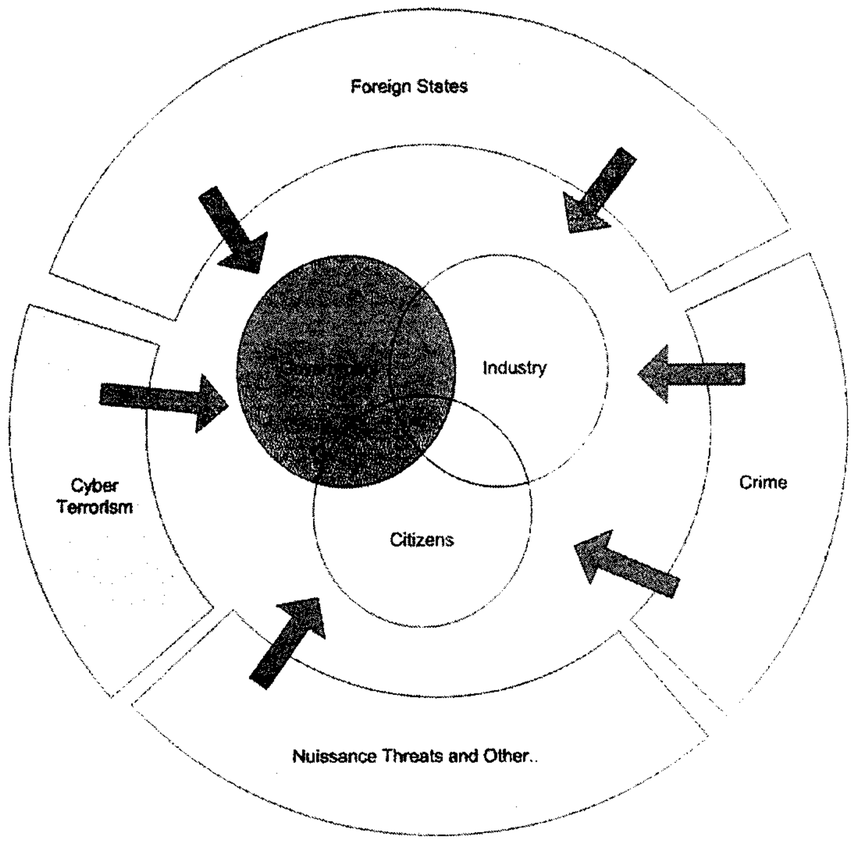
CTEC
CYBER THREAT EVALUATION CENTRE

✓ Cyber security center for the Government of Canada (GC-CTEC)

- operations
- SA
- threat knowledge

✓ Provide protection to government departments.

✓ Help departments protect themselves.



A world-class workplace for a world-class workforce
Un milieu moderne à l'appui d'un effectif moderne

Pages 143 to / à 151

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

de la Loi sur l'accès à l'information

CTEC

CYBER THREAT EVALUATION CENTRE

A world-class workplace for a world-class workforce
Un milieu moderne à l'appui d'un effectif moderne

Pages 153 to / à 160

are withheld pursuant to sections

sont retenues en vertu des articles

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

of the Access to Information

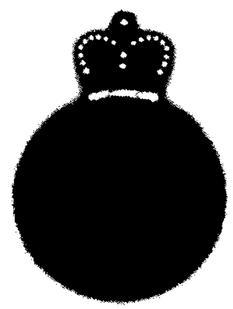
de la Loi sur l'accès à l'information

Computer Network Defence

(putting the "sigh" in cyber)

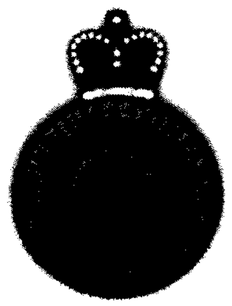
[redacted]
Team Lead, Cyber Threat Detection
Cyber Threat Evaluation Centre (CTEC) ITS

[redacted]@cse-cst.gc.ca [redacted]



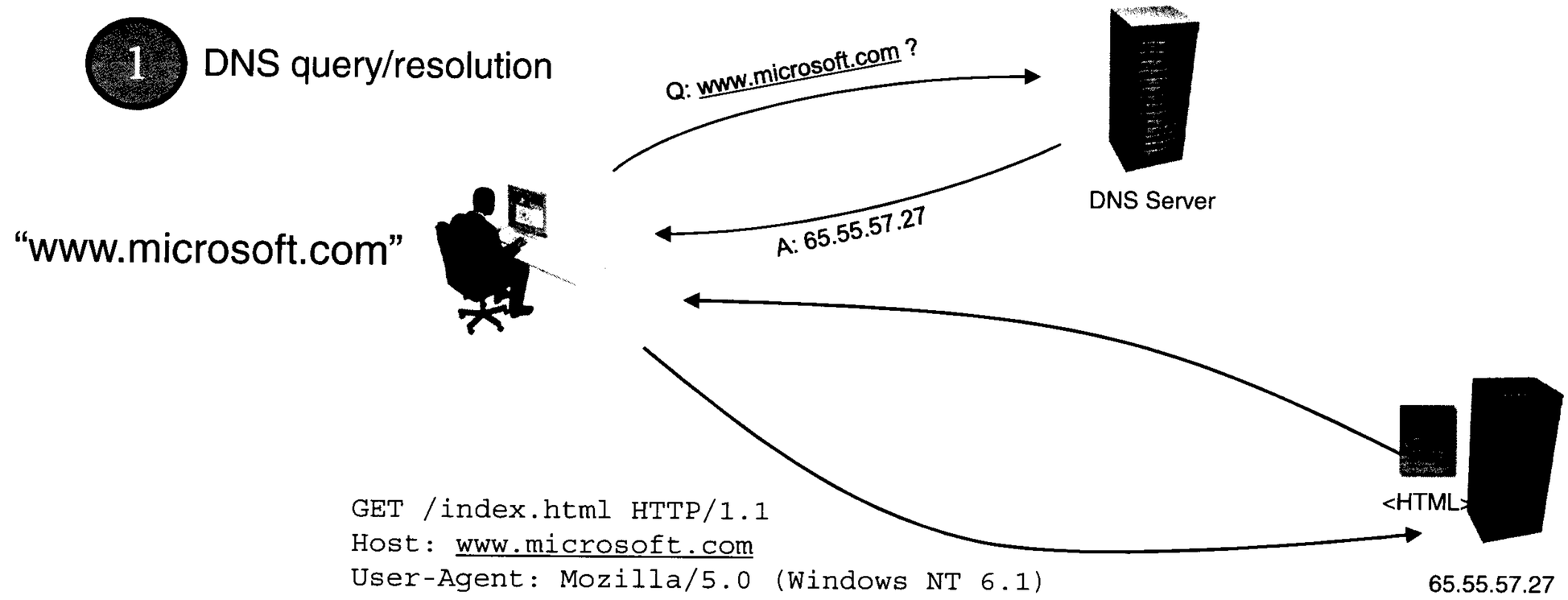
Cyber Lingo

- **IP Address: 204.125.67.15**
  4 'octets', each ranges from 0-255. IP is registered to a network owner
- **Domain Name: www.microsoft.com**
  Much more relatable than 64.4.11.42, no?
- **DNS: Domain Name System**
  Worldwide network to 'resolve' domain names (www.microsoft.com)
  To IP addresses.
- **Packets: "chunks" of network traffic**
  Think of an envelope with addressing info, and content inside
- **HTTP: Hyper Text Transfer Protocol**
  This is how we browse the web (GET, POST, 404, etc)

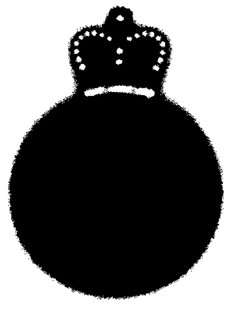


This is how we browse the web

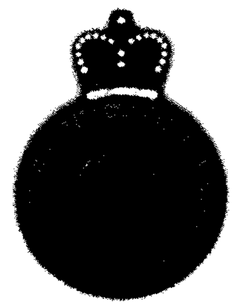
1 DNS query/resolution



2 HTTP request/response

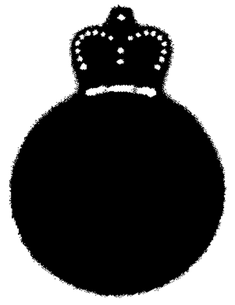


DEMO



Cyber Compromises

- Spear phishing (emails containing:)
  - Trojanised attachments
  - Malicious links
    - To trojanised files hosted on a server
    - To web pages crafted to compromise the browser
- Web Site seeding
- Server compromises (SQL injection, others)



Ripped from the Headlines

(more or less)

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

UNCLASSIFIED
CSEC Official Use Only

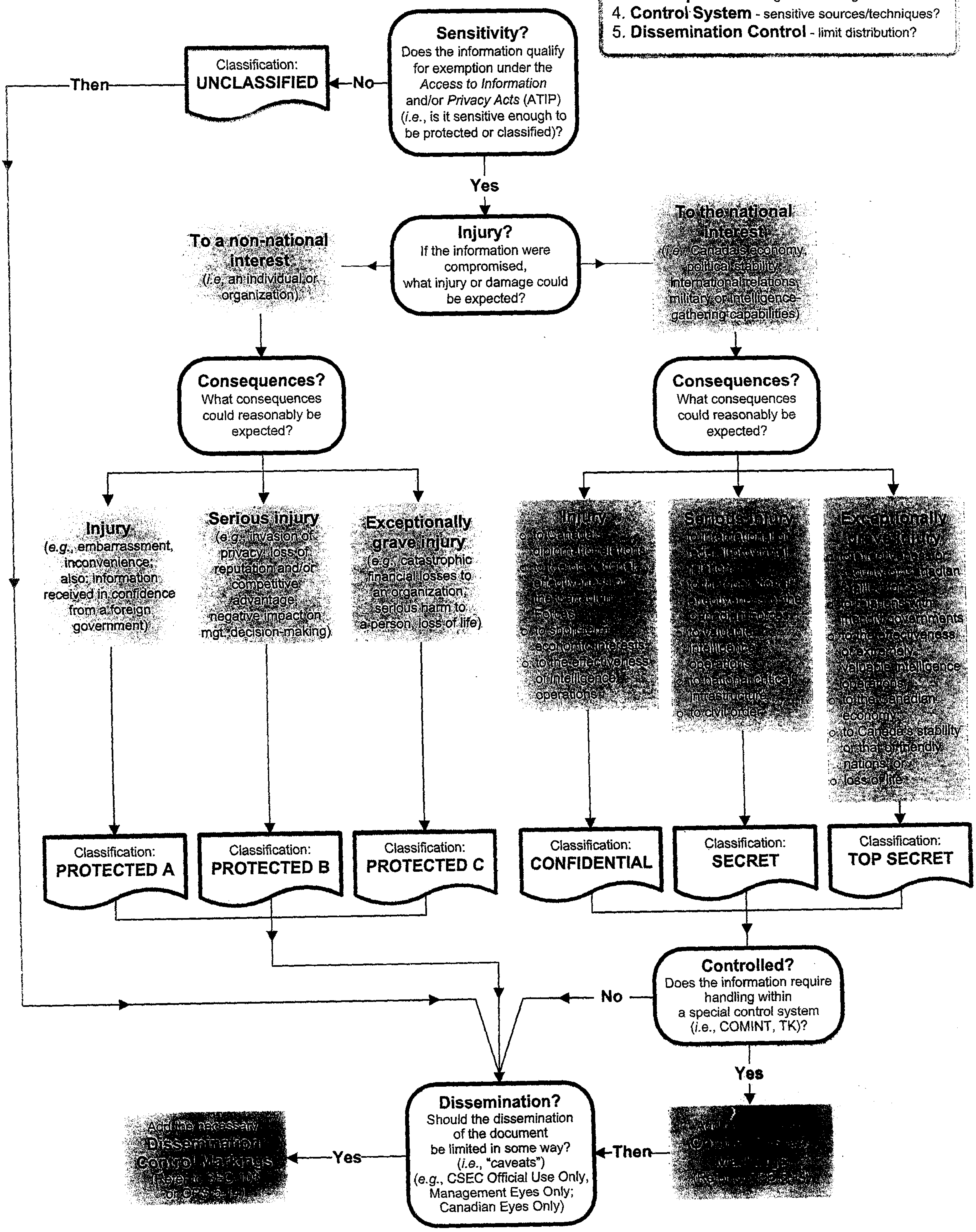
SEC-103 Classifying Information - Annex 1

How to Classify Information

It's up to you, the originator, to classify any information you produce. This chart walks you through the steps for making that judgement.

Things to think about as you decide:

1. **Sensitivity** - meet any ATIP exemptions?
2. **Injury** - to the national interest or not?
3. **Consequences** - degree of damage?
4. **Control System** - sensitive sources/techniques?
5. **Dissemination Control** - limit distribution?



Need Help? Check similar documents, consult more experienced colleagues, ask your manager.
Still have questions? Contact **Corporate Security** via ARS re: SEC-103. Contact [redacted] re: OPS-5-14.

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

SEC-103 **Classification des renseignements - Annexe 1**

NON CLASSIFIÉ
À des fins officielles du CSTC

Comment classifier des renseignements

Il incombe à l'auteur de classifier les renseignements qu'il produit. Ce diagramme vous présente les étapes à suivre pour vous assurer de prendre des bonnes décisions.

Choses auxquelles penser avant de prendre une décision :

1. **Sensibilité** - *les renseignements sont-ils exemptés* des lois sur l'AIPRP?
2. **Préjudice** - les renseignements pourraient-ils nuire à l'intérêt national ou non?
3. **Conséquences** - niveau de dommage?
4. **Système de contrôle** - sources/techniques sensibles?
5. **Contrôle de la diffusion** - distribution limitée?

Sensibilité?
Les renseignements peuvent-ils être exemptés en vertu des lois sur l'accès à l'information et protection des renseignements personnels (AIPRP) (c.-à-d. les renseignements sont-ils suffisamment *sensibles pour être protégés* ou classifiés)?

Non → Alors → Classification : **NON CLASSIFIÉ**

Oui

Préjudice?
Si les renseignements étaient compromis, quel préjudice ou dommage pourraient-ils entraîner?

Des questions d'intérêt non-national
(c.-à-d. une personne ou un organisme)

Des questions d'intérêt national
(c.-à-d. l'économie, la stabilité politique, les relations internationales, les forces militaires ou les capacités de collecte de renseignement du Canada)

Conséquences?
Quelles conséquences raisonnables pourraient en découler?

Préjudice
(p. ex., embarras, dérangement; également information reçue en confidence d'un gouvernement étranger)

Préjudice grave
(p. ex., atteinte à la vie privée, à la réputation et (ou) avantage concurrentiel; répercussions négatives sur la prise de décisions de la direction)

Préjudice extrêmement grave
(p. ex., pertes financières catastrophiques pour un organisme, préjudice sérieux envers une personne, décès)

Conséquences?
Quelles conséquences raisonnables pourraient en découler?

Préjudice
- aux relations diplomatiques du Canada
- à l'efficacité opérationnelle des Forces canadiennes
- aux intérêts économiques à court terme
- à l'efficacité des opérations de renseignement

Préjudice grave
- aux relations internationales ou fédérales-provinciales
- à l'efficacité opérationnelle des Forces canadiennes
- aux opérations importantes de renseignement
- à l'infrastructure essentielle nationale
- à l'ordre civil

Préjudice extrêmement grave
- à l'efficacité ou à la sécurité des Forces canadiennes et des forces alliées
- aux relations avec les gouvernements amis
- à l'efficacité des opérations extrêmement importantes de renseignement
- à l'économie canadienne
- à la stabilité du Canada ou à celle des pays amis
- au décès

Classification : **PROTÉGÉ A** | Classification : **PROTÉGÉ B** | Classification : **PROTÉGÉ C**

Classification : **CONFIDENTIEL** | Classification : **SECRET** | Classification : **TRÈS SECRET**

Systèmes de contrôle?
Est-ce que les renseignements doivent être manipulés au moyen de systèmes de contrôle spéciaux (c.-à-d., COMINT, TK, documents du Cabinet)?

Non →

Oui → Ajoutez les mentions nécessaires relatives aux systèmes de contrôle (Consultez le document OPS-5-14)

Diffusion?
Devrait-on limiter la diffusion du document?
(c.-à-d. mises en garde)
(p. ex., À des fins officielles du CSTC, Réservé aux cadres supérieurs; Réservé aux Canadiens)

Alors → Ajoutez les mentions nécessaires relatives aux systèmes de contrôle (Consultez le document OPS-5-14)

Oui → Ajoutez les mentions nécessaires de contrôle relatives à la diffusion (Consultez le document SEC-103 ou OPS-5-14)

Avez-vous besoin d'aide?
Consultez des documents semblables, demandez des conseils à des collègues plus expérimentés ou allez voir votre gestionnaire.

Vous avez toujours des questions?
Communiquez avec la **Sécurité interne** au moyen du système ARS concernant le document SEC-103, ou avec [redacted] concernant le document OPS-5-14.

ORIG VERSION.

s.15(1)

SIGINT Case Summary

Put your thinking caps on Lateral Thinking!!!!

MAN
BOARD

MAN OVERBOARD

Put your thinking caps on Lateral Thinking!!!!

STAND
I

I UNDERSTAND

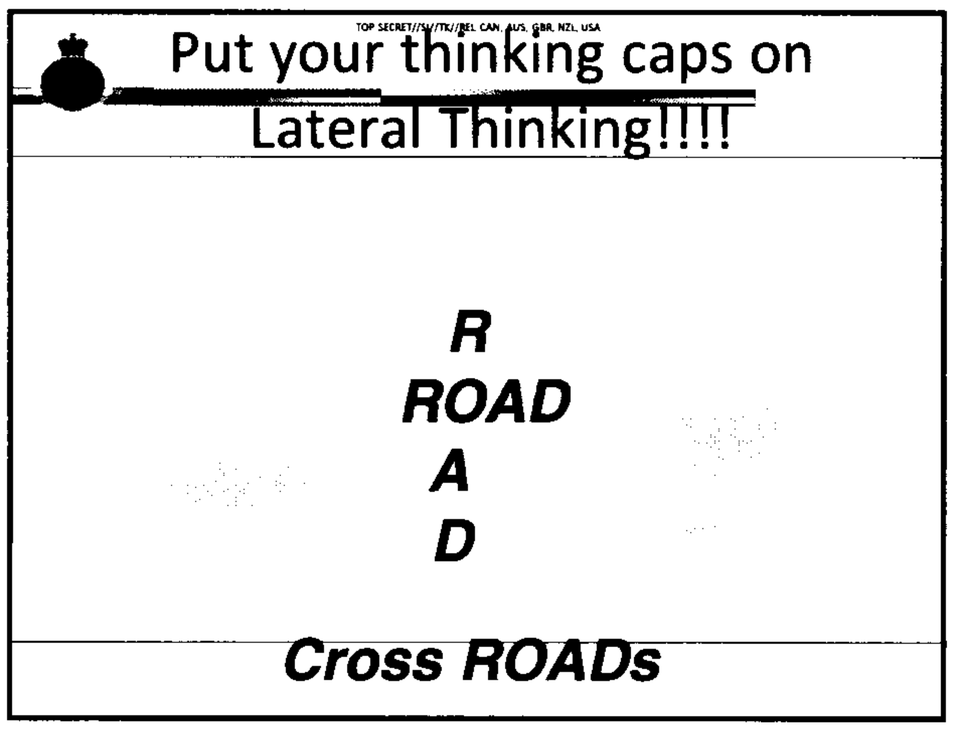
Put your thinking caps on Lateral Thinking!!!!

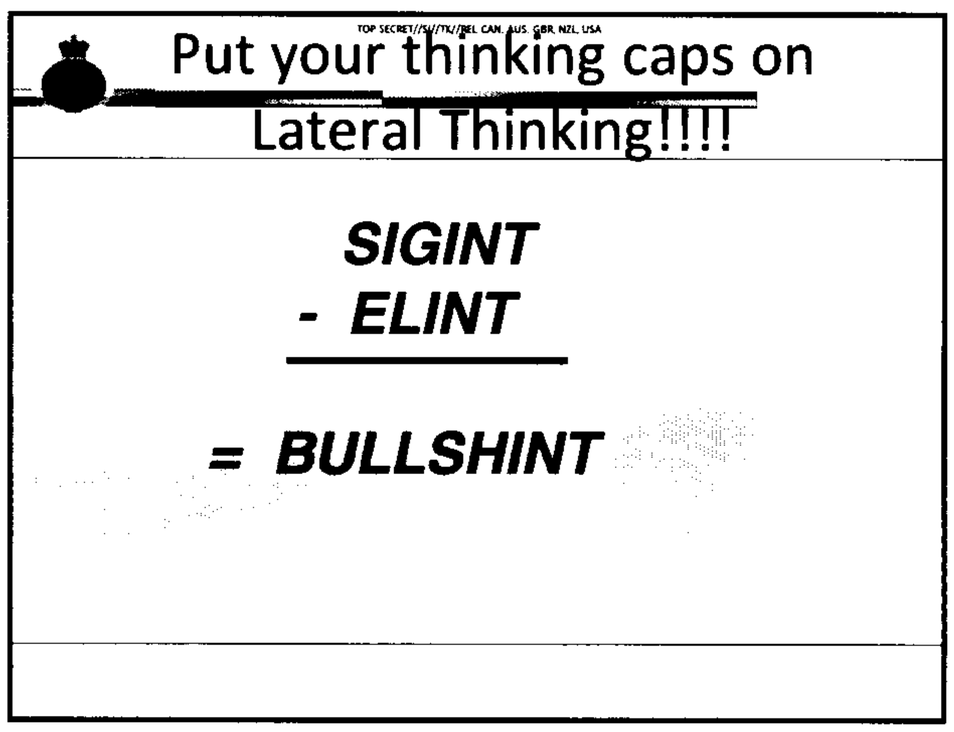
r/e/a/d/i/n/g

Reading between the lines

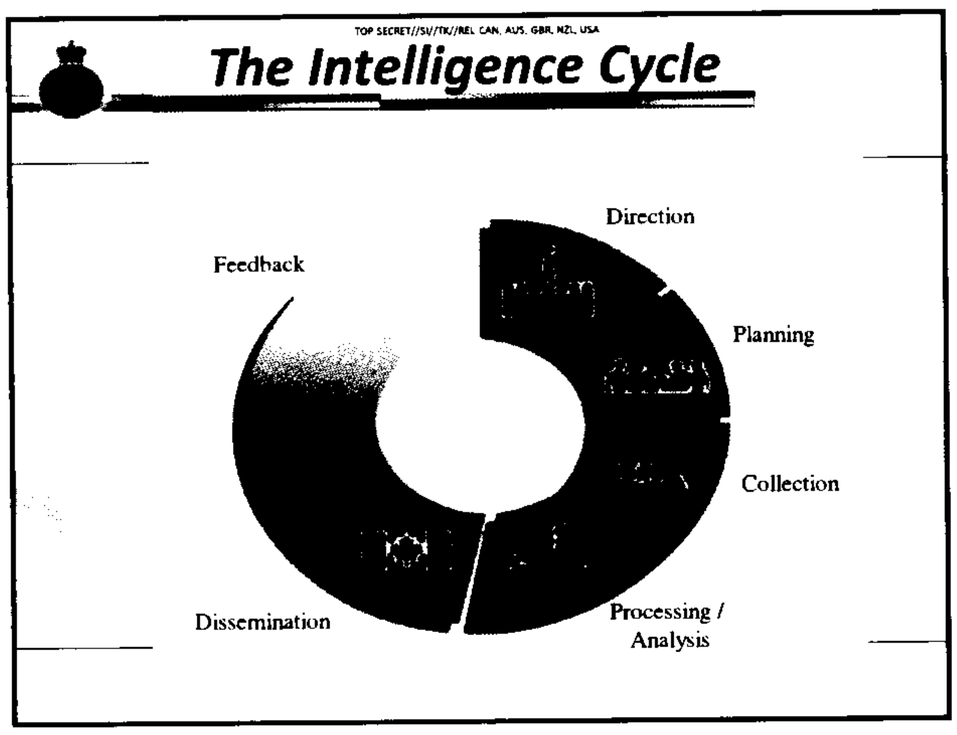
s.15(1)

TOP SECRET//SI//REL CAN, AUS, GBR, NZL, USA



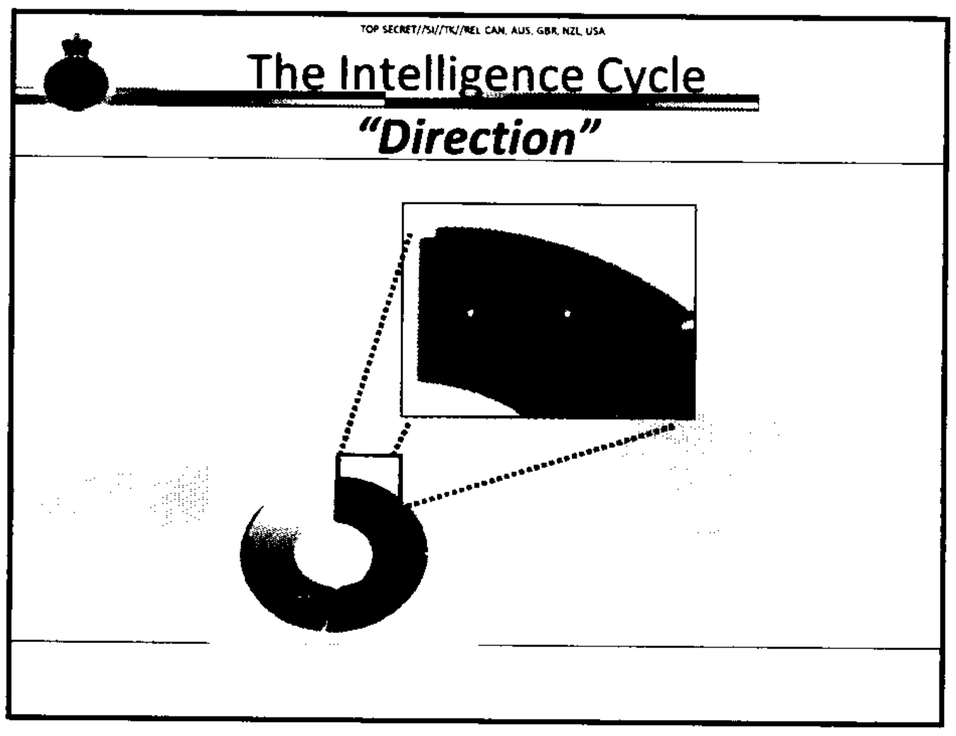


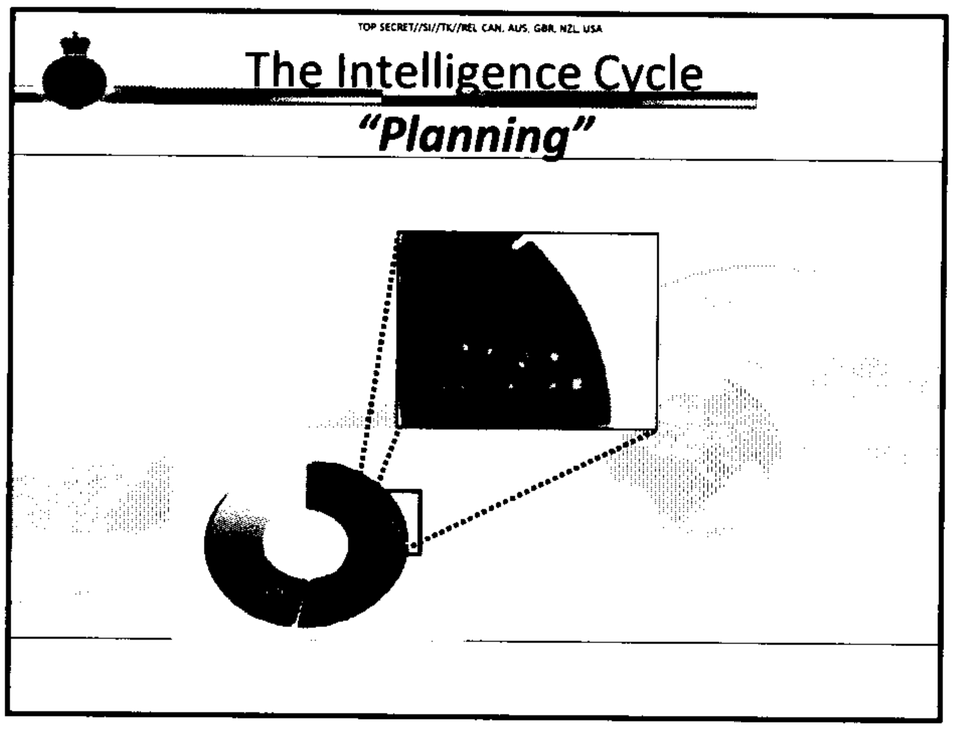
s.15(1)

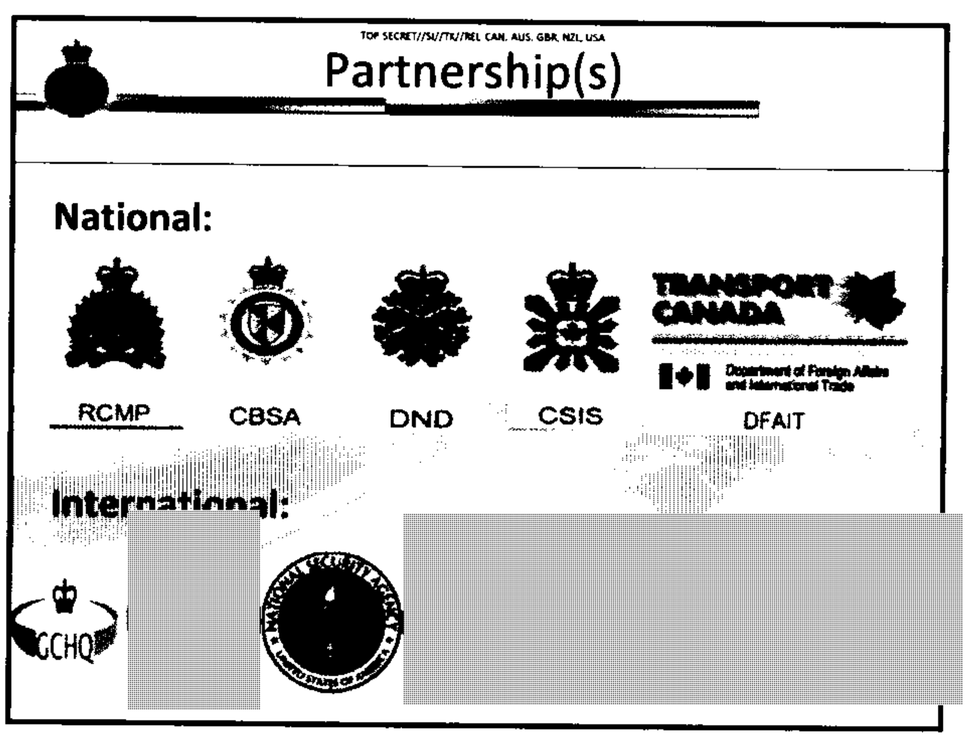


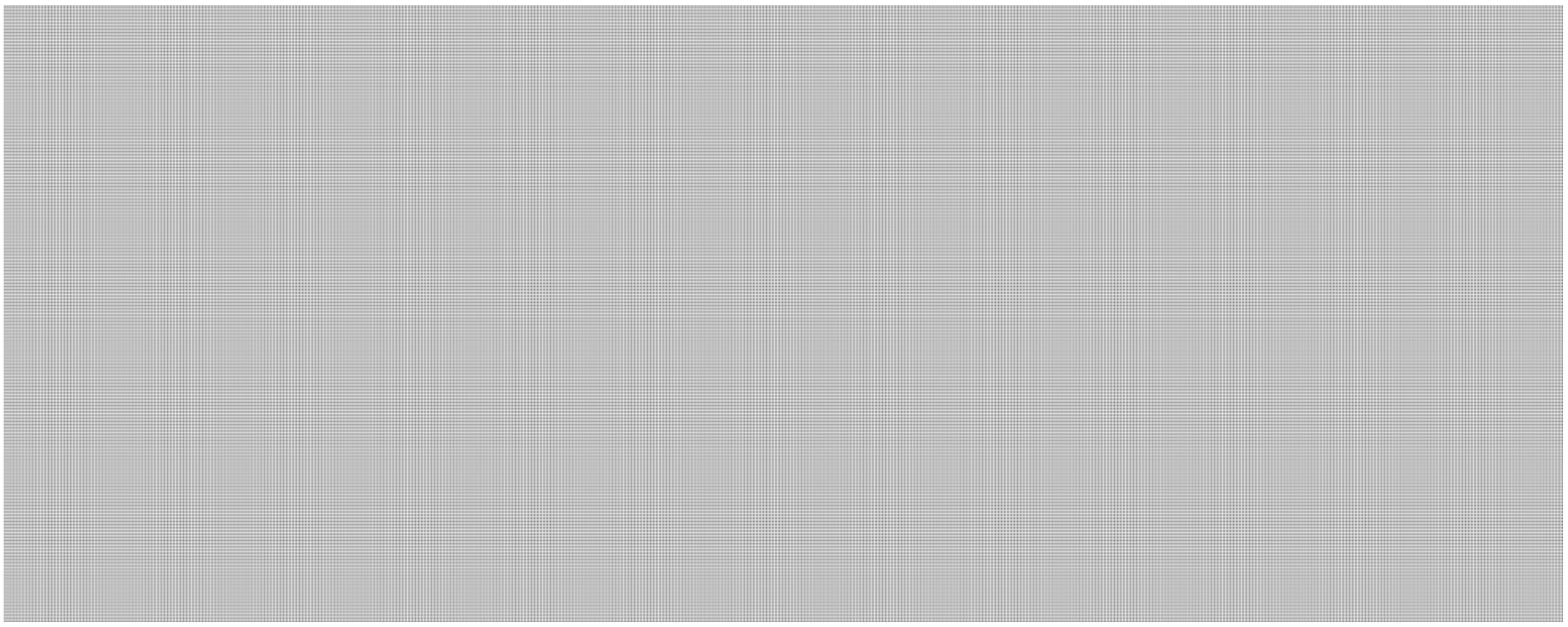
s.15(1)

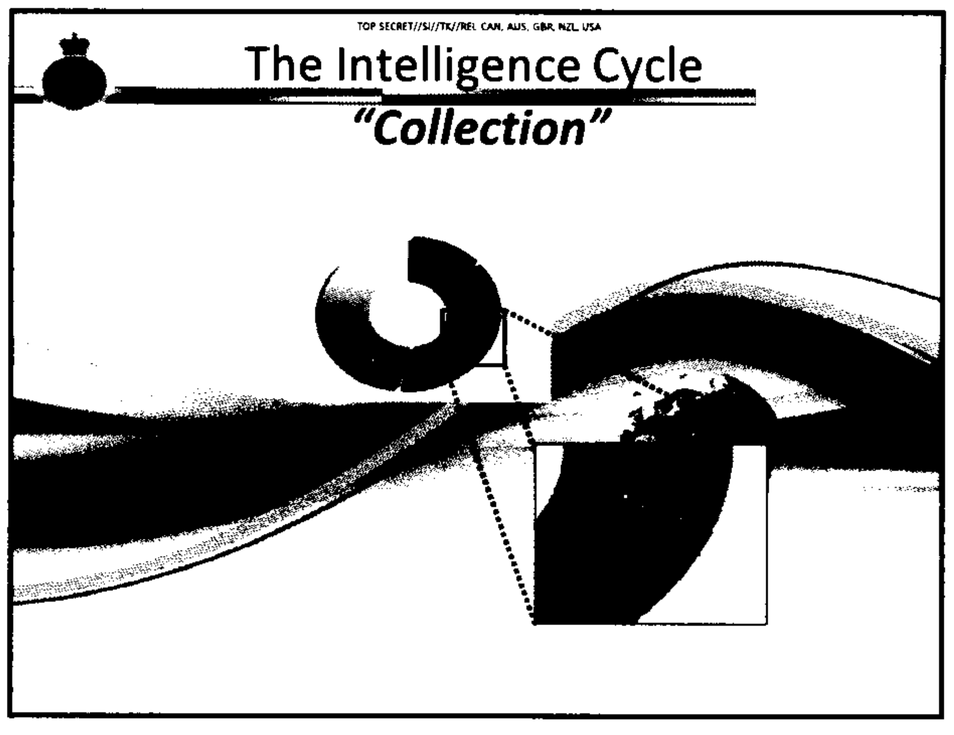
[redacted]

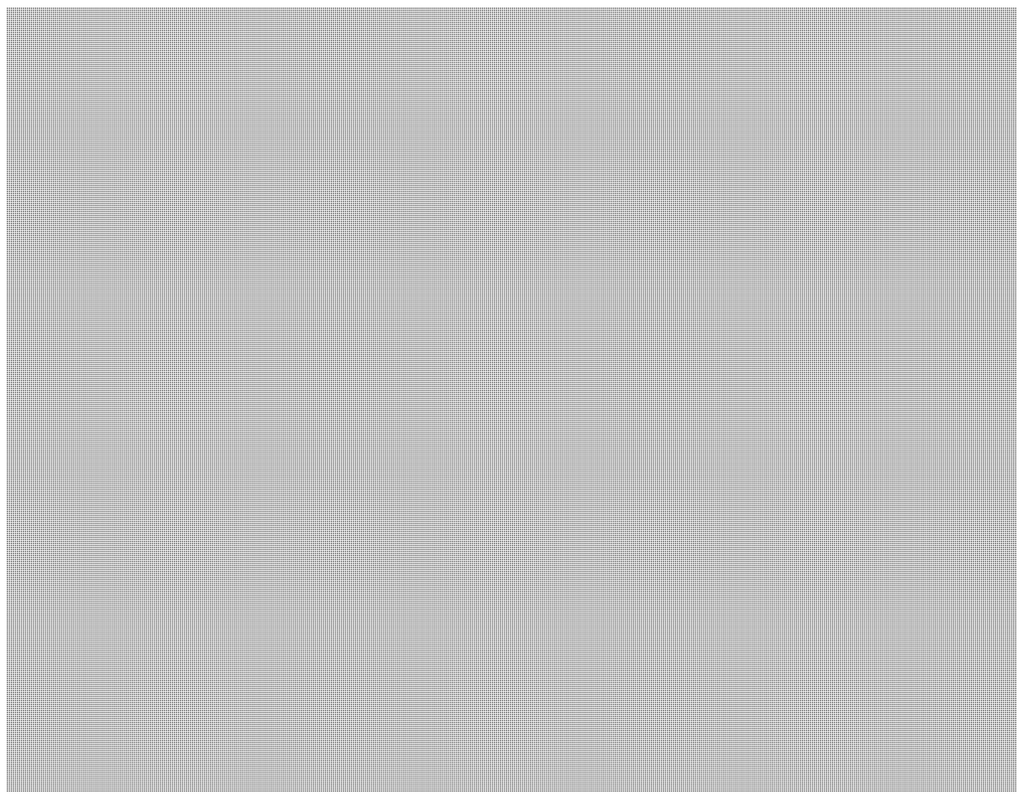


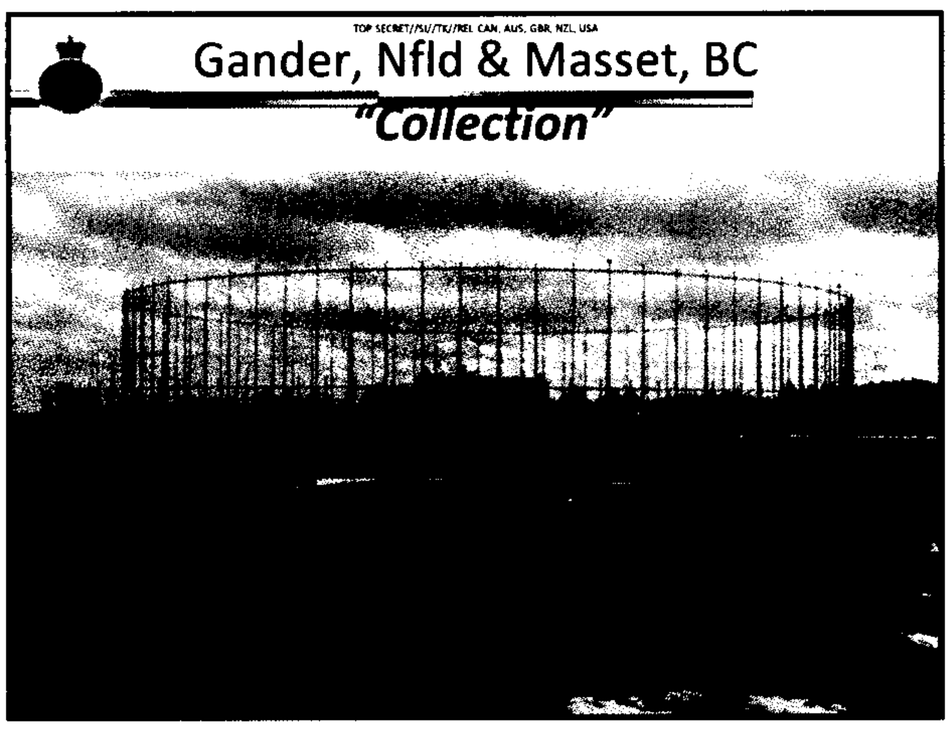


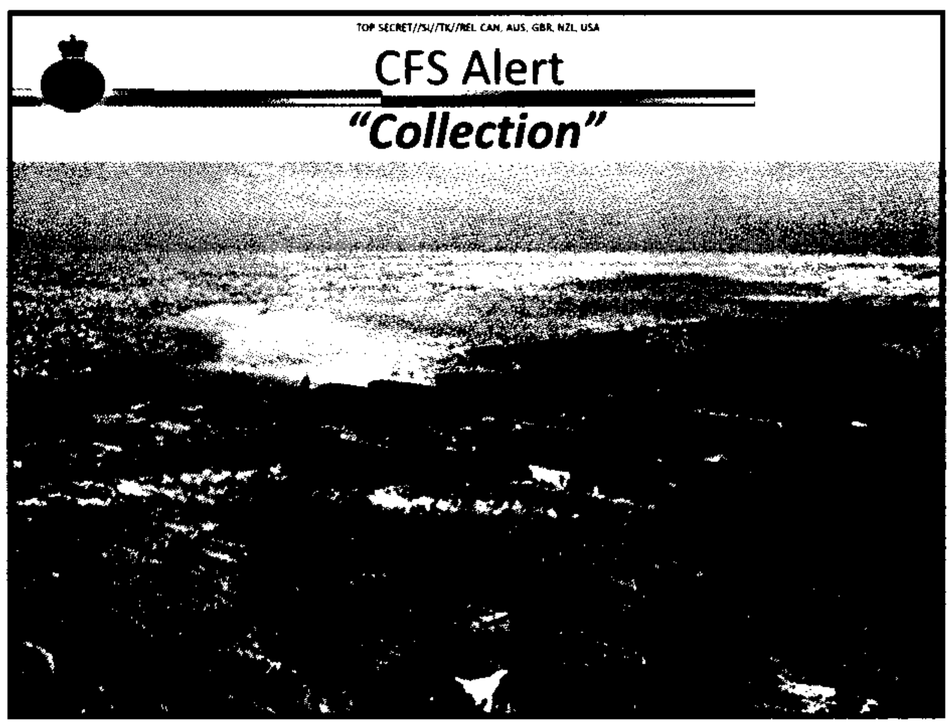




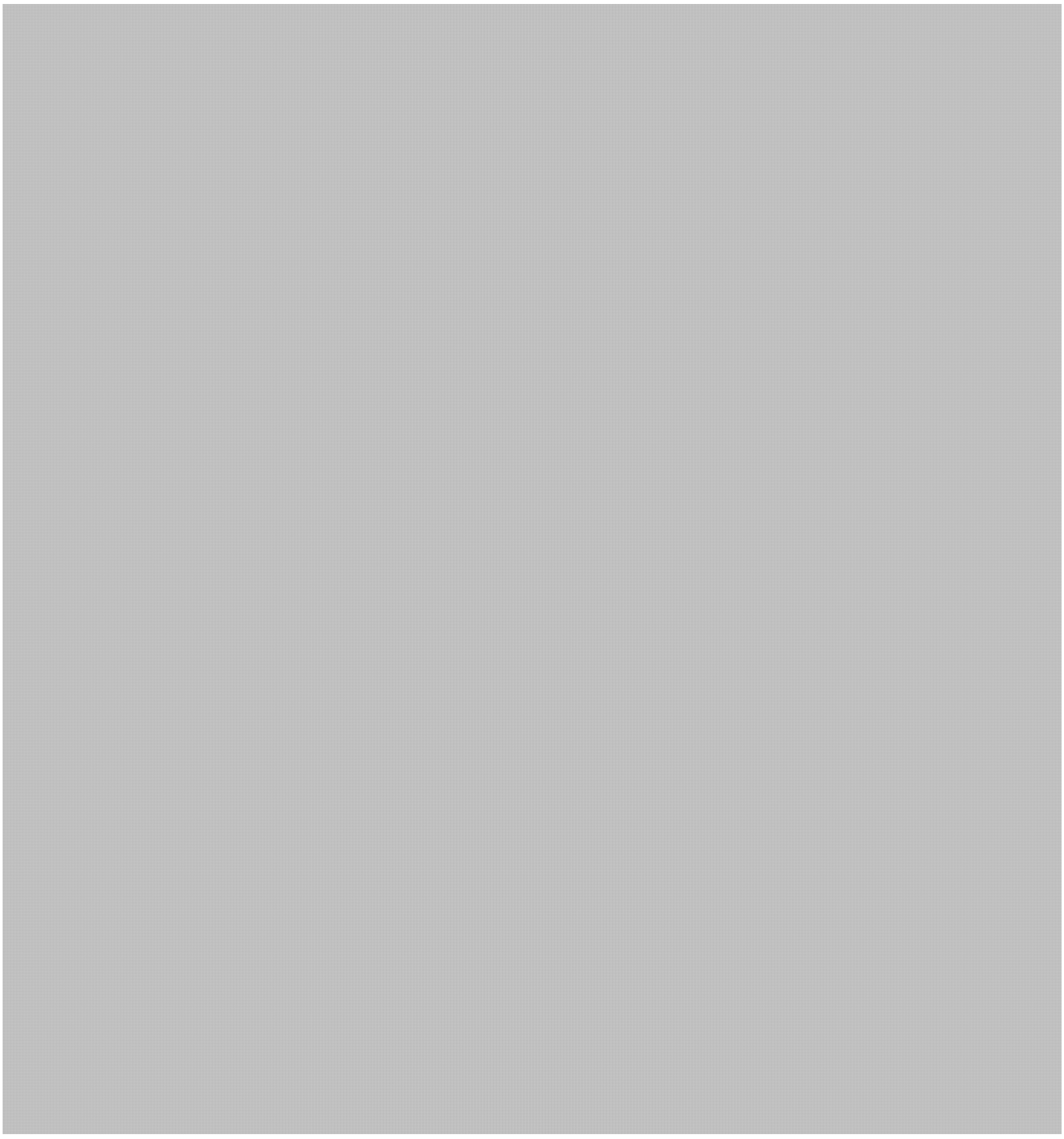






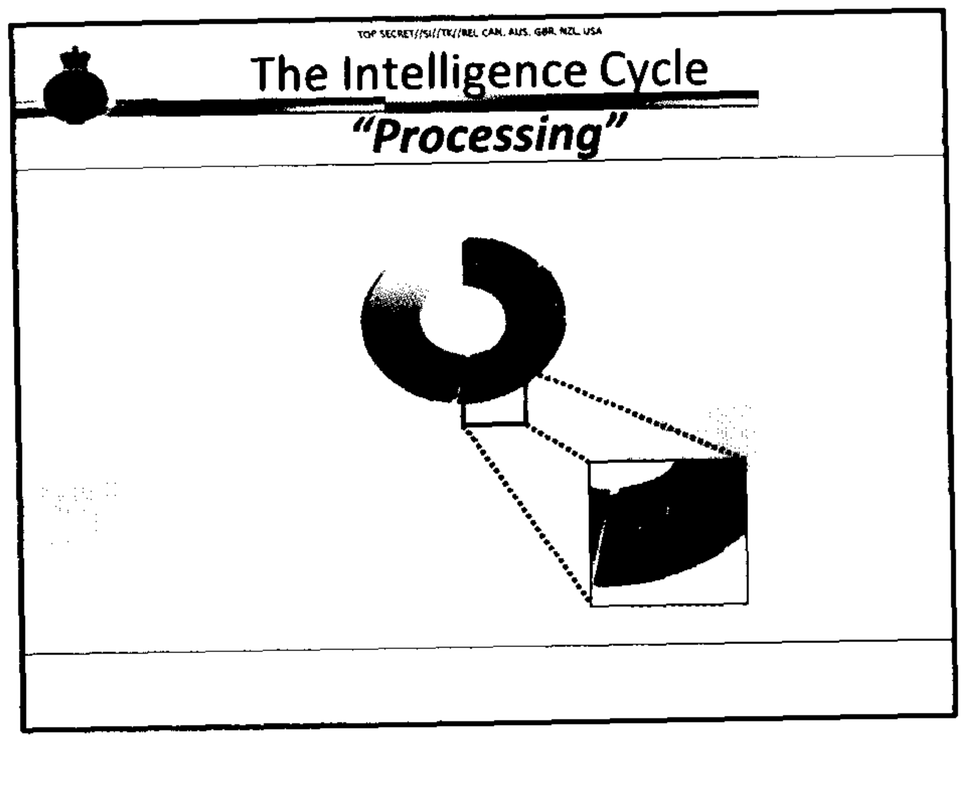


s.15(1)

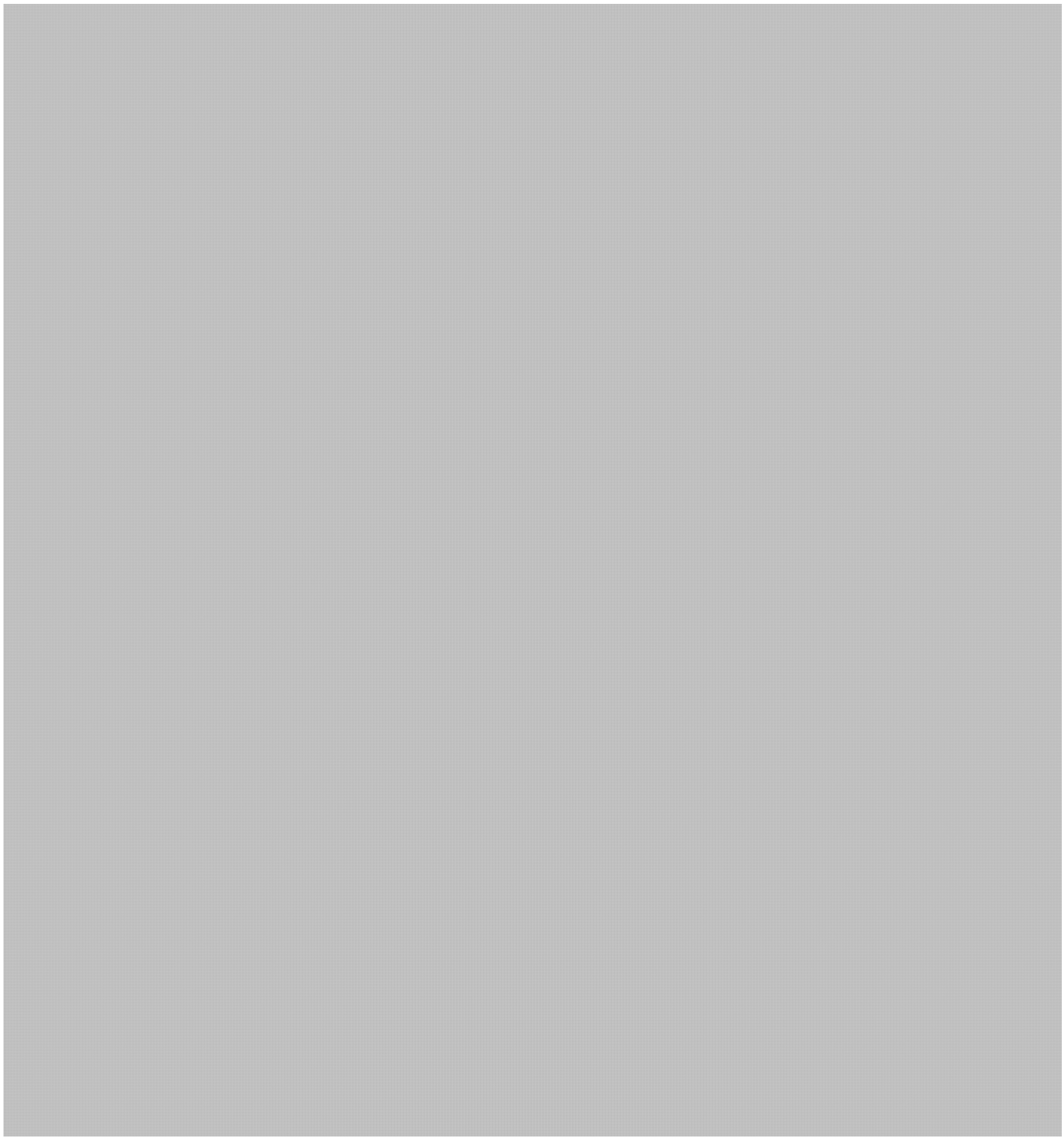


s.15(1)

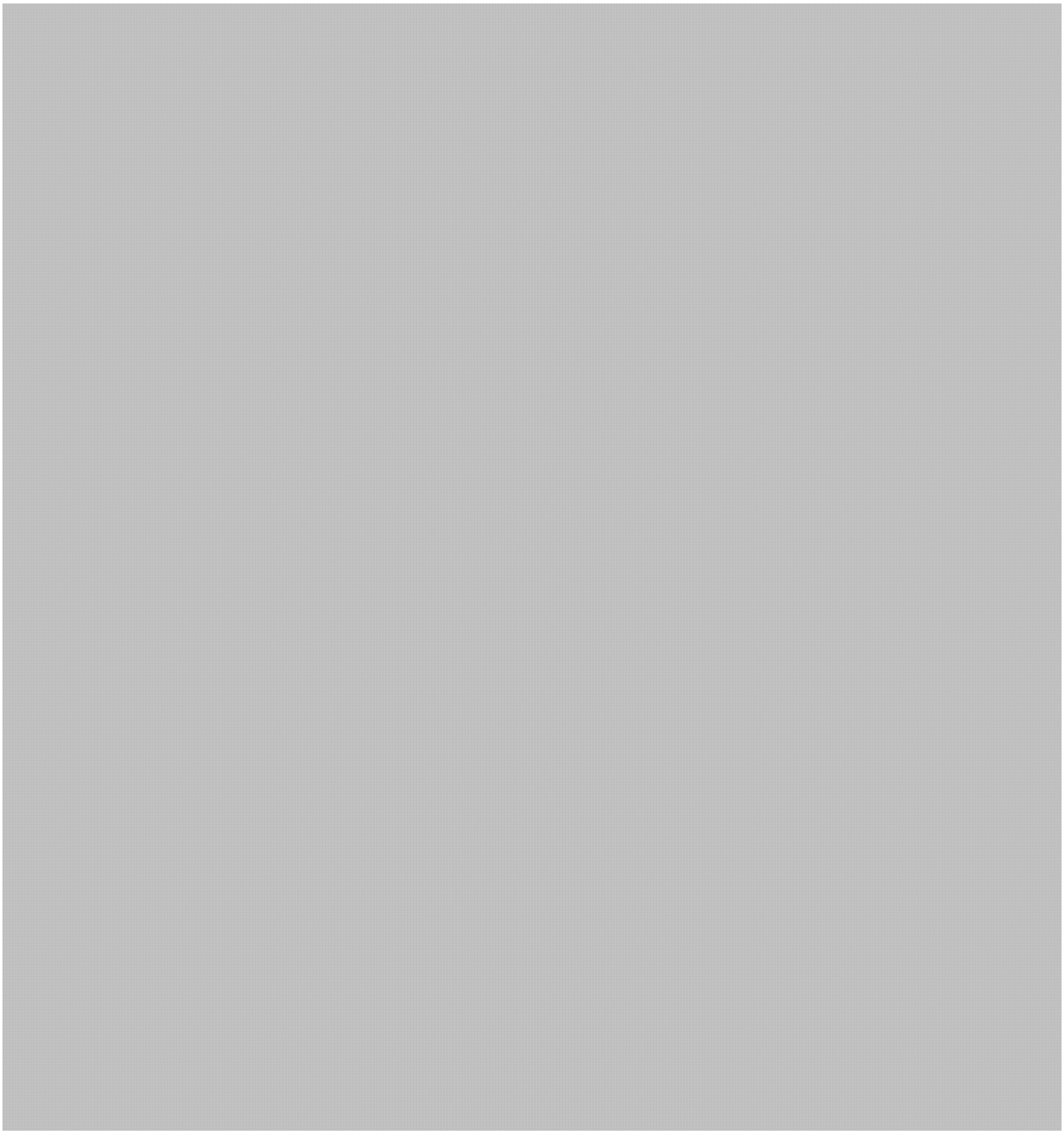
[redacted]



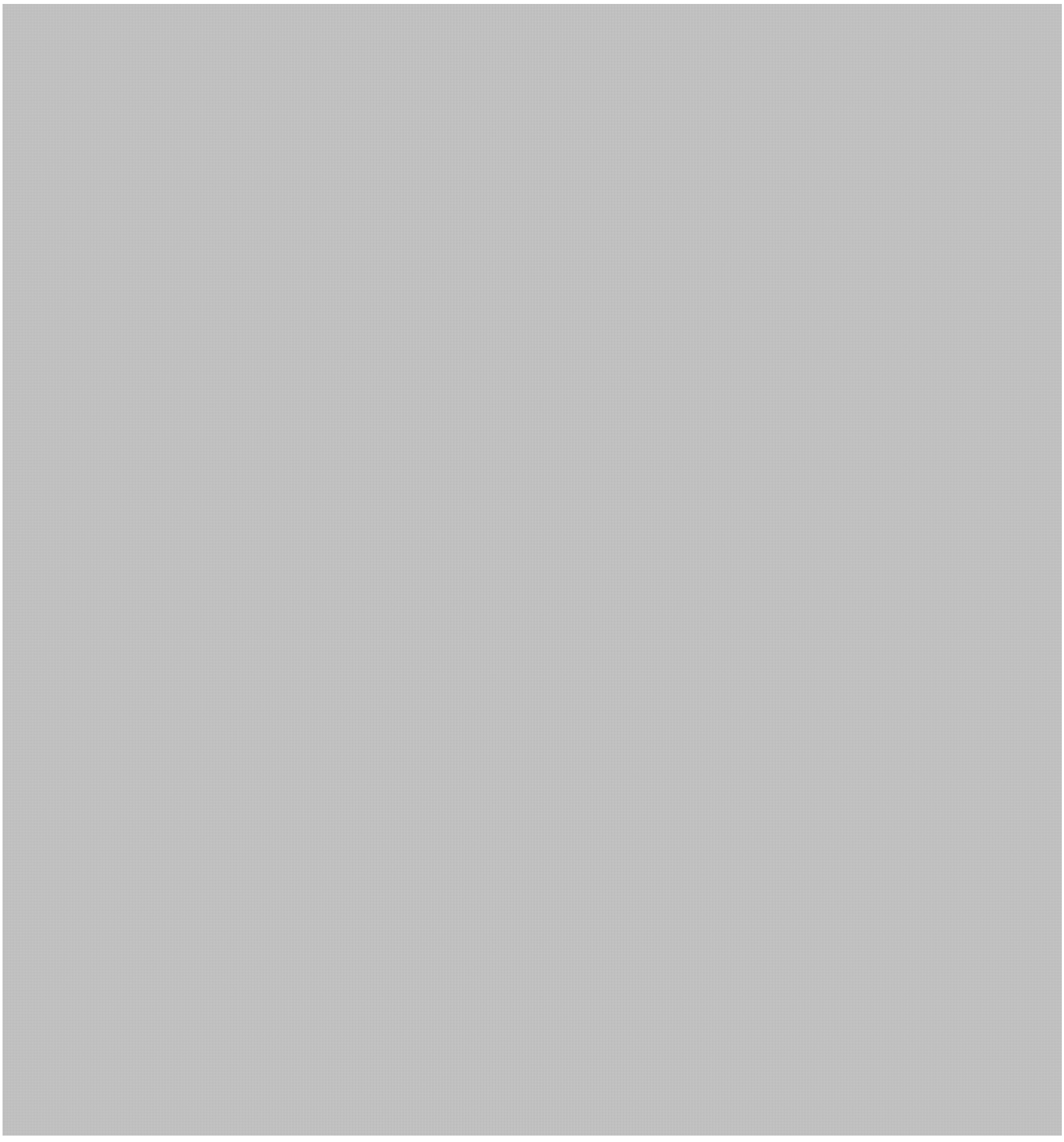
[redacted]



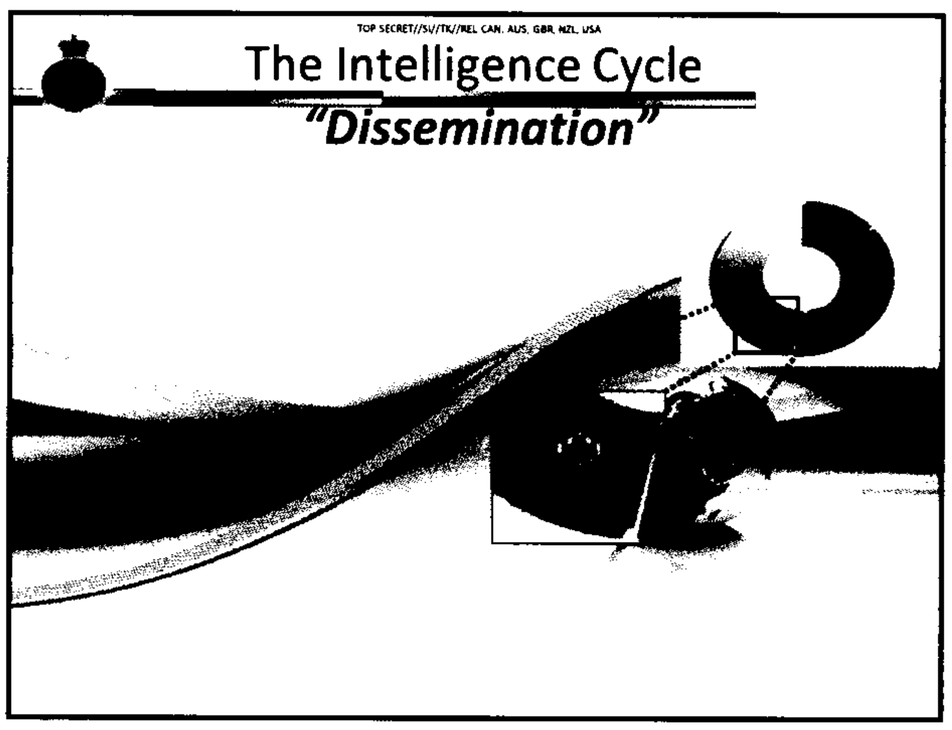
TOP SECRET//SI//REL CAN, AUS, GBR, NZL, USA



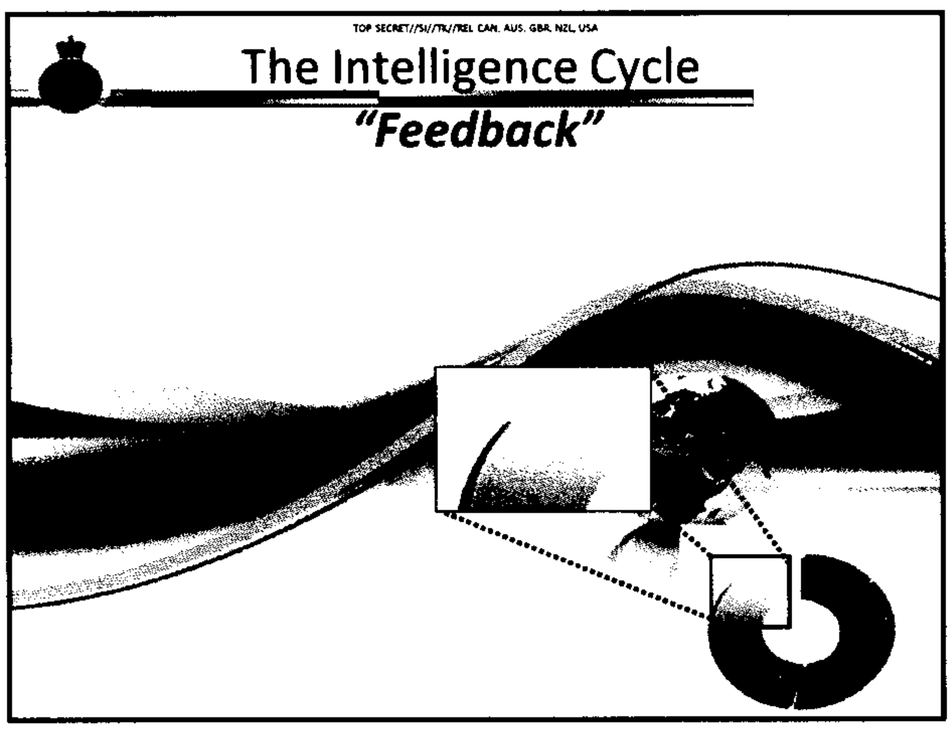
s.15(1)



s.15(1)



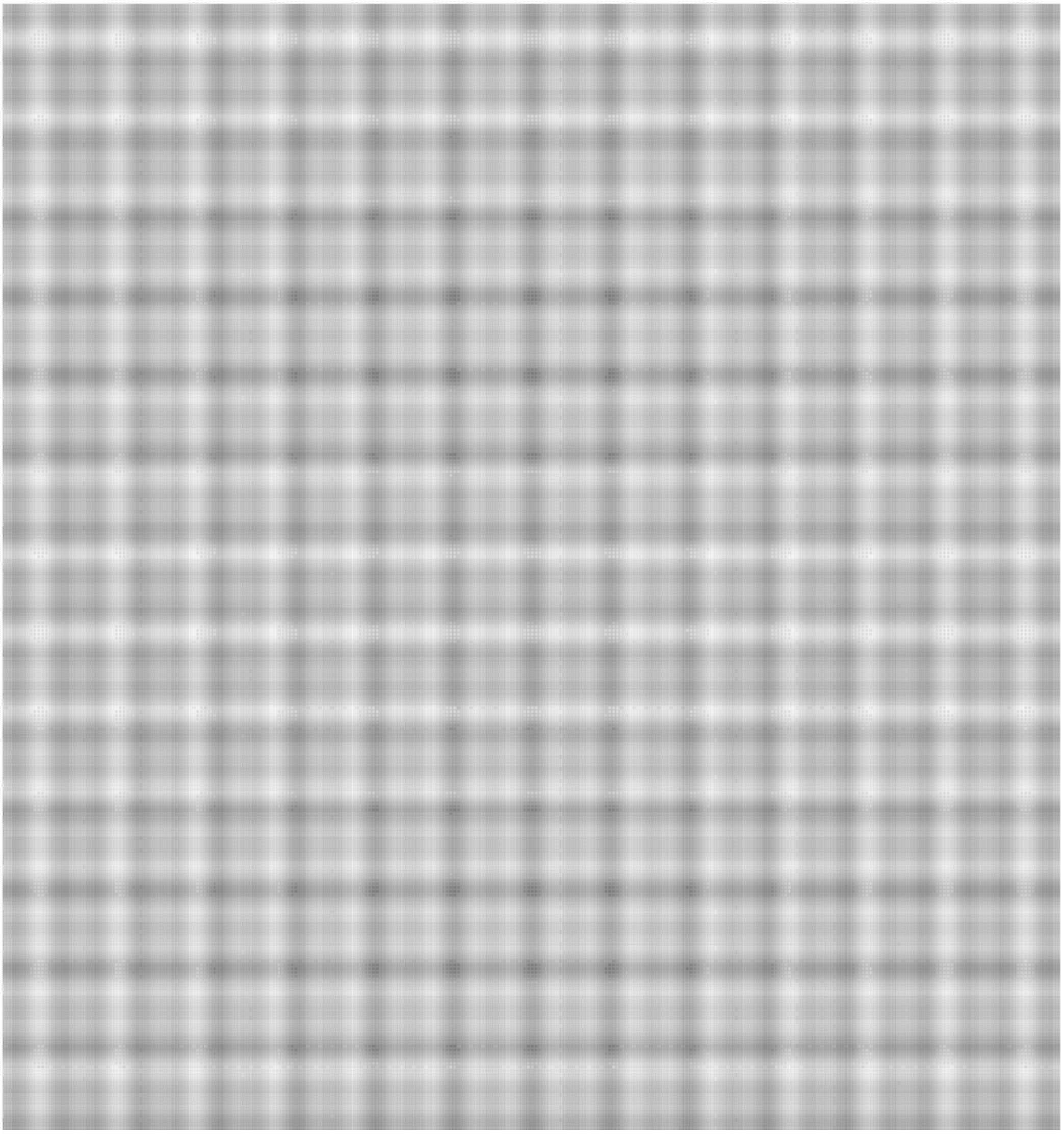
TOP SECRET//SI//REL CAN, AUS, GBR, NZL, USA



[redacted]

[redacted]

s.15(1)



s.15(1)

[redacted]

TOP SECRET//SI//TK//REL CAN, AUS, GBR, NZL, USA

This entire Briefing is classified:
TOP SECRET // COMINT //
[redacted]
//
Rel AUS / CAN / NZL / UK / USA

Wireless Security Demonstration

[redacted]
ATA-[redacted]
Head, COTS Tailored Evaluations

Canada

ATA-[redacted] COTS Tailored Evaluations

- Evaluation of commercial IT security products
  - Cryptographic products (e.g., VPNs)
  - Authentication products (e.g., smart cards)
  - Mobility products (e.g., BlackBerry and Apple)
- Development of advice and guidance to GC departments and agencies
- Vulnerability assessment of crypto products
- Security education and awareness for GC clients, including the Wireless Security course for the ITS Learning Centre

Canada

Evaluation of COTS Products

- Evaluation of cryptographic and other security aspects of commercial IT security products
- Vulnerability discovery of software and hardware implementations
- Recommendations on the use of IT security technologies and product

Canada

Wireless Security

- Evaluation of secure wireless technologies
  - RIM BlackBerry, iPhone, iPad and other PDAs
  - Bluetooth
  - Cellular and cordless telephones
  - Wireless LANs
- Research of RF and wireless technologies
  - Fully equipped RF lab, shielded chamber facility
- Training and guidance to GC clients

Canada

Research

- Wireless technologies
  - e.g., WiFi, Bluetooth, CDMA, GSM, UMTS, LTE, etc.
- RFID and Near Field Communications
- Smart cards
- Power and timing analysis
- Random Number Generation and Entropy
- Disk and USB encryption

Canada

Demo Disclaimer

- Interception of private information may violate Canadian Laws. Before you attempt any wireless testing in your organization you should consult your legal services.
- The use of various tools, products and references should not be interpreted as approval or endorsement from CSEC.

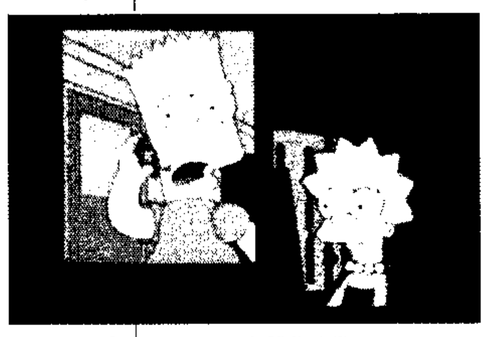
Canada

Bluetooth™ Audio Capture Demonstration

Bluetooth

Canada

Bluetooth Vulnerabilities in Popular Culture



The Simpsons™ "24 Minutes" Copyright 2007 FOX and affiliates

Bart: Lisa, are you on a secure line?

Lisa: I am, but you're using a *Bluetooth cell phone, the most vulnerable communications device known to man*!

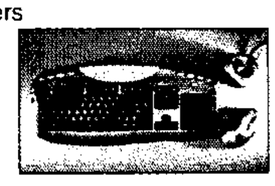
Bart: But it looks so cool!

2012V2 8

Canada

Bluetooth Applications

- Bluetooth technology developed for rapid set-up of short range communications (wire replacement)
  - Computer mice, keyboards and printers
  - Wireless speakers
  - Serial port connections
  - Hands-free headsets
  - Digital cameras
  - Games such as Nintendo Wii



- Remote control for audio and video systems
- File sharing and synchronization between laptops, mobile phones and PDAs

2012V2 9

Canada

Bluetooth Vulnerabilities

- Bluetooth has been developed for rapid set-up of short range communications-devices often designed for ease of use and convenience vs. security.
- Example: Bluetooth hands-free headsets- widespread use, designed for easy setup: use short, hard-coded PINs that are well known (e.g. '0000' or '1234'), some devices even use fixed unit keys for "instant connections".

2012V2 10

Canada

Bluetooth Audio Interception

- "Ease of use" features make Bluetooth headsets extremely vulnerable to attack:
  - No need to "crack" the PIN as it is well known (lists of model/PIN available on the Internet)
  - Interception and playback of audio from a Bluetooth headset is possible if pairing sequence is overheard.
- Note that audio interception capability is ***not*** the result of "breaking" the security protocol (although this is also possible)! The vulnerability exists due to the use of ***well-known, unchangeable*** PIN codes!

2012V2 11

Canada

Other Security Issues

- Passive eavesdropping at range
- Proximity tracking by BD_ADDR
- Non-standard implementations that bypass security
- "De-authentication" attack
- Human nature: conditioned response to malfunction- re-try, re-boot, re-***pair!!***

BlueSniper Rifle

***Blue*Bag**

Most discovered devices are Mobile (Smart) Phones

2012V2 12

Canada

Demonstration

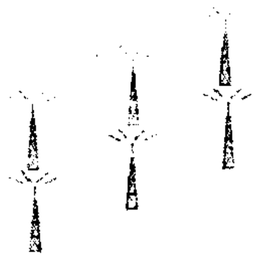
- Demo: audio intercept of Bluetooth headset paired to a cell-phone and also to a Bluetooth desktop phone adapter.
  1. Attacker synchronizes to target piconet by sending *inquiry message to headset device.*
  2. Attacker waits for user to pair to a telephone device to headset and uses the known PIN code to decode the communications
  3. Attacker is able to record and play back both sides of audio conversation.

Demonstration

- Demo 2: audio intercept of standalone Bluetooth headset from a remote PC.
  1. Attacker sends inquiry to target headset device. Due to implementation flaw or deliberate design (ease of use), the target device will go into pairing mode without user intervention.
  2. Attacker sends the known PIN code to establish communications with the headset
  3. Attacker is able to activate headset remotely and record and play back audio conversation from the vicinity of the headset.

Cellular Telephone Capture

Cellular Voice Service



- Evolution of mobile dispatch radio service (MTS- Mobile Telephone Service)
  - Conceived by AT&T in 1947, trialed in 1978, first commercial service in 1984.
  - Cellular concept is based on using large number of low power transceivers to *cover a large subscriber area.*
  - Allows more efficient use of frequency spectrum.
- All modern carrier voice services use the cellular model, but vary in frequency band use, reuse strategies, and transmission/encoding schemes.

Wireless Voice Threats and Vulnerabilities

- GSM has complex modulation/coding and provision for confidentiality and integrity (encryption).
  - Encryption is only over wireless link, decrypted at base station
  - Algorithms not GC approved, have been broken
  - SIM cards can be cloned over-the-air
  - Still vulnerable to denial of service attacks via jamming
- CDMA is more complex than GSM, but still vulnerable to intercept and spoofing. CDMA is more resistant to jamming of the actual transmission; however, the GPS signal used for network timing is vulnerable.
- Common to all technologies: the fact that safeguards are all **optional**- service providers may elect to turn them off to make network debugging easier or to save costs.

GSM

- Many other commercial and "hacker" products available for GSM intercept

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

Demonstration

- CDMA cellular phone interception:
  - Commercial receiver, passively monitors both base station and handset transmissions
  - Targeted capture and real-time playback of voice calls and SMS

2012V2 19

Canada

Communications Security Establishment | Centre de la sécurité des télécommunications

Cordless Telephone

Canada

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

Cordless Phones

- 46/49 MHz analogue, 900 MHz analogue and digital, 2.4 GHz digital, 5.8 GHz digital
  - Analogue phones are not secure
  - Digital security codes – base to handset
  - Digital Spread Spectrum (DSS)
  - Digital better but not entirely secure
- DECT 6.0 phones
  - "Digital European Cordless Telecommunications"
  - TDMA digital encryption (proprietary, often disabled by default to extend range and battery life)
  - Base station is implicitly trusted (no mutual authentication- can be spoofed)
  - Not GC approved for designated or classified use

2012V2 21

Canada

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

Demonstration

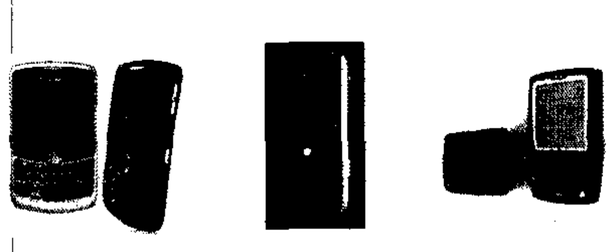
- DECT 6.0 Cordless phone interception:
  - Commercial PC Card DECT controller (original price $25, after hack discovered $250)
  - Linux driver and simple VoIP vocoder software
  - Targeted capture and playback of DECT voice calls and DTMF information

2012V2 22

Canada

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

BlackBerry™ Security



2012V2 23

Canada

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

BlackBerry Background

- The RIM BlackBerry™ is ubiquitous among business users and particularly at senior management levels in the GC.
- CSEC has identified and mitigated many BlackBerry vulnerabilities over the years.
- BlackBerry and mobile device-related CSEC publications:
  - ITSA-18 *General Guidelines for the Use of Wireless Devices in the Federal Government*
  - ITSA-32 *Intelligence Threats to Cellular Telephones*
  - ITSB-06 *CSEC Approves Secure BlackBerry*
  - ITSB-19 *Security Measures - Wireless Electronic Devices*
  - ITSB-57 *Security of BlackBerry PIN-to-PIN Messaging*
  - ITSG-06 *Clearing and Declassifying Electronic Data Storage Devices*
  - ITSG-23 *BlackBerry® Enterprise Server Isolation in a Microsoft Exchange Environment*
  - ITSPSR-16 *Personal Communications Services (PCS) and Cellular System Vulnerability Assessment*
  - ITSPSR-18 *Personal Digital Assistant Vulnerability Assessment*

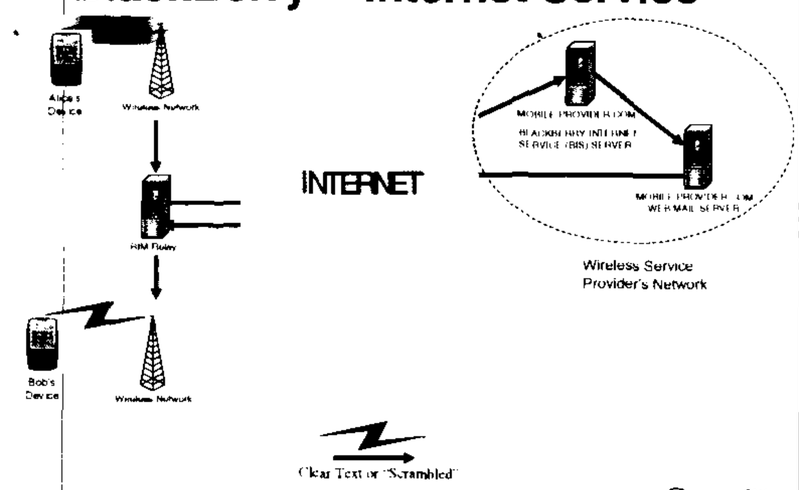
2012V2 24

Canada

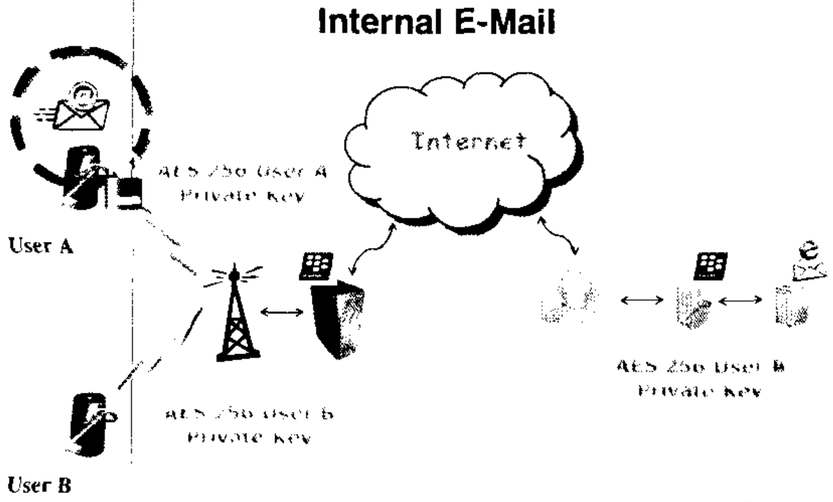
Blackberry Editions

- BlackBerry Internet Service
  - Commercially available BlackBerry available to all consumers
  - Uses BlackBerry Internet Service (BIS) of wireless service provider
  - In latest BIS, ***global*** encryption key (**common to all devices**) and 3DES/AES algorithms protecting BIS e-mail, BB PIN-based traffic (Messenger, Groups) only.
- Enterprise Edition
  - Corporate/Government customers
  - Uses BlackBerry Enterprise Server (BES) in corporate computer centre- manages ***individual*** private keys for each *Enterprise BlackBerry*
  - FIPS 140 validated cryptographic module – enabled via IT policy, CSEC-approved algorithm *protects e-mail and browsing* traffic
  - Central Administration via IT Policy (password lengths, remote *wipe, message archiving, etc)*
  - Content Protection encrypts device contents

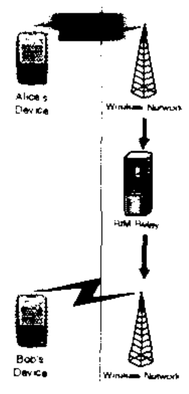
BlackBerry™ Internet Service



BlackBerry Enterprise E-mail Internal E-Mail

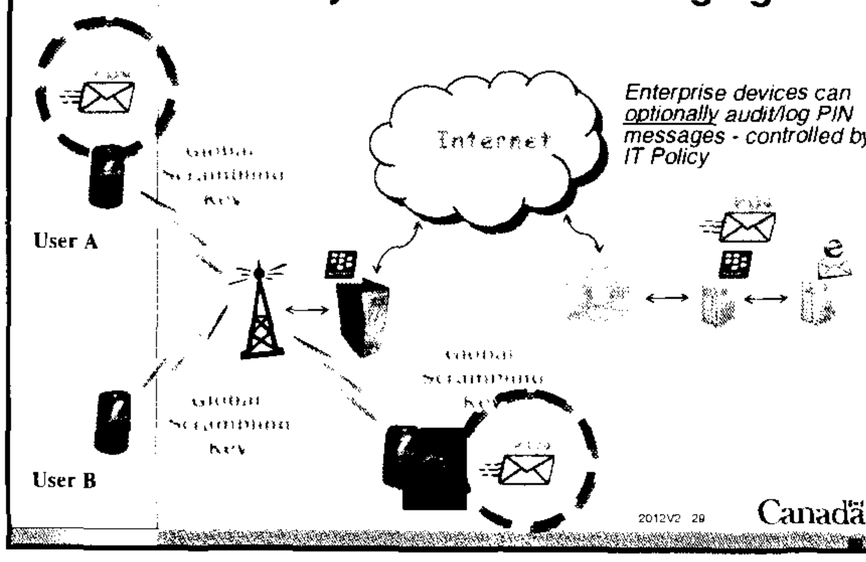


BlackBerry PIN-to-PIN Messaging



- Quick messaging facility directly between BlackBerry devices, *does not rely on corporate e-mail infrastructure*
- Messages protected using global encryption key: RIM advises customers to consider messages only as "scrambled" and not encrypted.
- PIN-to-PIN is underlying mechanism for BlackBerry Messenger/Groups and subject to same vulnerability

BlackBerry PIN-to-PIN Messaging



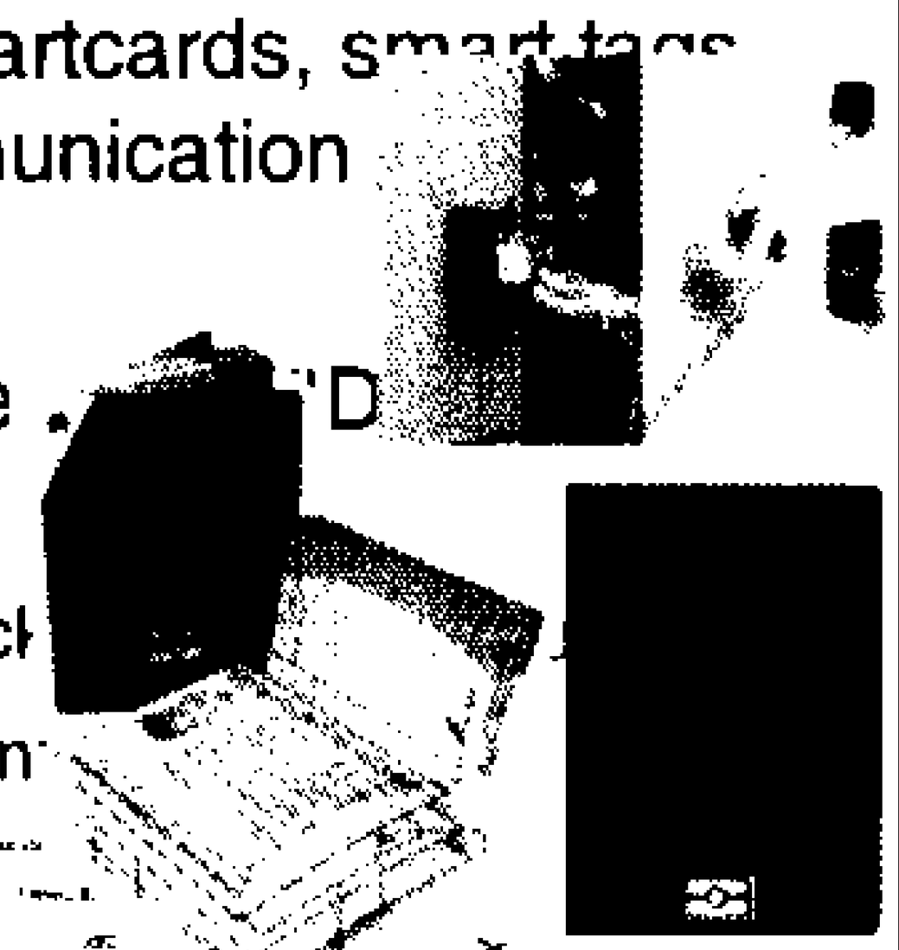
Enterprise devices can optionally audit/log PIN messages - controlled by IT Policy

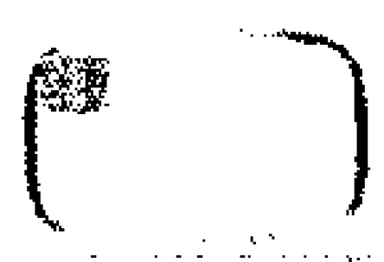
Questions ?

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

(RFID) Radio Frequency IDentification

- Technology using radio waves to automatically identify objects or people
- Also described as contactless smartcards, smart tags, proximity cards, Near Field Communication, wireless payment
- Many ISO standards used for diffe... RFID applications
  - Product inventory, toll collection, e-tick...
  - ...ca... sports, paymen...
  - O/... and B...
  - gh... MHz
  - 10-15 cm wireless range



2012V2 31 Canada

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

Marketing RFID as "Security"

Securing Travel Documents With RFID
PREMIUM CONTENT
The Western Hemisphere Travel Initiative (WHTI) is a joint U.S. Department of State and U.S. Department of Homeland Security (DHS) plan to implement...

Reducing the Risk of Terrorism With RFID
PREMIUM CONTENT
Alex Water Service, a utility based in ... has itself, has implemented an RFID based system for both security and asset-management applications. The...

Report from Data Center World: RFID increases IT asset security

RFID credit cards are more secure than magnetic stripe cards...

RFID Brings Safety to ...

Using RFID to Enhance Mobile Banking Security

RFID speeds checkout and increases security at library

Comparison of Near Field Communications (NFC) and Bluetooth 4.0 Characteristics in Vehicles

	NFC	BT 4.0	Note
Security	High*	Good	* NFC higher security due to low distance for interception/interference and Point-to-Point, together with cryptography

2012V2 32 Canada

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

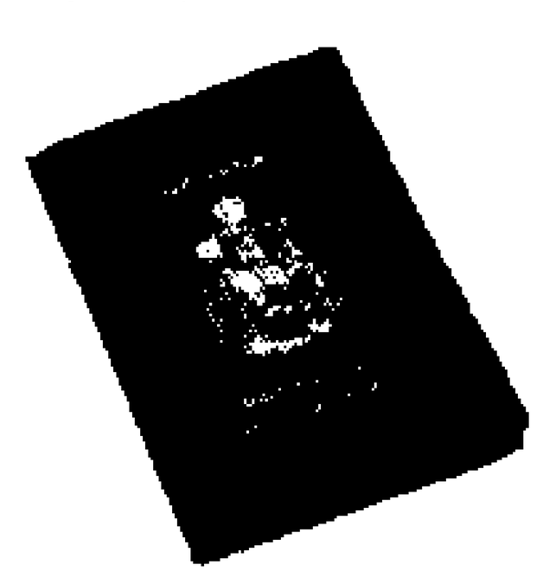
When RFID ePassports Fail Security

Elvis ... cloned in minutes

...ts Have Hacked It

...d – US next?

IT Expert in Britain Warns that Canadian RFID E-passports not Secure Enough



A current Canadian Passport

(RFIDWorld.ca) A British IT expert warns that Canada's new RFID-tagged E-passports can easily be hacked into and are not secure enough.

Adam Laurie, Director of Aperture Labs Limited pointed out that using a biometric chip does not make the passport secure enough because any other interdum can buy the equipment needed—just for $100—which can be used to clone the information on the passport. In addition to that, he added that there is even a free version of software that can do the same cloning job for anyone.

To show how easy it was to hack into and obtain someone's passport information, Laurie and his team made a fake passport for the dead singer Elvis Presley in 2008 and used it in an automated passport scanner. After being scanned, the machine was not able to read that it was a forged passport. The passport went through as completely valid when scanned at the Amsterdam Airport

[redacted]

2012V2 33 Canada

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

When RFID Access/Transit Cards Fail Security

RFID-Hack Hits 1 Billion Digital Access Cards Worldwide

The Dutch government has ... widely used Mifare Classic ...

NXP RFID encryption cracked

MUNICH, Germany — The Chaos Computer Club (Hamburg, Germany) has cracked the encryption scheme of NXP's popular Mifare Classic RFID chip. The ... transit applications including fare ... cards. NXP ...

...rom releasing MIFARE flaws

[redacted] Standard 1k is on your neck!

[redacted] number generator on chip
- 16-bit entropy
- resets when chip enters EM... (not random at all)

VIP

MiFare RFID c... thought
Seconds not hours to ...
Geeta Dayal
April 15, 2008

PROTECT YOUR PIN

Card can be read
Card can be cloned

[redacted]

Weak proprietary cryptographic algorithm
- 48-bit key
- only 20-bit effective security

Canada

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

When RFID Voting Systems Fail Security

RFID-Based Electronic Voting: What Could Possibly Go Wrong?

Vulnerabilities With Proposed RFID E-Voting Initiative Identified by ...

Research Conducted at Tel Aviv University by Dr. Avishai Wool Reveals Multiple Attack Vectors for Disrupting New Voting Technology

Israeli RFID-based voting system shown to be insecure

Attacks on RFID-Based Electronic Voting Systems

Alameda County Uses RFID to Speed Election Results

Mobile Ticket Control System with RFID Cards for Administering Annual Secret Elections of University Committees

2012V2 35 Canada

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

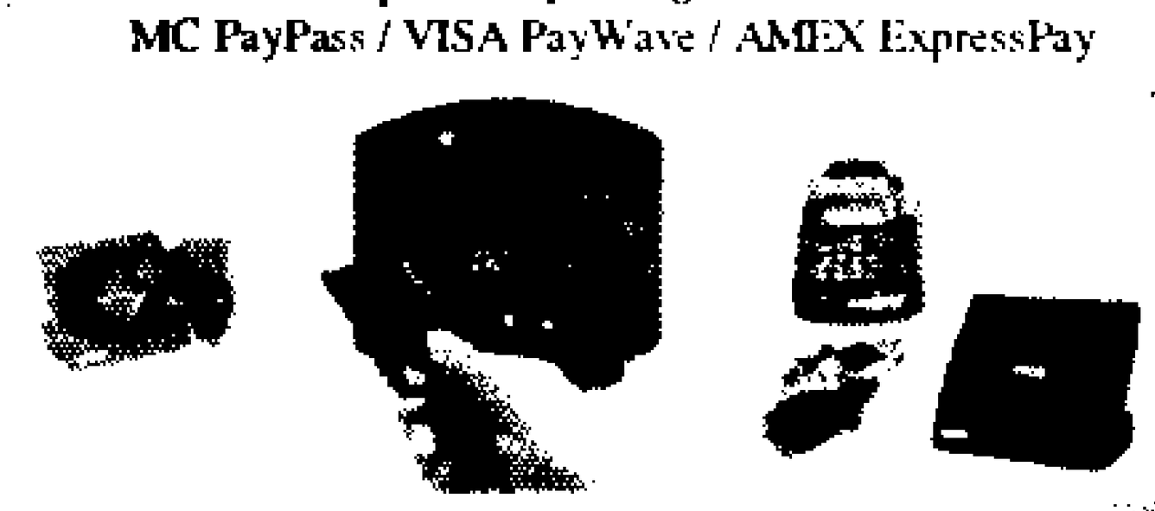
When RFID Credit Cards Fail Security

[redacted] Skimming DEMO

...ily hacked with $8 reader

[redacted] payment systems based on EMV (Europay / MasterCard / Visa) [redacted] specifications – available to anyone who wants to implement them

Examples of *tap-and-go* credit cards:
MC PayPass / VISA PayWave / AMEX ExpressPay



...ng at conference to demonstrate...

Step 0. start project in late November
Step 1: purchase a ~$90 standard RFID reader
Step 2. download free code online for reading EMV cards
Step 3. study and modify the code to extract MC information [redacted]
Step 4: skim colleagues' credit cards to test and improve [redacted]
Step 5. perform online/phone Christmas shopping, [redacted]
(thanks to Tom C., Sylvain M., Jan R., [redacted])

2012V2 36 Canada

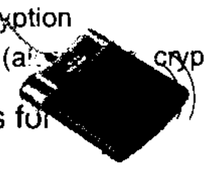
RFID Systems – Some Common Attacks

- Skimming / eavesdropping with range extension
  - Boost illegitimate RFID reader / sniffer antenna gain to obtain 30cm / 9m distance
  - Enable more exploits such as
    - Replay attack
    - Clone attacks
    - Crypto attacks => compromise secret key(s)
- Impersonate authorised tags or readers in RFID system
  - Gain certain privileges (physical or data access)
  - Enable further compromises depending on application
- Denial of service (physical attacks)
  - Jam relevant frequency band => 13.56 MHz
  - Damage or remove tags and even readers



Security Measures for RFID Applications

- RFID is an air interface requiring protection like any wireless technology
  - Chip and reader mutual authentication
  - Communication channel encryption
  - Verify proper implementation (a[illegible] crypto stre[illegible])
- Hardware countermeasures for
  - RF shielding when not in use
  - Resistance to SCA and tampering
  - Physical data-write protection
- Do not forget readers and backend systems (on internet?) security too !!!

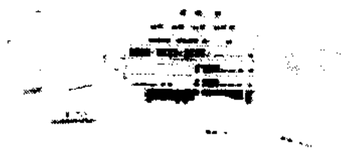
WLAN / IEEE 802.11 Security

Wireless LAN Overview

- Local Area Network that use radio waves as the carrier
- Complement fixed networks by providing mobility to users
- Uses the IEEE 802.11 open standard
- Wi-Fi Alliance for product testing and certification
- Advantages over wired LANs:
  - Fast and easy to deploy
  - Increased mobility inside buildings

Domestic/Consumer vs. Enterprise Wi-Fi

- The difference is **significant**: security, capacity, complexity and cost
- Enterprise Wi-Fi can cater to security requirements for most PROTECTED B scenarios
- Must be implemented correctly!!! **NOT** a "Plug and Play" system: Network **and** RF planning is required for secure deployment.
- Requires RADIUS-type authentication and additional infrastructure.

IEEE 802.11 Air Interface Standards

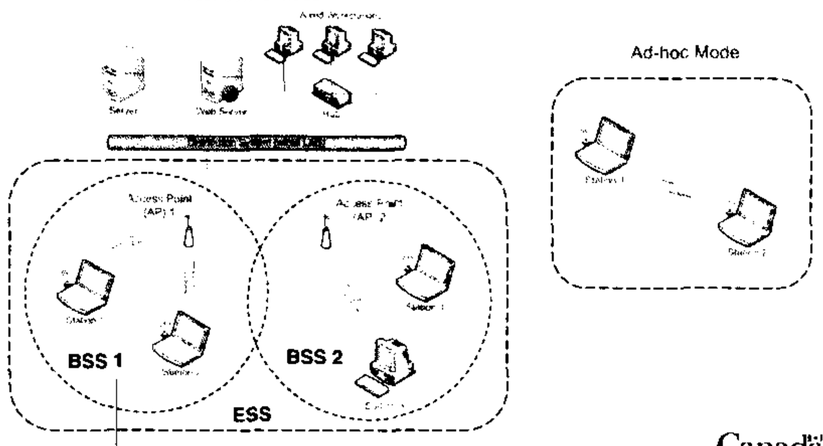
Standard	Year	Frequency (GHz)	Bit Rate (Mbps)	Compatible with
802.11a	1999	5.0	54	802.11a
802.11b	1999	2.4	11	802.11b
802.11g	2003	2.4	22 & 54	802.11b, 802.11g
802.11n	2009	2.4/5.0	Up to 600 Mbps	802.11 a/b/g

- Spread Spectrum techniques:
  - Frequency Hopping (FHSS)
  - Direct sequence (DSSS)
  - Orthogonal Frequency Division Multiplexing (OFDM)
- Spatial Multiplexing techniques:
  - Multiple Input, Multiple Output (MIMO) – resistant to eavesdropping

WLAN Architectures

Infrastructure Mode

Ad-hoc Mode



WLAN Safeguards and Vulnerabilities

Security Mechanism	Authentication	Encryption	Vulnerabilities
WEP	Open (no authentication), Shared Key (Password) Authenticates device, not user.	"RC4" – short key, fast and simple algorithm for older hardware	Weak algorithm, easily breakable with known attacks and freely accessible tools One password, many users- difficult to manage
WPA	Pre-Shared Key, 802.1X Server-based user authentication 802.1X can implement mutual authentication, user authentication	Enhanced security wrapper around WEP mechanism- meant to improve security but still remain compatible with older hardware	Weak algorithm Weak passwords are easily broken If shared password is used, same password management issue as WEP
WPA2	Pre-Shared Key, 802.1X Server-based user	AES-based security, also backwards	Weak passwords are easily broken

WLAN Vulnerabilities: Default Configurations

- Typical factory defaults are not secure
  - SSID set by manufacturer (e.g. "Linksys")
  - Security disabled by default (no encryption)
- Older devices only support WEP
- Open Authentication
  - APs broadcast their SSIDs
  - APs let anyone connect to them
- APs can be configured to only allow certain media access control (MAC) addresses to connect
  - MACs are sent with each packet and can be sniffed and spoofed

WLAN Vulnerabilities Man in the Middle Attacks

- APs never have to prove their identity to clients
- Attackers can pretend to be an AP and let clients willingly give them their data
- Fake AP can then forward traffic to a real AP and modify traffic on the way, or insert a malicious payload
- Also known as "evil twins"

Wi-Fi Protected Setup (WPS)

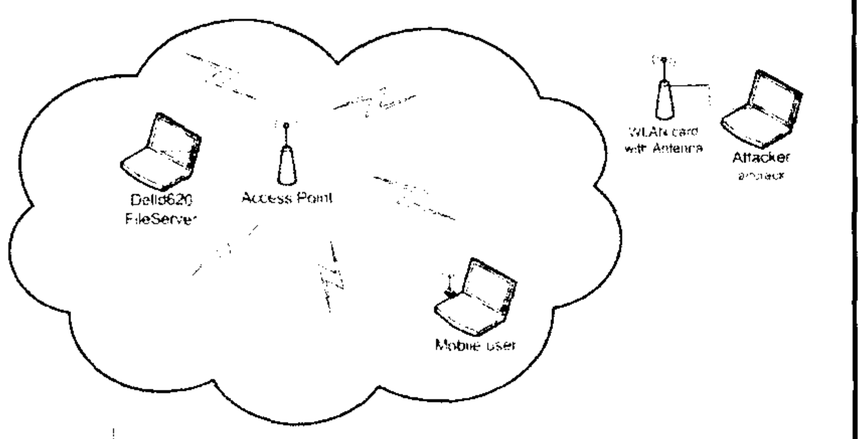
- Introduced in 2007- intended to be an easy way for users to configure secure Wi-Fi connections without technical knowledge
- Access point shares security info and other parameters (pre-shared key, other config info) with client. Client configures itself with these parameters and can subsequently connect securely.
- Original incarnation: user must manually operate a push-button located on the access point to initiate.
- WPS also introduced "PIN" mode- no longer requires user to be physically present at access point to press button: clients can now be set up simply by typing in an 8-digit PIN code (usually printed on a sticker on the bottom of the access point)
- ***Strong WPA2 passphrase now turned into weak 8-digit PIN;***
- *Poor design of PIN verification system further weakens system: max. 11000 guesses needed to find PIN and gain access to system*

Recommendation: DISABLE WPS, use 802.1X RADIUS authentication wherever possible!

Updates to 802.11

- 802.11w – protected management frames: intended to prevent de-authentication/spoofing attacks (ratified 2009)
  - Adds cryptographic protection to prevent deauth and association spoofing. Key derived from 4-way handshake, therefore only available if using WPA/WPA2
  - Available in latest releases of Enterprise-class routers
- 802.11v – network management features: allow centralized management/configuration of wireless devices on the network (balloting 2011)

Demo



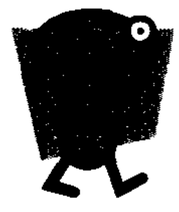
Canada

WLAN Security Recommendations

- Use a Virtual Private Network (VPN)
- If using WEP, disable SSID broadcasts and enable MAC Address Filtering
- Change the default settings / factory configuration (SSID, HTTP and management passwords)
- Put APs outside the corporate firewall, and protect WLAN users with a firewall
- Upgrade equipment to use WPA2 or 802.11i (EAP-TLS with certificates is best recommendation at moment if not using VPN)
- Audit & monitor for unusual activity and rogue APs

Canada

Questions ?



Canada

CSEC
Emergency Management
and
YOU

Emergency Management Office
January 2012

Why Emergency Management?

EMO Purpose:

To protect CSEC's staff, data and infrastructure in the event of an incident or crisis so that the organization can continue to deliver its critical services.

Authorities for the Program:

- Emergency Management Act
- Policy on Government Security
- Operational Standard on Business Continuity
- Canada Labour Code

What are the Threats?

Natural Disasters:

- Weather / Geological / Health

Human-Made Accidental:

- Fire / Infrastructure / Hazardous materials / CBRNE

Human-Made Intentional:

- Terrorism / Workplace violence / Sabotage / Cyber

Are the Threats Real?

Major Disasters in Ontario and Quebec, 1990-2005:

14 floods, 11 forest fires, 4 train wrecks, 15 chemical incidents, 14 industrial fires, 24 storms, 2 epidemics, 6 tornados…

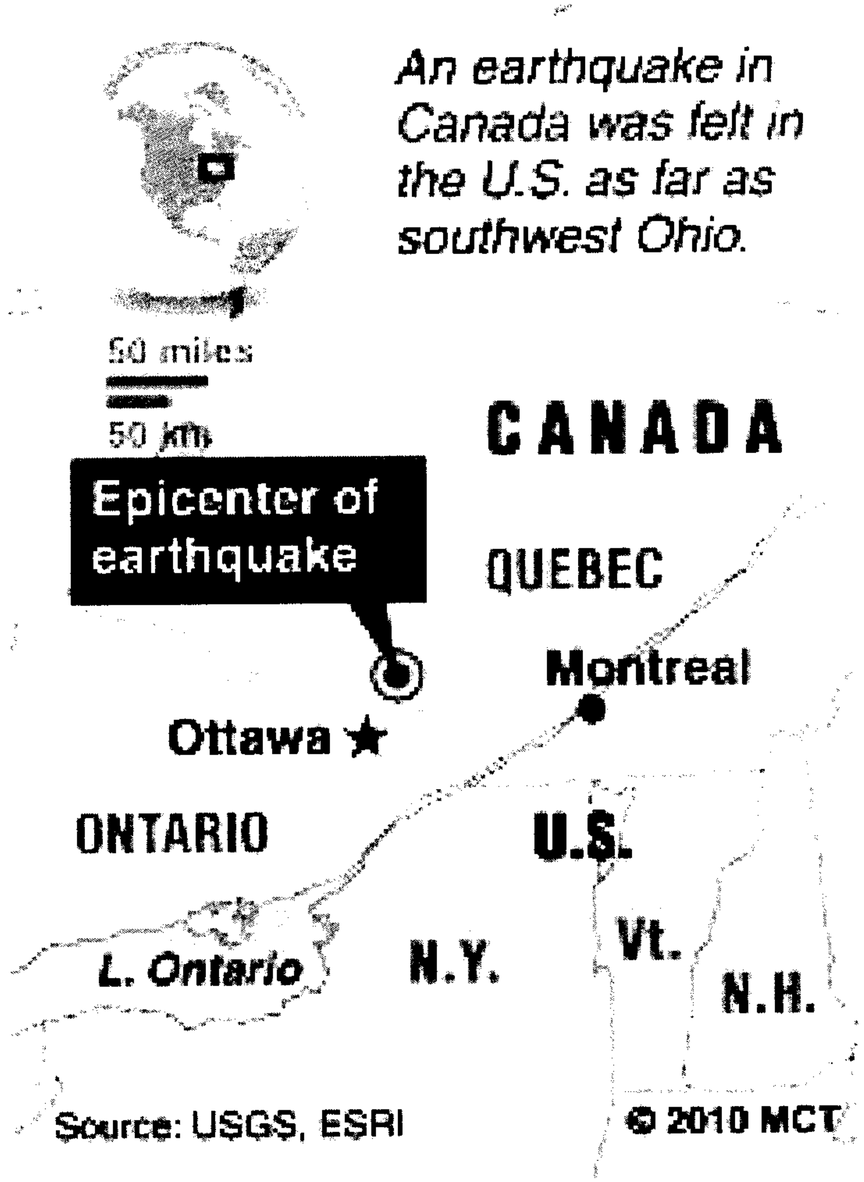
- Total fatalities: 194
- Total injured: 1516
- Total evacuated from their homes: 664,400

Remember This?

- No, not a nuclear test ;-)
- Sunrise Propane in Toronto – August 2008
- Sunday before dawn
- 10,000 people evacuated
- Some not back in homes 6 months later
- Exploding propane tanks rain down on highway 401

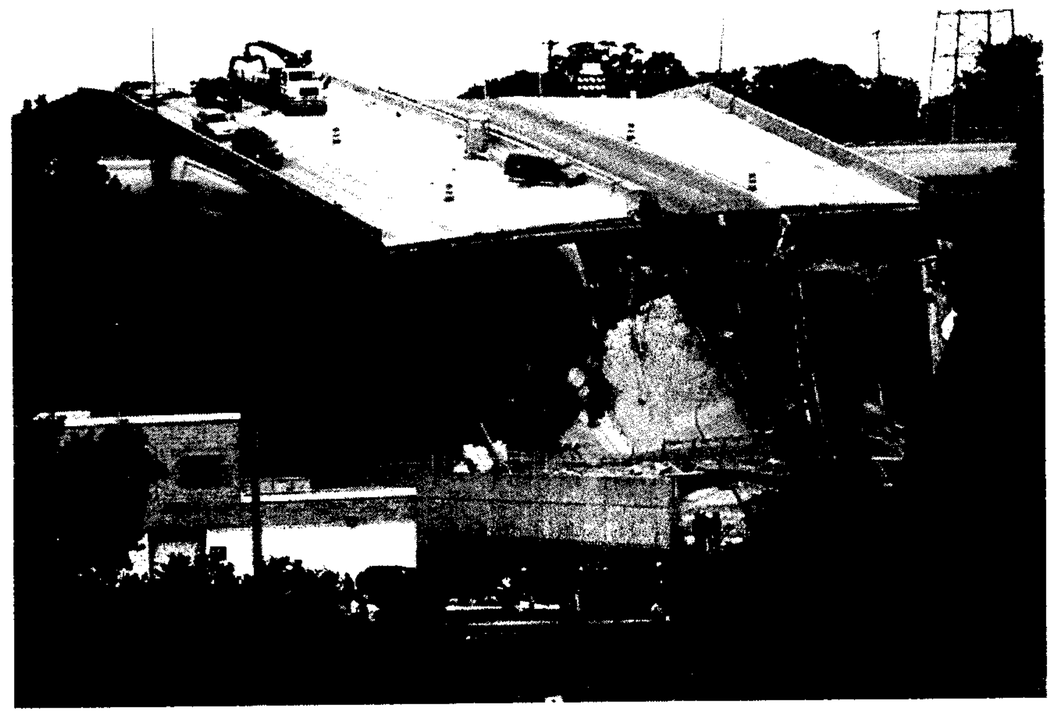
Remember June 23, 2010?

- 5.0 earthquake at 13:41
- Epicentre 56km north
- An incident, not a crisis
- …this time
- Geological evidence of 7.0 in the region
- We expect a 6.0-6.5 quake to happen closer
- It could damage 264 buildings, injure 135, kill 4 and leave 102,000 tons of rubble



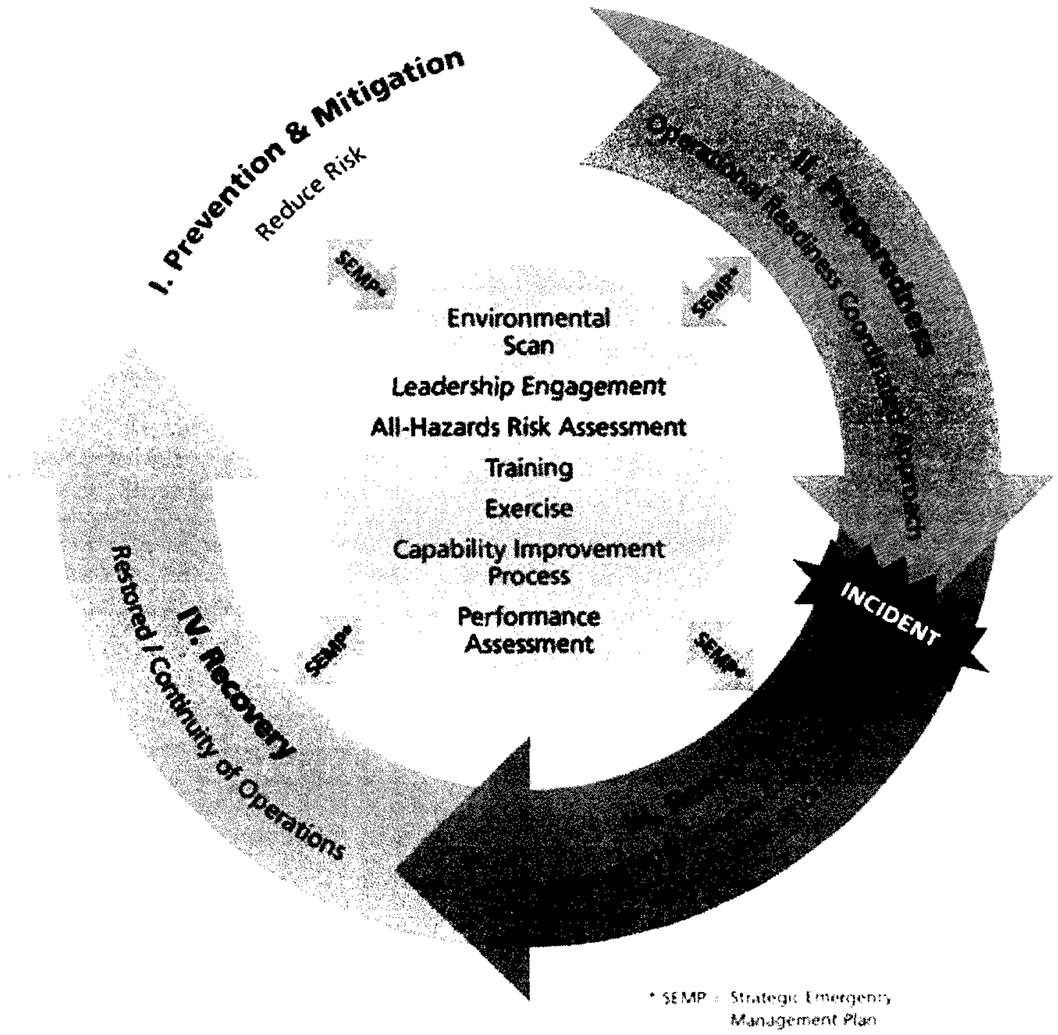
Does Emergency Management Save Lives?

- **August 2007 – the I-35W bridge in Minneapolis collapses during rush hour**
- **13 killed, 145 injured**
- **If the city had not invested in emergency planning, it's estimated 70 more people would have lost their lives**



The Emergency Management Cycle

Emergency Management Continuum



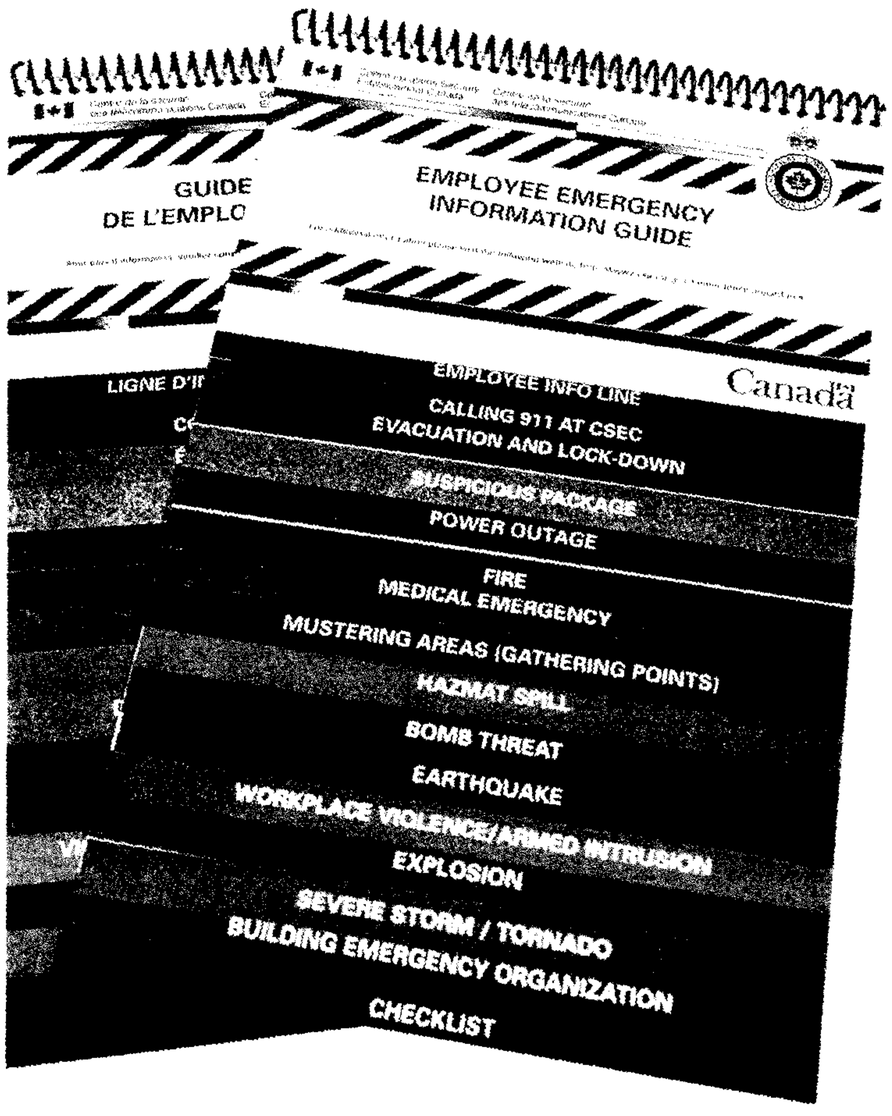
s.15(1)

Business Continuity at CSEC

- CSEC currently has this many critical services:
- These services are deemed critical

- Business Continuity Plans (BCPs): every critical service, group or activity area has one
- The plan may include an alternate location where you can perform your work
- Find out about yours and if you play a role in it!

Employee Emergency Information Guide

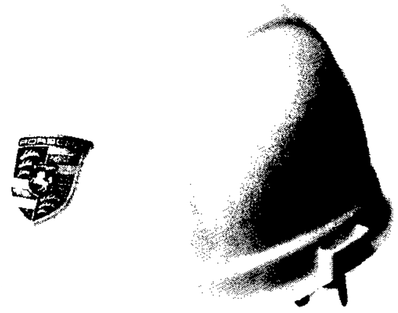


- Keep it <u>on</u> your desk
- Read through the scenarios
- Quiz yourself on them – it could save your life!
- The guide shows you what to do in the most likely emergencies

Your *Building Emergency Organization*

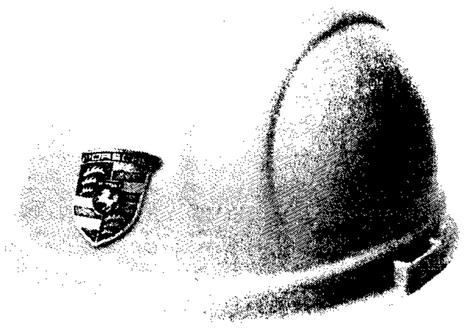
Building Seniors

- Responsible for staff during an incident



Chief Emergency Wardens

- Direct Floor Wardens
- Advise Building Seniors



Floor Emergency Wardens

- Directs staff during incident
- Clears own wing / floor

Evacuation and Mustering

- Follow instructions of your Floor Warden or first responders
- Go to mustering area
- Check in with your manager or one in your group / activity area
- Await instructions before re-entering building or leaving the area

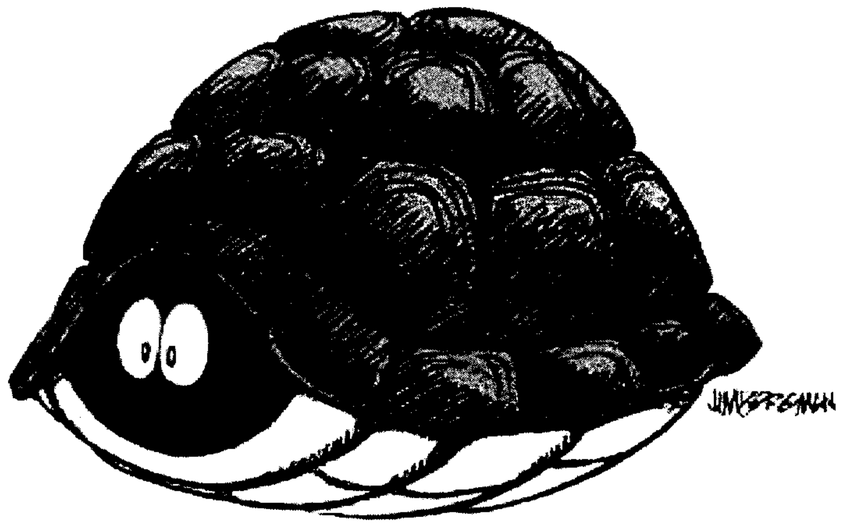
s.19(1)

Lock-Down

- Used vs. an internal threat (terrorism, workplace violence…)
- Lock doors to your work area
- Stay under cover and inconspicuous
- Wait for a trusted authority to tell you the lock-down is over

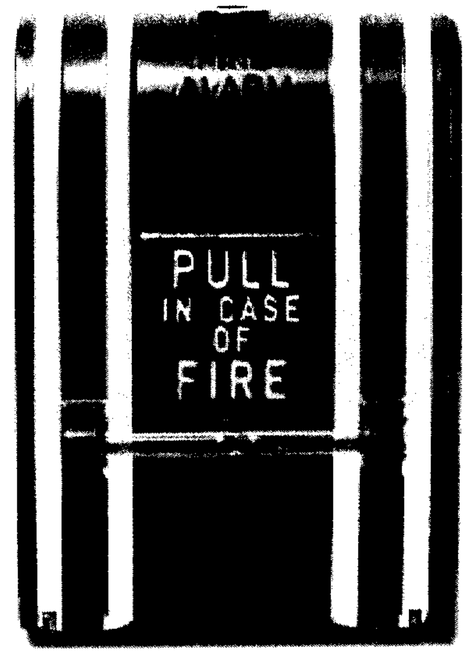
Shelter-in-Place

- **Used vs. an external threat (tornado, HAZMAT spill…)**
- **Lock and seal windows**
- **Avoid proximity to windows if required**
- **Wait for further information and instructions from your Building Emergency Organization**

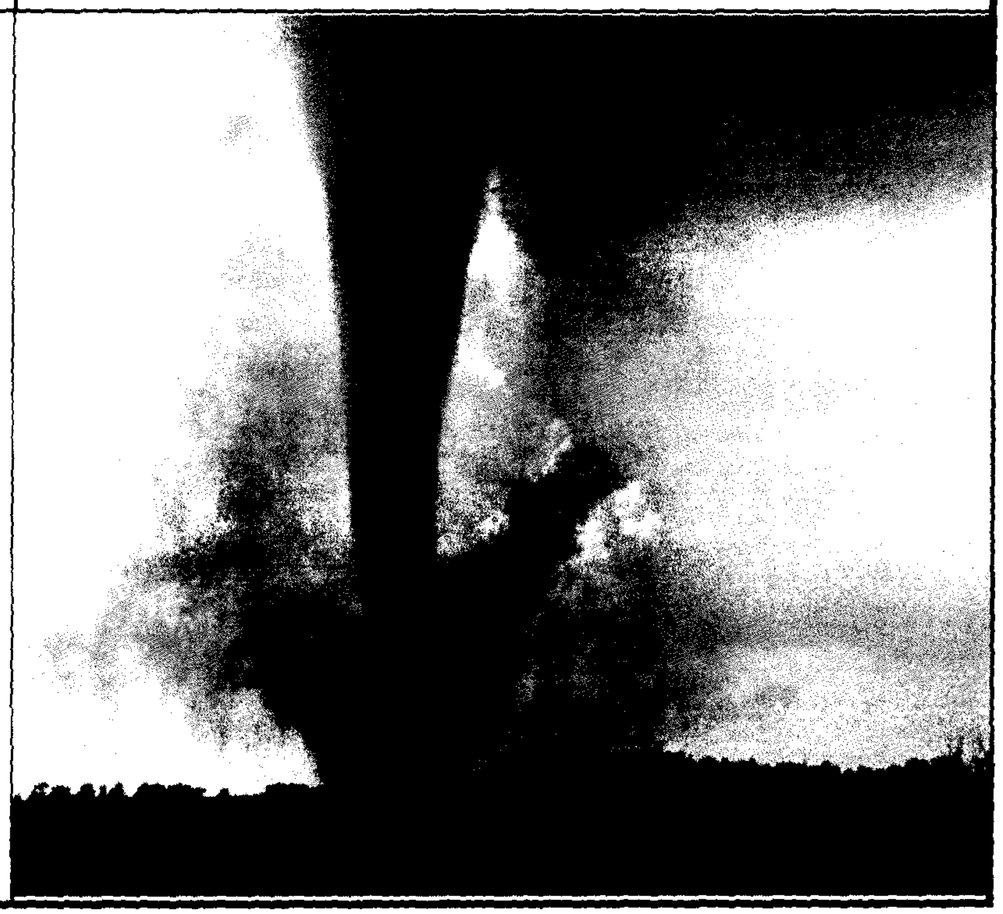


NEVER...

- **NEVER pull a fire alarm unless you see smoke or flames with your own eyes!**
- **Fire alarm triggers automatic building evacuation**
- **In some emergency scenarios, this may cause people to head *toward* the danger and result in loss of life**



Incident vs. Crisis

Not every incident...	...becomes a real *crisis*.
	

Incident- vs. Crisis-Management

During the ***Initial*** Response to an incident, we use the…	If the Incident Evolves into a ***Crisis***, We Switch to the…
Incident Management Plan • ***Building Emergency Organizations*** • ***Employee Emergency Information Guide***	***Crisis Management Plan*** •**CSEC *Emergency Operations Centre (EOC)***

s.19(1)

Emergency Operations Centre

What the EOC Does:

1. Maintains situational awareness in a crisis
2. Centralizes all communications
3. Allows all elements of CSEC to function at their best to meet the challenge

Critical for YOU

1. Make sure you have your manager's contact information and that he / she has yours
2. Make sure you know your mustering area
3. Make sure you learn how to react appropriately in the various emergency scenarios outlined in the EEIG
4. Keep your copy of the EEIG easily accessible at your desk (OHS will be checking!)
5. Get involved – we need Floor Wardens, EOC staff, plan writers, etc.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

AS A SEPARATE AGENCY

LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA (CSTC)

UN ORGANISME DISTINCT

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

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

HOW CSEC CAME TO BE / INSTITUTION DU CSTC

- In 1946 an Order-in-Council approved 179 positions for the National Research Council (NRC) in order to continue the wartime effort of the Communications Research Branch and was called Communications Branch, NRC

- Until 1975, the Minister of State for Science and Technology was accountable to Parliament for CBNRC and funding was provided from DND, External Affairs and the RCMP

- En 1946, un décret autorise la création de 179 postes au Conseil national de recherches (CNR) dans le but d'assurer la continuité du soutien, en temps de guerre, à la Direction des télécommunications, qui prend un nouveau nom, celui de Direction des télécommunications du CNR (DTCNR).

- Jusqu'en 1975, le ministre d'État chargé des Sciences et de la Technologie doit rendre compte, devant le Parlement, de la DTCNR qui est financée par le MDN, le ministère des Affaires extérieures et la GRC.

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

HOW CSEC CAME TO BE / INSTITUTION DU CSTC

- In 1975 the Communications Branch National Research Council was re-named to Communications Security Establishment (CSE) and its Minister would be the Minister of National Defence

- CSE would be the national agency responsible for Canadian COMSEC and SIGINT programs

- C'est à partir de 1975 que l'organisme est désormais désigné sous le nom de Centre de la sécurité des télécommunications (CST) et qu'il relève du ministre de la Défense nationale.

- Le CST devient ensuite l'organisme national responsable des programmes COMSEC et SIGINT canadiens.

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

NEW PLACE IN GOVERNMENT / NOUVELLE PLACE DU CSTC AU SEIN DU GOUVERNEMENT

- November 16, 2011, CSEC's Place in Government (PinG) changed
- CSEC is now a "stand-alone" agency within the National Defence portfolio
- The Chief, CSEC now reports directly to the Minister of National Defence

- Le 16 novembre 2011, la place du CSTC au sein du gouvernement (PauG) est redéfinie
- Le CSTC obtient le statut d'organisme autonome, mais demeure rattaché au ministère de la Défense nationale (MDN)
- Ainsi, le chef du CSTC relève directement du ministre de la Défense nationale

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

NEW PLACE IN GOVERNMENT / NOUVELLE PLACE DU CSTC AU SEIN DU GOUVERNEMENT

- CSEC is still listed as a separate agency under Schedule V of the Financial Administration Act (FAA) but now without the association to DND, and is also now a full department under Schedule I.1 of the FAA

- En vertu de l'Annexe V de la *Loi sur la gestion des finances publiques* (LGFP), le CSTC est toujours considéré comme un organisme distinct Toutefois, son association au MDN n'est plus explicite, et l'organisme obtient, par conséquent, le statut de ministère conformément aux termes de l'Annexe I.1 de la LGFP

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

CSEC'S CURRENT LEGISLATION / LOIS ACTUELLES DU CSTC

- PC 2011-1301 added CSEC to Schedule I.1 to the *Financial Administration Act (*FAA) as a department and as such, the position of Chief, CSEC is now a Deputy Head

- PC 1975-708 - the "Exclusion of Positions and Employees Approval Order" still excludes CSEC from the application of the Public Service Employment Act (PSEA). CSEC is in the process of updating it's EAO

- Le décret C.P. 2011-1301 prévoit l'ajout du CSTC à la liste des ministères figurant en Annexe I.1 de la *Loi sur la gestion des finances publiques* (LGFP). Par conséquent, le chef du CSTC devient désormais administrateur général

- C.P. 1975-708 – Selon le « Décret d'exclusion des postes et employés », le CSTC n'est toujours pas soumis à la *Loi sur l'emploi dans la fonction publique* (LEFP). Au reste, le CSTC s'apprête à mettre à jour le décret d'exclusion le concernant

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

CSEC'S CURRENT LEGISLATION / LOIS ACTUELLES DU CSTC

- 2007 - Instrument of Delegation of Human Resources Management Authorities delegated human resource management authorities from the DM ND to various authority levels within CSEC. This will be updated to reflect the change to the position of Chief CSEC

- 2007 – L'instrument de délégation des pouvoirs liés à la gestion des ressources humaines a permis au SM/MDN de déléguer les pouvoirs en matière de ressources humaines à divers niveaux de pouvoirs à l'intérieur du CSTC. L'énoncé de cette mesure sera amendé de façon à tenir compte des changements apportés aux fonctions du chef du CSTC

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

STAFFING AUTHORITIES / POUVOIRS DE DOTATION EN PERSONNEL

- CSEC has always had an Exclusion Approval Order (EAO) which excluded us from the application of the Public Service Employment Act
- CSEC is currently updating it's EAO to ensure that it continues to respect CSEC's national security requirements as well as uphold the values of the PSEA

- Le CSTC a toujours joui d'un décret d'exclusion qui l'a exempté de l'application de la *Loi sur l'emploi dans la fonction publique*
- Le CSTC est en train de mettre le décret d'exclusion à jour, de façon à maintenir le respect des exigences du CSTC en matière de sécurité nationale et à refléter les valeurs de la LEFP

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

WHAT IS A SEPARATE AGENCY? / QU'EST-CE QU'UN ORGANISME DISTINCT?

- Separate Agencies such as CSEC are listed under Schedule V of the FAA
- CSEC is part of what is known as the "federal public administration" and NOT the "core public administration"

- Les organismes distincts, comme le CSTC, sont répertoriés dans la liste figurant en Annexe V de la LGFP
- Le CSTC fait partie de ce que l'on considère comme « l'administration publique fédérale » et NON de « l'administration publique centrale »

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

WHY SEEK SEPARATE AGENCY STATUS? / POURQUOI CHERCHER À OBTENIR LE STATUT D'ORGANISME DISTINCT?

- CSEC's mandate warrants a certain degree of autonomy from central administration
- Certain operational requirements are not well addressed within traditional collective agreements. CSEC has the potential to rationalize the collective bargaining structure to one that fits more closely with our operations. We must though, still negotiate under a Treasury Board Secretariat (TBS) approved mandate

- Le mandat du CSTC garantit un certain degré d'autonomie relativement à l'administration centrale
- Les conventions collectives traditionnelles ne parviennent pas à tenir compte adéquatement de certaines exigences opérationnelles. Le CSTC peut rationaliser la structure des unités de négociation collective pour en créer une qui convient mieux à ses opérations. Par contre, le CSTC doit encore négocier sa convention conformément au mandat approuvé par le Secrétariat du Conseil du Trésor

BENEFITS AS A SEPARATE AGENCY/ AVANTAGES D'ÊTRE UN ORGANISME DISTINCT

- CSEC's unique HR requirements benefit from having its own classification and compensation plans

- Our classification system (UNISON) is tailored to the specific nature of our operations and to best represent the value that CSEC feels should be placed on specific jobs

- Our compensation plan is tied to the classification system. This facilitates the recruitment of specially skilled individuals

- En raison de ses exigences en matière de RH, le CSTC bénéficie de son propre système de classification et de ses régimes de rémunération

- Le système de classification (UNISON) du CSTC peut être adapté à la nature particulière de ses opérations et peut mieux représenter la valeur que l'on devrait porter à certains postes

- Le système de rémunération du CSTC est rattaché à son système de classification. Ce concept facilite le recrutement de personnes particulièrement compétentes

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

DISADVANTAGES AS A SEPARATE AGENCY / DÉSAVANTAGES D'ÊTRE UN ORGANISME DISTINCT

- Difficult to obtain the support/advice and guidance of TBS or other central agencies

- CSEC must have its own HR infrastructure in place – we can not rely on the provision of services from the public service

- Il est difficile d'obtenir de l'appui, des conseils et de l'orientation du Secrétariat du Conseil du Trésor ou d'autres organismes centraux.

- Le CSTC doit avoir sa propre infrastructure de RH; il ne peut compter sur les services offerts par la fonction publique.

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

CSEC TODAY / LE CSTC AUJOURD'HUI

CSEC Human Resources Management Authorities are exercised in accordance with the:

- *Financial Administration Act* (FAA)
- *Public Service Labour Relations Act* (PSLRA)
- *Employment Equity Act* (EE)
- *Canadian Human Rights Act* (CHRA)
- *Public Service Superannuation Act* (PSSA)
- *Canada Labour Code* Part II (CLC Part II)
- *Official Languages Act* (OL)[1]
- *Access to Information and the Privacy Act* (ATIP)

1 CSEC is not subject to all of the OL Directives that flow from the OL Act

Les pouvoirs liés à la gestion des ressources humaines du CSTC sont exercés en vertu des lois suivantes :

- *Loi sur la gestion des finances publiques* (LGFP);
- *Loi sur les relations de travail dans la fonction publique* (LRTFP);
- *Loi sur l'équité en matière d'emploi* (EE);
- *Loi canadienne sur les droits de la personne* (LCDP);
- *Loi sur la pension de la fonction publique* (LPFP);
- *Code canadien du travail, partie II* (CCT, partie II);
- *Loi sur les langues officielles*[1];
- *Loi sur l'accès à l'information* et *Loi sur la protection des renseignements personnels* (AIPRP)

1 Le CSTC n'est pas assujetti à toutes les directives relatives aux langues officielles que comporte la *Loi sur les langues*

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

CSEC TODAY / LE CSTC AUJOURD'HUI

CSEC enjoys the flexibilities of being a Separate Agency and as a Deputy Head, the Chief CSEC has been delegated the following human resources management authorities:

- determining CSE's human resource requirements and their allocation and utilization
- training and development needs and terms and conditions relating to training
- classification
- pay regulation, hours of work and leave
- performance awards
- disciplinary standards
- collective bargaining

En tant qu'organisme distinct, le CSTC jouit d'une certaine souplesse. En outre, le Conseil du Trésor a délégué, au chef du CSTC, certains pouvoirs en matière de gestion des ressources humaines :

- l'identification des exigences, de l'allocation et de l'utilisation des RH
- Les exigences et modalités relatives à la formation et au perfectionnement
- la classification
- la rémunération, les heures de travail et les congés
- les primes au rendement
- les normes disciplinaires
- la négociation collective

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

CSEC TODAY / LE CSTC AUJOURD'HUI

These flexibilities come with an obligation to:

- adhere to existing applicable Legislation
- consult with TBS if we choose to **SIGNIFICANTLY** modify HR or compensation policies
- uphold the provisions of its relevant collective agreement
- respect the values of the Federal Government environment in its day-to-day activities

Toutefois, cette souplesse entraîne un certain nombre d'obligations :

- adhérer aux lois applicables
- consulter le SCT si le CSTC décide d'apporter des modifications **CONSIDÉRABLES** aux politiques de RH ou de rémunération
- respecter les dispositions de sa convention collective pertinente
- respecter les valeurs du gouvernement fédéral dans ses activités quotidiennes

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

CSEC IN THE FUTURE / PROCHAINEMENT, AU CSTC

- HR will continue to exercise maximum flexibility with respect to policies, procedures and guidelines and terms and conditions of employment to ensure the needs of CSEC are considered and well respected

- Les RH continueront à être le plus souple possible en vertu des politiques, des procédures, des lignes directrices et des modalités d'emploi, pour veiller à ce que l'on tienne rigoureusement compte des besoins du CSTC

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CONCLUSION

QUESTIONS?

DES QUESTIONS?

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Foundational Learning Curriculum

Introduction to IT Security

Canada

Outline

- Why IT Security?
- What is GC IT Security?
- How does CSEC support Government of Canada (GC) IT Security?

Why IT Security?

Policy on Government Security (PGS):

"Government security is the assurance that information, assets and services are protected against compromise…"

"…security threats, risk and incidents must be proactively managed to help protect the government's critical assets, information and services, as well as national security."

Why Cybersecurity?

Canada's Cyber Security Strategy:

"Canadians want to be prepared for all types of 21st century threats, and they want to be assured that the information being stored and shared in Government computers is protected."

Hon. Rona Ambrose, 3 Oct 2010

"A secure cyberspace is vital to sustaining and building Canada's economic advantage."

Hon. Christian Paradis, 3 Oct 2010

Key Definitions

- Threat: Any potential event or act, deliberate, accidental or natural hazard that could cause injury to employees or assets, and thereby affect service delivery adversely.

- Compromise: The unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information.

- Vulnerability: An inadequacy related to security that could increase susceptibility to compromise or injury.

IT security seeks to protect from:

Unauthorized Access or Use

Unauthorized Disclosure: *CONFIDENTIALITY*

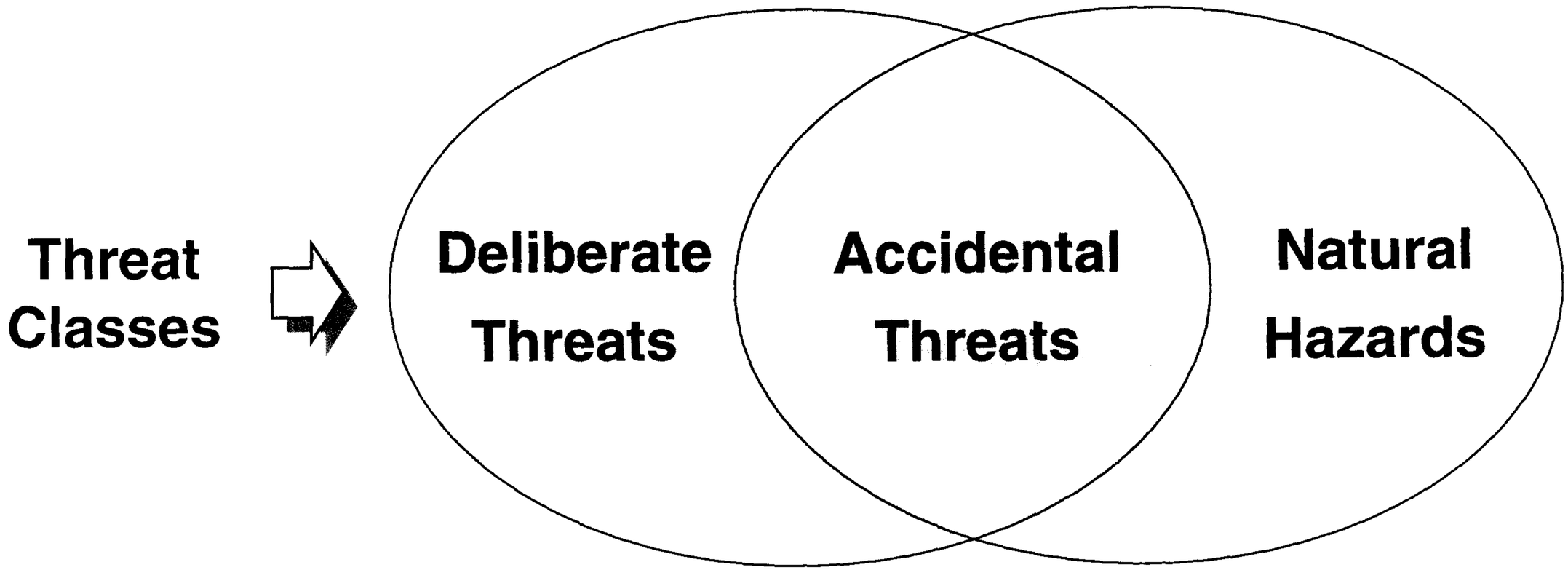
Unauthorized Modification: *INTEGRITY*

Unauthorized Destruction/Disruption: *AVAILABILITY*

Canada

Threat Classes

Human Agents



Classes of Threats and Examples

Threat Class	*Actors*	*Typical Events*
Deliberate	State Sponsored Terrorists Industrial Hackers Organized Crime/Criminals Disgruntled Employees	
Accidental	Employees Outsiders Other organizations	
Natural Hazards	Mother Nature and Father Time.	

General Threat Picture

Cyber Defence Report

- Cyber threat actors
- Severity of incidents
- Commonly detected threat vectors

Adversary Tools & Techniques

- Spoofing/Pharming
- Social engineering
  - Phishing/vishing
  - Identity theft
- Theft/Tampering
- Elevation of Privilege
- DoS/DDoS
  - Jamming (EW)
  - Botnets
- SPAM
- Malware
  - Trojan
  - Worms/Virus
  - Rootkits
  - Spyware

A Specific Point - Insider Problems

- Many users **believe** that:
  - nothing (or very little) of importance exists on their computers
  - technology alone can solve the security problems
  - all threats are external
  - nothing bad can happen to them – until it does

[redacted]

- [redacted]
  - Opening email attachments from strangers
  - Poor password and patch management
  - Leaving PCs on, unattended
  - Web-surfing, social networking at work
  - Sharing information and machines
  - Not reporting security violations
  - Poor control of personal electronic devices

So, why IT security?

So, what is GC IT Security?

What is IT Security within the GC?

"...safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

"...will also include safeguards applied to the assets used to gather, process, receive, display, transmit, reconfigure, scan, store, or destroy information electronically."

MITS

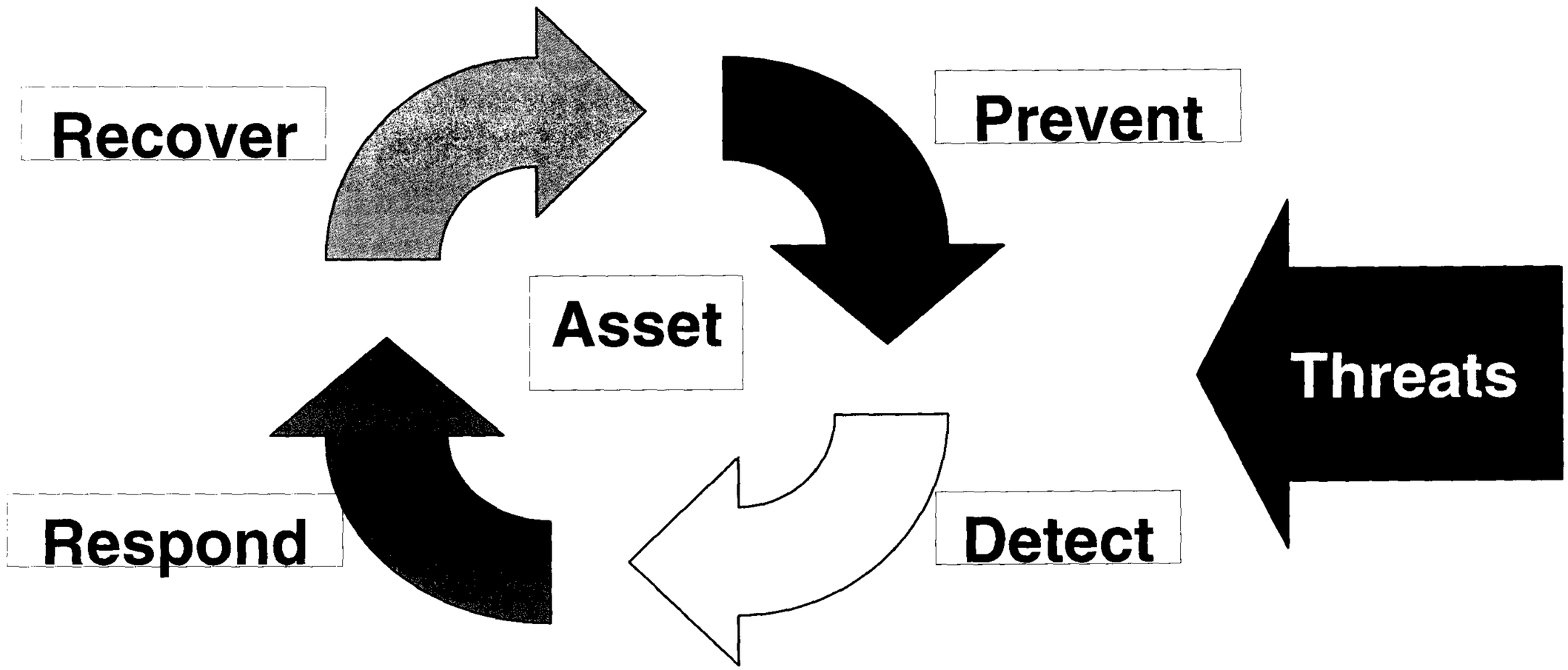
Canada

Principles of Management of IT Security

- Service delivery **requires** IT security
- IT security practices **need** to reflect the changing environment
- The Government of Canada (GC) is a single entity
- Working together to support IT security
- Decision-making **requires** continuous risk management

Operational Security Standard Management of IT Security (MITS)

A Key Concept - Active Defence Strategy



MITS, Part III, Section 15.

Canada

Safeguard Examples

Management Safeguards	Technical Safeguards	Operational Safeguards

• Security Policy
• Asset Categorization
• Risk Management
• Contracting
• Sharing Info/Assets
• Assessment & Audit
• Security Awareness
	• Evaluated Products
	• Access Control
	• Cryptography/PKI
	• Network Security
	• Mobile Computing
	• Wireless Devices
	• Emission Security
		• Incident Management
		  • Detection
		  • Response
		  • Reporting
		  • Recovery
		• Configuration Mgt.
		• Patch Management
		• Capacity Planning

Communications Security (COMSEC) - A Primer

- a sub-set (discipline) of IT Security
- the protection that results from the application of **cryptographic**, **transmission** and **emission** security measures to information stored, processed or transmitted electronically.
- includes the **physical** and **personnel** security measures required to safeguard COMSEC material.

COMSEC Disciplines

- **Cryptographic Security** (CRYPTOSEC):
  - authorized keys, authorized equipment
- **Transmission Security** (TRANSEC):
  - Operating procedures, frequency hopping/spread spectrum, (anti-jamming)
- **Emission Security** (EMSEC):
  - Reduction of compromising emanations, [redacted] separation

Objectives of COMSEC

- To ensure that covert acquisition of intelligence is not possible from any IT system transmitting or receiving sensitive material.

But bad things do happen!

- To ensure that any attempt to tamper, modify or deceive IT systems or operators is immediately detected by authorized personnel.

Protecting COMSEC Information

- Dependence on IT is growing
  - Institutions/industry can't function without operational IT
  - *Awareness/Training/Education* is essential
- COMSEC information is a primary target
  - Adversaries want information about your IT and COMSEC
  - Unauthorized access defeats security safeguards
- Breach of COMSEC jeopardizes much more material
  - Future communications
  - Past communications

So, what is GC IT Security?

How does CSEC support GC IT Security?

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

CSEC Mandate

A. To acquire and use information from the global information infrastructure (GII) for the purpose of providing foreign intelligence, in accordance with Government of Canada (GC) intelligence priorities;

B. To provide advice, guidance and services, to help ensure the protection of electronic information and of information infrastructures of importance to the GC; and

C. To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC as a Lead Security Agency (LSA)

As a lead security agency, CSEC " provides leadership and coordination for departmental activities that help ensure the **protection of electronic information and information systems of importance** and serves as the government's **national authority** for SIGINT and **COMSEC**."

Policy on Government Security (PGS)

Canada

ITS and Canada's Cyber Security Strategy

- improve capacity to detect and defend against cyber threats.
- increase capacity to collect and analyze foreign intelligence on foreign cyber actors and adversaries.
- design and deliver standardized incident handling training to the IT Security Incident Recovery Team (ITSIRT) and to the broader Government IT community.
- In collaboration with other departments and agencies, develop enterprise IT security designs, supported by private industry insight, expertise, and best practices.

How does CSEC support GC IT Security?

Conclusion

- Why IT Security?
- What is GC IT Security?
- How does CSEC support Government of Canada (GC) IT Security?

Questions

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Values and Ethics at CSEC

Foundational Learning Curriculum Presentation

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

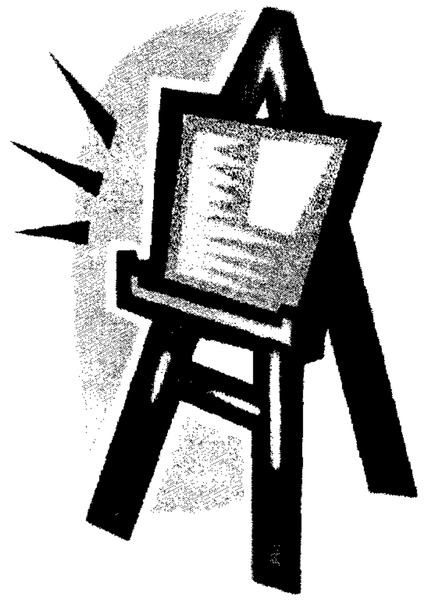
CSEC VALUES AND ETHICS WORKSHOP

Canada

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

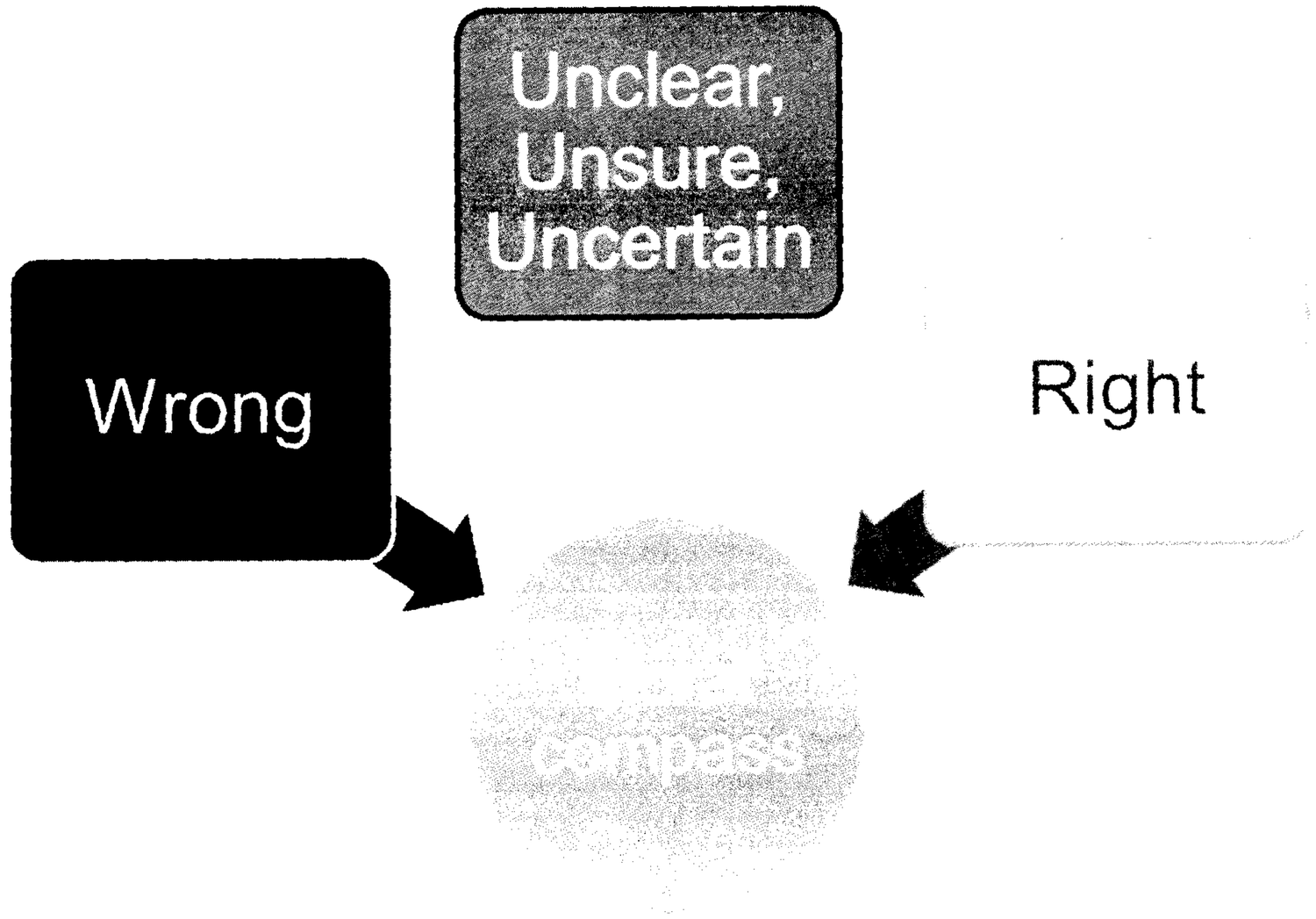
Presentation Outline

- **Values and Ethics**
- **CSEC's Values and Ethics Code**
- **Disclosure of Wrongdoing**
- **Conflict of Interest**
- **Case Studies** (Hypothetical)



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

Ethical Spectrum



Canada

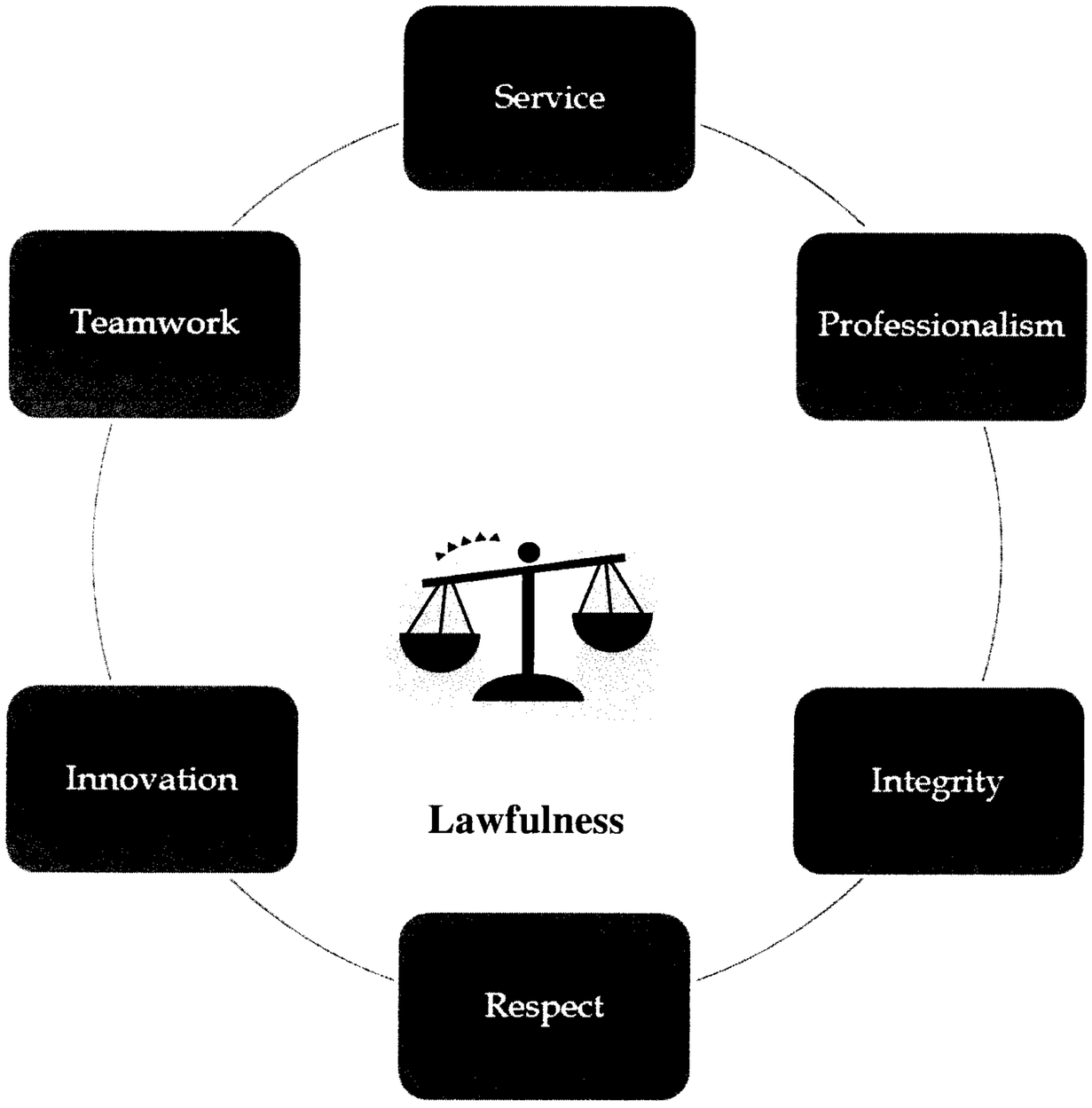
Values (Def'n.)

- Fundamental principles, beliefs or maxims that underlie the attitudes, perceptions, priorities and behaviours of an individual or, when adopted by a group of individuals or an organization, of the group or organizational membership

- Personal values
- Organizational values

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

SPIRIT OF THE LAW



Canada

Ethics (Def'n.)

- In an organizational context, ethical behaviour, or *ethics*, is the expression or "coming to life" of an organization's values through the conduct of its employees—the organization's "values in action" or "applied values".

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

CSEC Values & Ethics Code

- Defines the *values* and *ethics* of CSEC to guide and support employees in their professional activities

- Contributes to public confidence in the integrity of CSEC's operations and its objectivity in providing information and advice

- Describes the process to deal with issues, questions or concerns regarding ethics in the workplace

- Important since CSEC is excluded from the "Public Service Disclosure Protection Act" in regard to Values and Ethics, Conflict of Interest and *Wrongdoing*

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

Wrongdoing (Def'n.)

Any of the following within the context of, or in relation to, CSEC:

- A contravention of any Act of Parliament or the legislature of a province or territory, or of any regulations made under any such Act
- A misuse of public funds or a public asset
- A gross mismanagement
- A serious breach of the *CSEC Values and Ethics Code* or security policies
- An act or omission that creates a substantial and specific danger to the life, health and safety of persons, or to the environment, other than a danger that is inherent in the performance of the duties or functions of an employee
- Knowingly directing or counselling a person to commit a wrongdoing set out above

Canada

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

Internal Disclosure of Wrongdoing (Def'n.)

- The provision of any information by an employee in good faith and in accordance with established procedures based on the belief that the information could show that a wrongdoing has been, is being or is about to be committed, or that the employee has been asked to commit a wrongdoing.

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

C(I) - Internal Disclosure Mechanism

- **Means to discuss or report serious ethical issues encountered in CSEC, without fear of *reprisal*.**

- **If you suspect a wrongdoing or want ethics advice, you can speak to your manager or contact the DGAEE/Ethics Officer.**

- **If you are being asked to act contrary to the Values & Ethics Code, or are the target or victim of a reprisal, you can also report this in confidence to the DGAEE/Ethics Officer.**

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Internal Disclosure Process

Advice

- Initial meeting with Ethics Office to characterize situation

Screening

- Review and initial consultations to determine grounds to terminate or continue

Investigation

- Data mining
- Interviewing
- Consultations

Reporting

- Report with conclusions
- Notification to all parties concerned
- Management letters

Canada

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

A(I) - Conflict of Interest Measures (1)

What are They?

- Rules of conduct.
- Aimed to minimize the possibility of a real or apparent conflict of interest (COI) arising between an employee's private interests and duties.
- Maintains public confidence in CSEC's impartiality and objectivity.
- Protects employees from allegations.

Real vs Potential vs Apparent COI

- **Real:** Your public duties & responsibilities are influenced
- **Potential:** Your public duties & responsibilities could be influenced
- **Apparent:** A reasonably informed person could conceive that a COI exists, even if there is neither a potential or real conflict.

Canada

A(I) - Conflict of Interest Measures (2)

How Does it Impact Me?

- The Code outlines employee responsibilities which address:
  - Private affairs and interests
  - Outside employment activities
  - Gifts, benefits and hospitality
  - Preferential treatment
  - Taking advantage of (or benefiting from) information
  - Use of government property

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

A(I) - Conflict of Interest Measures (3)

Process – If You Have Something to Declare

- **Review your situation upon hire and, if required, you must submit a Confidential Report to Labour Relations (LR) via DGHR within 60 days of initial appointment.**
- **You are obligated to review your situation on an ongoing basis and resubmit if required:**
  - as your duties change
  - as your assets/liabilities/outside activities
  - hospitality/benefits
- **If in doubt – ask manager, DGHR or DGAEE – better safe than sorry (disciplinary measures)**
- **LR will analyze the case and make recommendations to DGHR to either:**
  - avoid or withdraw from your activities;
  - have an asset sold at arm's length or placed in blind trust;
  - pursue as is with or without conditions.
- **You will receive a letter from DGHR.**

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Cases

(Hypothetical)

Case #1 - Roll-Up The Rim (and Win?)

Scenario

You enter Tim Hortons with a friend during its periodic contest. You both get a coffee and she pays for yours. When you finish your coffee and roll up the rim, you find that the cup qualifies to win a vehicle. What would you do?

Case #1 - Roll-Up The Rim (and Win?)

Scenario

You enter Tim Hortons with a friend during its periodic contest. You both get a coffee and she pays for yours. When you finish your coffee and roll up the rim, you find that the cup qualifies to win a vehicle. What would you do?

Inform

- Pretend that the cup is not a winner. You don't want your friend to feel badly.
- Tell her that the cup is a car winner so she can celebrate your good fortune.
- Mention that the cup is a winner but don't say of what unless she asks.

Act

- Keep the car. The coffee was a gift, you have the cup, and there was no stipulation that any winnings would go to your friend which you agreed to as a condition of accepting the free coffee.
- Keep the car but pay her back for the coffee.
- Keep the car but offer to always pay for *her* coffee from now on.
- Sell the car and give her half (or some share) of the amount received.
- Give her the cup. After all, she paid for it and it might have been hers otherwise. To you a friend is more important than a car.

➢ Situational factors might influence your response.

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

Case #2 – What's Your Problem?

Scenario

- Jean is a new CSEC employee in the SIGINT business line.
- He is given an operational procedure, OPS-1-X. As he reads it, it seems to require doing something inconsistent with an objective of OPS-1 in that it would negatively impact the privacy of Canadians without an operational benefit.
- He discusses his conclusion with a few other colleagues. They don't seem concerned about his point and suggest that he is making too much of it because what is described is how this has been done for several years.
- None of the proposed explanations specifically address Jean's concern; he remains confused and troubled.

Question: What should Jean do in this situation?

Canada

Case #2 – What's Your Problem?

Scenario

- Jean is a new CSEC employee in the SIGINT business line.
- He is given an operational procedure, OPS-1-X. As he reads it, it seems to require doing something inconsistent with an objective of OPS-1 in that it would negatively impact the privacy of Canadians without an operational benefit.
- He discusses his conclusion with a few other colleagues. They don't seem concerned about his point and suggest that he is making too much of it because what is described is how this has been done for several years.
- None of the proposed explanations specifically address Jean's concern; he remains confused and troubled.

Question: What should Jean do in this situation?

Suggested Responses

- Go to his supervisor/manager.
  - Can go to DGAEE.
    - Resolve it to the point of satisfactory understanding.
      - Jean may be right--*group think* may be contributing to acceptance of inappropriate procedures, interpretations and/or conduct.

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

Case #3 – It's Tax Season…

Scenario

Charles likes to keep busy in the evenings and earn extra income. Charles has therefore decided to do income tax reports for clients. His job at CSEC is in the finance department (contract & procurement). Charles has exhausted his list of friends/family members to whom he can offer his services. He decides that he'll offer income tax filling services to the consultants that CSEC will be hiring in the months to come, as their files come to his desk.

Questions

- What should Charles consider as key elements when making his decision to promote his services?
- What should Charles do in this situation?

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

Case #3 – It's Tax Season…

Scenario

Charles likes to keep busy in the evenings and earn extra income. Charles has therefore decided to do income tax reports for clients. His job at CSEC is in the finance department (contract & procurement). Charles has exhausted his list of friends/family members to whom he can offer his services. He decides that he'll offer income tax filling services to the consultants that CSEC will be hiring in the months to come, as their files come to his desk.

Questions

- What should Charles consider as key elements when making his decision to promote his services?
- What should Charles do in this situation?

Suggested responses

- **Charles should consider whether his outside activities are in conflict with his duties at CSEC (real/potential/perceived). He should consider submitting a confidential report.**
- **If it is determined that there is no conflict then the work must be completed outside of normal working hours, CSEC equipment is not to be used and the activities should not distract from the employee's performance of their official duties.**
- **Charles needs to ask himself if he is privy to the list of consultant names because of his role/duties. Public servants should not knowingly take advantage of, or benefit from, information that is obtained in the course of their official duties and that is not generally available to the public.**
- **If Charles chooses to advertise his services he should not do so on the CSEC intranet forum (disclaimer upon log on "I agree"). He can do this on the bulletin boards only. No direct solicitation.**

Canada

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

Case #4 – IT Security Dilemma

Scenario

- Mary is a new employee at CSEC in an IT Security section that evaluates IT products for Government of Canada use.
- She wants to be professional and complete in the advice she gives because she believes in "anticipating, understanding and responding appropriately to client needs."
- She is aware of a potential concern with one of the products that a client department might use for a system as a result of a classified briefing she received during a visit to an allied counterpart of CSEC.
- The *Security of Information Act* defines the information she has as "special operational information".
- No one she is dealing with in the client department has the appropriate clearance.

Question: What should Mary do in this situation?

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

Case #4 – IT Security Dilemma

Scenario

- Mary is a new employee at CSEC in an IT Security section that evaluates IT products for Government of Canada use.
- She wants to be professional and complete in the advice she gives because she believes in "anticipating, understanding and responding appropriately to client needs."
- She is aware of a potential concern with one of the products that a client department might use for a system as a result of a classified briefing she received during a visit to an allied counterpart of CSEC.
- The *Security of Information Act* defines the information she has as "special operational information".
- No one she is dealing with in the client department has the appropriate clearance.

Question: What should Mary do in this situation?

Suggested Response

- Discuss with her manager. Mary may not be authorized to resolve it.
    - There are internal (senior-level) mechanisms to deliberate such issues, consider what is in the national interest, and to render appropriate decisions.

Canada

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

Case #5 – Everybody Does It (? Or !)

Scenario

- Peter is a term CSEC employee in a directorate whose employees frequently travel to conferences to remain current in their field.
- Two senior directorate employees bragged in front of him about how easy it is to generate "entertainment" money on trips by claiming for meals that are actually provided free of charge as part of the conference registration.
- They indicated that the boss was aware of the practice and turned a blind eye to it when signing their claims.
- Peter wasn't sure if he had heard them correctly and spoke with Sally, a co-op student, who was also in the office at the time. Her understanding was the same as his.
- Peter finds it hard to work with people he no longer respects because of what he now believes about their ethics and behaviour. He still hopes to become an indeterminate employee one day.

Case #5 – Everybody Does It (? Or !)

Scenario

- Peter is a term CSEC employee in a directorate whose employees frequently travel to conferences to remain current in their field.
- Two senior directorate employees bragged in front of him about how easy it is to generate "entertainment" money on trips by claiming for meals that are actually provided free of charge as part of the conference registration.
- They indicated that the boss was aware of the practice and turned a blind eye to it when signing their claims.
- Peter wasn't sure if he had heard them correctly and spoke with Sally, a co-op student, who was also in the office at the time. Her understanding was the same as his.
- Peter finds it hard to work with people he no longer respects because of what he now believes about their ethics and behaviour. He still hopes to become an indeterminate employee one day.

Questions

- What CSEC value(s) are involved in this situation?
  - ***Integrity***, ***Professionalism***, and potentially ***Lawfulness***

- What could Peter do in this situation?
  - Contact DGAEE.

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Case #6 – Will you Support the SPCA?

Scenario

Nancy is a real dog lover. She also strongly believes in the value of dog shelters such as the SPCA (Society for the Prevention of Cruelty to Animals). Nancy has decided to help the SPCA in their fundraising events this year. She therefore takes it upon herself to personally canvass all of her co-workers for a monetary donation.

Question

- What should Nancy consider as key elements before deciding to canvass her team mates?

Case #6 – Will you Support the SPCA?

Scenario

Nancy is a real dog lover. She also strongly believes in the value of dog shelters such as the SPCA (Society for the Prevention of Cruelty to Animals). Nancy has decided to help the SPCA in their fundraising events this year. She therefore takes it upon herself to personally canvass all of her co-workers for a monetary donation.

Question

- What should Nancy consider as key elements before deciding to canvass her team mates?

Suggested Responses

- Require prior authorization from the CCSE to solicit donations, prizes or contributions in kind from organizations/individuals other than those specified. Only 3 approved by Government of Canada (GCWCC-United Way, Blood Donor, and Poppy – Remembrance Day).
- You can sell/advertise/solicit voluntary purchases/contributions by posting on bulletin boards (not intranet). You will also find that individuals also post in lunch rooms to sell things or to raise funds for charities/children's group activities. Direct solicitation should not be taking place.
- You are not permitted to use CSEC equipment.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Other Discussion/Questions

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Case #1 - Roll-Up The Rim (and Win?)

Scenario

You enter Tim Hortons with a friend during its periodic contest. You both get a coffee and she pays for yours. When you finish your coffee and roll up the rim, you find that the cup qualifies to win a vehicle.

Question: What would you do?

Note: *This is a hypothetical situation for discussion and illustrative purposes only.*

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

Case #2 – What's Your Problem?

Scenario

- Jean is a new CSEC employee in the SIGINT business line.
- He is given an operational procedure, OPS-1-X. As he reads it, it seems to require doing something inconsistent with an objective of OPS-1 in that it would negatively impact the privacy of Canadians without an operational benefit.
- He discusses his conclusion with a few other colleagues. They don't seem concerned about his point and suggest that he is making too much of it because what is described is how this has been done for several years.
- None of the proposed explanations specifically address Jean's concern; he remains confused and troubled.

Question: What should Jean do in this situation?

Note: *This is a hypothetical situation for discussion and illustrative purposes only.*

Canada

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

Case #3 – It's Tax Season…

Scenario

- Charles likes to keep busy in the evenings and earn extra income.
- Charles has therefore decided to do income tax reports for clients.
- His job at CSEC is in the finance department (contract & procurement).
- Charles has exhausted his list of friends and family members to whom he can offer his services.
- He decides that he'll offer income tax filling services to the consultants that CSEC will be hiring in the months to come, as their files come to his desk.

Questions

- What should Charles consider as key elements when making his decision to promote his services?
- What should Charles do in this situation?

Note: *This is a hypothetical situation for discussion and illustrative purposes only.*

Canada

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

Case #4 – Choices?

Scenario

- Mary is a new employee at CSEC in an IT Security section that evaluates IT products for Government of Canada use.
- She wants to be professional and complete in the advice she gives because she believes in "anticipating, understanding and responding appropriately to client needs."
- She is aware of a potential concern with one of the products that a client department might use for a system as a result of a classified briefing she received during a visit to an allied counterpart of CSEC.
- The *Security of Information Act* defines the information she has as "special operational information".
- No one she is dealing with in the client department has the appropriate clearance.

Question: What should Mary do in this situation?

Note: *This is a hypothetical situation for discussion and illustrative purposes only.*

Canada

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

Case #5 – Everybody Does It (? Or !)

Scenario

- Peter is a term CSEC employee in a directorate whose employees frequently travel to conferences to remain current in their field.
- Two senior directorate employees bragged in front of him about how easy it is to generate "entertainment" money on trips by claiming for meals that are actually provided free of charge as part of the conference registration.
- They indicated that the boss was aware of the practice and turned a blind eye to it when signing their claims.
- Peter wasn't sure if he had heard them correctly and spoke with Sally, a co-op student, who was also in the office at the time. Her understanding was the same as his.
- Peter finds it hard to work with people he no longer respects because of what he now believes about their ethics and behaviour. He still hopes to become an indeterminate employee one day.

Questions

- What CSEC value(s) are involved in this situation?
- What could Peter do in this situation?

Note: *This is a hypothetical situation for discussion and illustrative purposes only.*

Canada

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

Case #6 – Will you Support the SPCA?

Scenario

- Nancy is a real dog lover.
- She also strongly believes in the value of dog shelters such as the SPCA (Society for the Prevention of Cruelty to Animals).
- Nancy has decided to help the SPCA in their fundraising events this year.
- She therefore takes it upon herself to personally canvass all of her co-workers for a monetary donation.

Questions

- What should Nancy consider as key elements before deciding to canvass her team mates?

Note: *This is a hypothetical situation for discussion and illustrative purposes only.*

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

EMPLOYEE RESPONSIBILTIES

- Complete a *Confidential Report* to identify outside interests
- Represent CSEC Ethically
- Resolve conflict in favour of public interest
- Decline gifts, benefits and/or hospitality
- Avoid dealings that could result in preferential treatment
- Safeguard information obtained through official business and not use this information for personal gain
- Use government property only for officially approved activities

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Wrap Up

Canada

Office of the
Communications Security
Establishment Commissioner

Bureau du
commissaire du Centre de la
sécurité des télécommunications

CSE Commissioner

Presentation to new CSEC employees – Foundational Learning Curriculum
June 19, 2012

Darryl Sitka, Director of Operations, OCSEC
www.ocsec-bccst.gc.ca

UNCLASSIFIED

Mandate of Commissioner

- Duties under *National Defence Act*:
  - reviewing CSEC activities;
  - conducting investigations in response to complaints about CSEC; and
  - informing Minister of National Defence
- Supported by powers under *Inquiries Act*
- Also mandate under *Security of Information Act* relating to special operational information of CSEC

Reviewing CSEC Activities

Purpose of Commissioner's review mandate is to ensure:

- activities conducted by CSEC under ministerial authorization are, in fact, those authorized by Minister;
- CSEC complies with the law and if Commissioner believes it may not be complying, to report this to the Minister and Attorney General;
- CSEC does not direct its SIGINT and IT security activities at Canadians; and
- CSEC develops and effectively applies satisfactory measures to protect privacy of Canadians in all activities it undertakes

Reviews – What to Expect

- Assessment of CSEC activities for compliance with legal requirements, ministerial requirements, and policies and procedures (review criteria)
- Reports document CSEC's activities and practices and contain findings about review criteria
- Review is of ex-post activities, but includes ex-ante reasons
- Examination of hard-copy and electronic information, interviews and observation of managers and analysts conducting activities, test contents of systems and databases

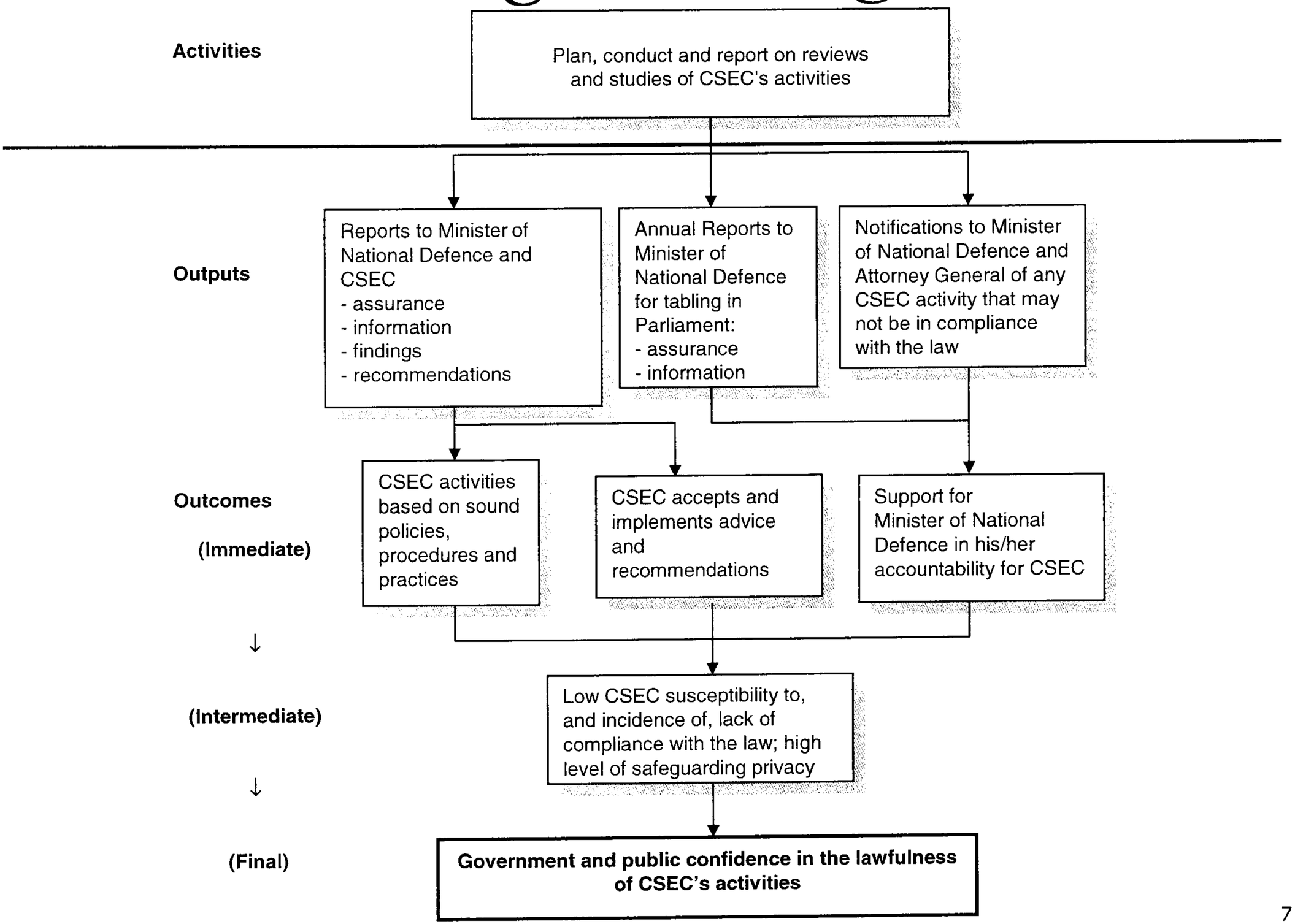
Recommendations

- Commissioner may make recommendations to Minister aimed at correcting discrepancies between CSEC's activities and expectations established by review criteria
- Since 1997, 68 classified review reports containing 133 recommendations – CSEC implemented or working to address 93 percent (124 out of 133)

Shared Objective:

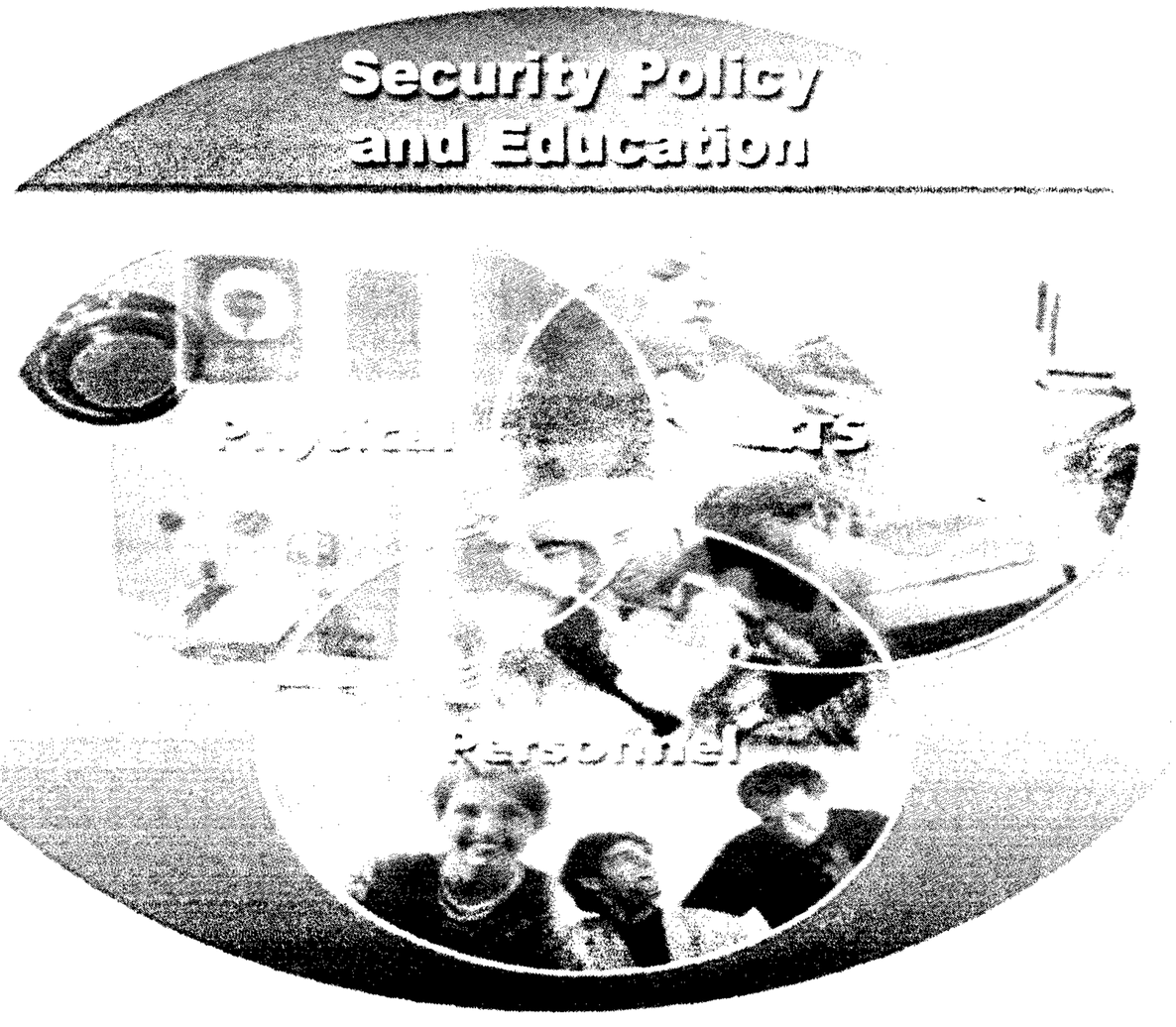
- Strengthen CSEC practices that contribute to compliance and incorporate measures to protect the privacy of Canadians

Review Program – Logic Model



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Physical Security Services



Corporate Security Directorate

Direction de la sécurité interne

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Agenda

- Building Passes
- Building Access
- Room Access
- Random Inspection
- Visitors
- Sensitivity of Information
- Caveats
- Movement of Sensitive Assets
- Security Containers
- Information Storage
- Secure Disposal of Sensitive Information
- Workspace Security
- Media Requests/Questions

Building Passes

- Must wear your photo badge between your shoulder and waist – do not conceal

- Wear your pass at work only

Building Passes

Advise CSEC commissionaires and contact ID Pass Control by:

- Completing (EXPLANATION OF LOSS OF CSEC IDENTIFICATION CARD/BUILDING PASS) Cerrid number 629549
- Loss of ID form
    - Send form to ID pass control
    - 3-day wait before card replacement
    - Show picture ID, sign in
    - Visitor pass
    - No pin or swipe
    - Forgot picture ID??
    - Your supervisor must identify you

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

Building Passes

Guide to CSEC Building Passes (Badges) (Annex to SEC-301)	
Badge	**Interpretation**
	• Photo badges (issued only if access is required more than 10 days per month)*

Building Access

- Controlled 24/7 by guard staff
    - CORE hours (06:00 – 18:00)
    - Non-core hours (18:00 – 06:00)
- After Hours
    - report to guard post upon arrival – they are aware of who is on site in case of emerg
    - Annex [redacted] and CPP – call ahead is required at [redacted] (guard availability to open building)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Room Access

- Responsibility - GSA (Group Security Administrator)
- Only the GSA may make a request to ID Pass Control

Random Inspection

- Random Inspection Authorities:
    - Defence Controlled Access Area Regulations (DCAARs)
    - Inspection and Search Defence Regulations (ISDRs)
- Policy Sec-303
    - Performed by security staff
    - Inspection of bags, purses, back packs, briefcases etc…
    - Display contents
    - Verification for electronics and properly secured sensitive assets
    - Violations recorded - sent to your GSO for follow up

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

Visitors

- All CSEC sponsor must complete CSEC Visitor Access Notification (CVAN)

- You may also modify or cancel these requests on line

- Visitors must have ***work-related*** requirements or participating in a CSEC sanctioned event

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

Visitors

- Last minute visits
  - Prepare a Request for Access of a Visitor (RFAV) form
  - [redacted] visitor must be escorted at all times
- Each employee must escort their guests
- If you see a guest with no escort – take charge – escort the guest to the Commissionaire's desk

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Sensitivity of Information

- CSEC is subject to the Policy on Government Security (July 2009) set by the Treasury Board:
  - Types of sensitivity levels
    - Protected Information (information of a personal or organizational interest)
    - A, B, C
  - Classified Information (National Interest)
    - Confidential, Secret, Top Secret
    - Injury, serious injury, grave injury

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Caveats

- Added security markings to a document's classification
- These additional measures establish the level of need-to-know
  - i.e. CEO (Canadian Eyes only)
    CSEC Official Use Only

Movement of Sensitive Assets

- CSEC Confederation Heights Campus includes:
  - SLT, EDB, IB, CPP and the Annexes
  - LTA/POD 1 are NOT part of the Confederation Heights Campus (asset movement receipt required
- Procedure:
  - Receipt requested by employee via intranet
  - Kept with CSEC [redacted] and sensitive information
  - Employees must not take classified or protected material home
  - Directors receive their group's report at the end of each month

s.15(1)

s.16(2)(c)

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

Security Containers

- [redacted]
- [redacted]
- All secure items MUST remain in your possession at *all times*
- *Report any loss immediately*
- Handle and store all sensitive documents as per the "**SEC-103: "Annex 2 - CSEC Document Handling Guide"**

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Storage

- SLT -
- EDB -
- IB, CPP, Annex E & F -
-
- LTA/POD 1 –

Information Storage

- Classified or protected documents must be covered or hidden from view when an uncleared visitor is present.

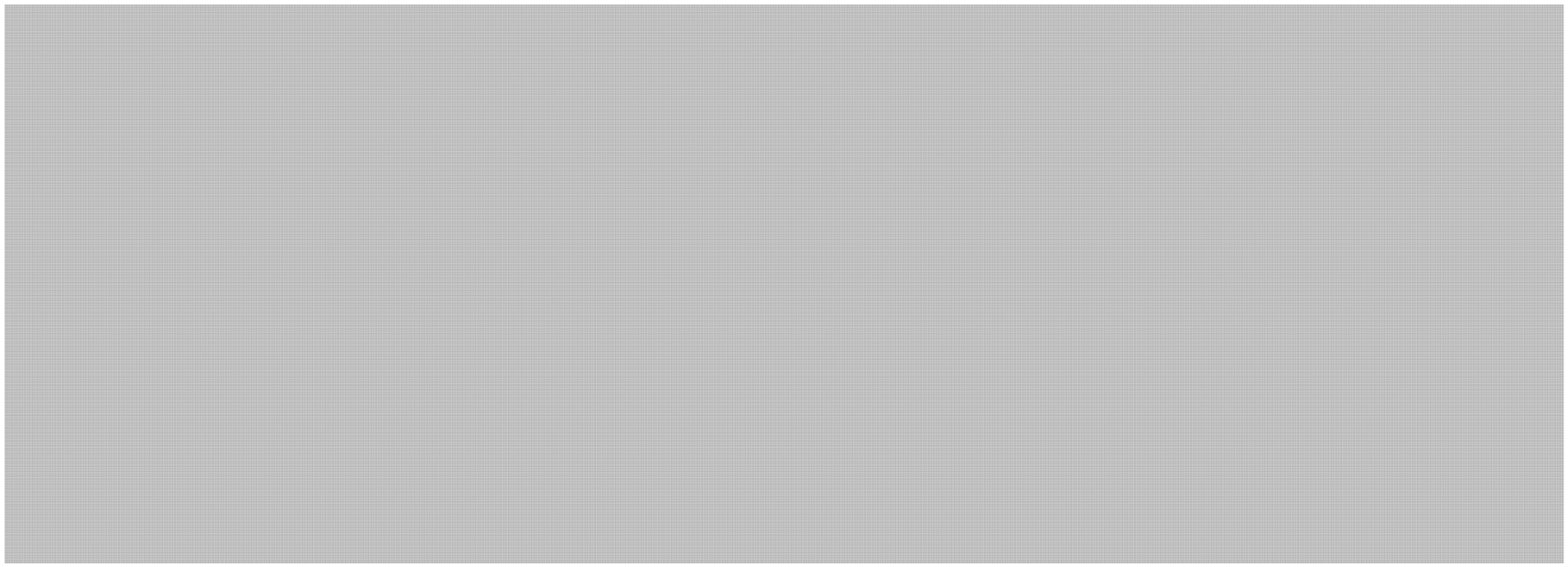
- Use appropriate secure containers to store protected or classified information

- Workstation drawers/overhead compartments – no storage of protected or classified information

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

Secure Disposal of Sensitive Information

- Disposing of unclassified, *protected* and/or *classified* information



Workspace Security

- Offices must be closed when left vacant

- If door not armed – guards have the responsibility to enter, verify for sensitive information left unsecured, leave violation notice

- When away from your workstation for an extended period display the

yellow warning sign

- Do not have classified discussions in the hallway, cafeteria, shuttle, washrooms or any other common area

Workspace Security (cont'd)

- Last person to leave complete a sweep of the office area to ensure:
  - Sensitive material is secured (as per building requirements)
  - Cabinets are locked (as per building requirements)
  - Electrical appliances are turned off
  - Doors and windows are closed and properly secured
  - Security alarm is activated

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

Workspace Security (Cont'd)

[redacted]

WHY?

s.15(1)

s.16(2)(c)

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

[redacted]

s.15(1)

s.16(2)(c)

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

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

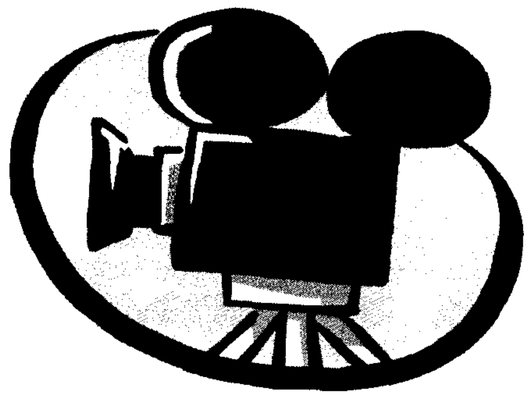
Media Requests/Questions

- Refer all questions from the news media or general queries to the CSEC Public Affairs Office

- Do not give out personal information or phone numbers to callers

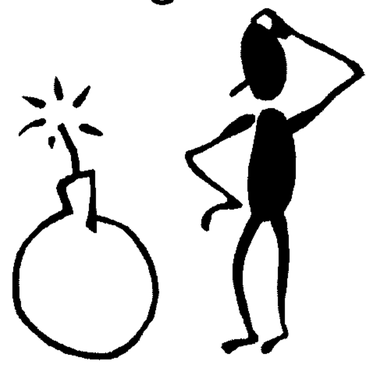
- Offer to relay a message

- Do not confirm or deny any information



Reminders

- Report any suspicious or unattended packages on CSEC grounds to Security via phone or [redacted]
- Bomb threat/911 – What to do?? Read the emergency guide.



- Report any strange behavior (for example) to Security via phone or [redacted]
  - Someone taking pictures of employees, vehicles at work
  - A car circling the parking area regularly
  - A co-worker behaving differently

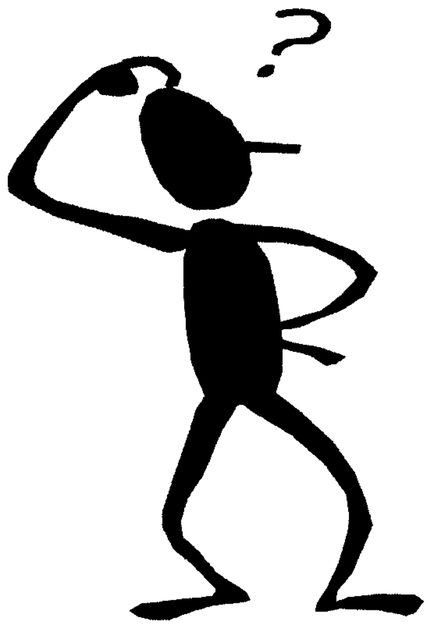
Final Thoughts

- Security is everyone's business… Security practitioners give you tools and advice to do your job securely.

- We rely on you to also take security seriously.

- Security is key to our success. It enables us to accomplish our mission.

ANY QUESTIONS?

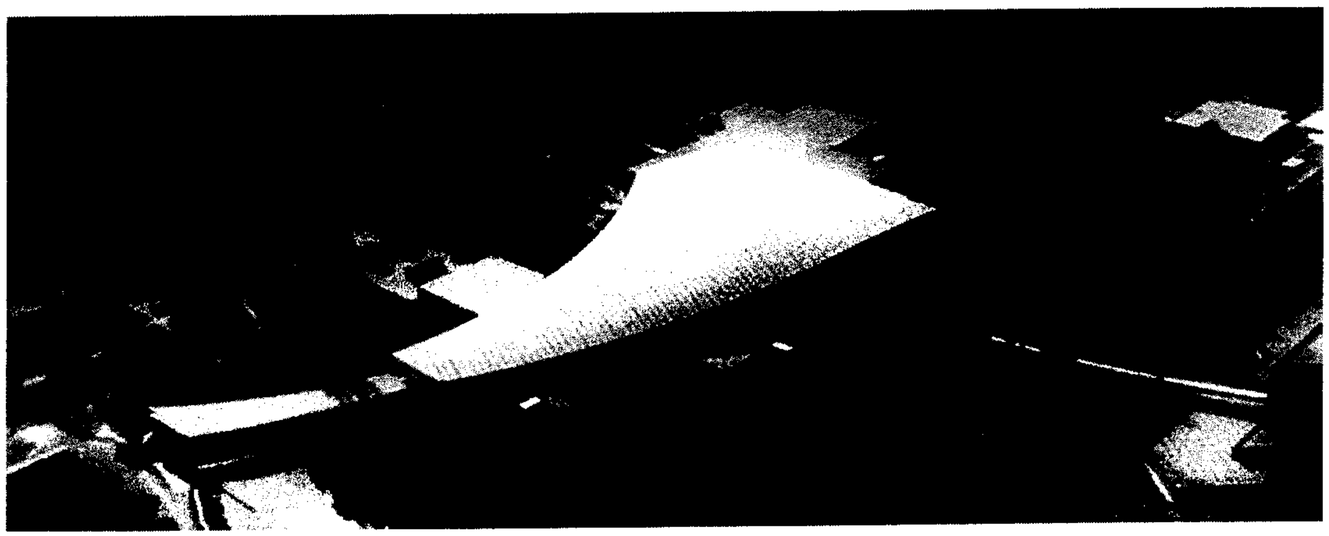


If you have security questions, send an electronic request via: [redacted] under the caption Corporate Security Services

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

THREATS TO CSEC



Corporate Security Directorate

Direction de la sécurité interne

Canada

Objective

- Understanding the threat to CSEC from:
  - Foreign Intelligence Services
  - Those sympathetic to terrorists groups
  - Trusted Insiders
  - Cyber attacks

s.16(2)(c)

s.15(1)

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

TOP SECRET INFORMATION
WITHIN FEDERAL GOVERNMENT

[redacted]

Corporate Security Directorate / Direction de la sécurité interne

Canada

Context

- Since 9/11 we have almost doubled in size and greatly diversified our workforce
- [redacted]
- [redacted]

Threats to CSEC

Threats to CSEC

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

Threats to CSEC

[redacted]

Corporate Security Directorate / Direction de la sécurité interne

Canada

s.15(1)

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

[redacted]

[redacted]

Threat to CSEC

[redacted]

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

[redacted]

s.15(1)

s.16(2)(c)

s.15(1)

s.16(2)(c)

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

Threat to CSEC

[redacted]

Corporate Security Directorate / Direction de la sécurité interne

Canada

Threat to CSEC

[redacted]

[redacted] Threat to CSEC

[redacted]

s.15(1)

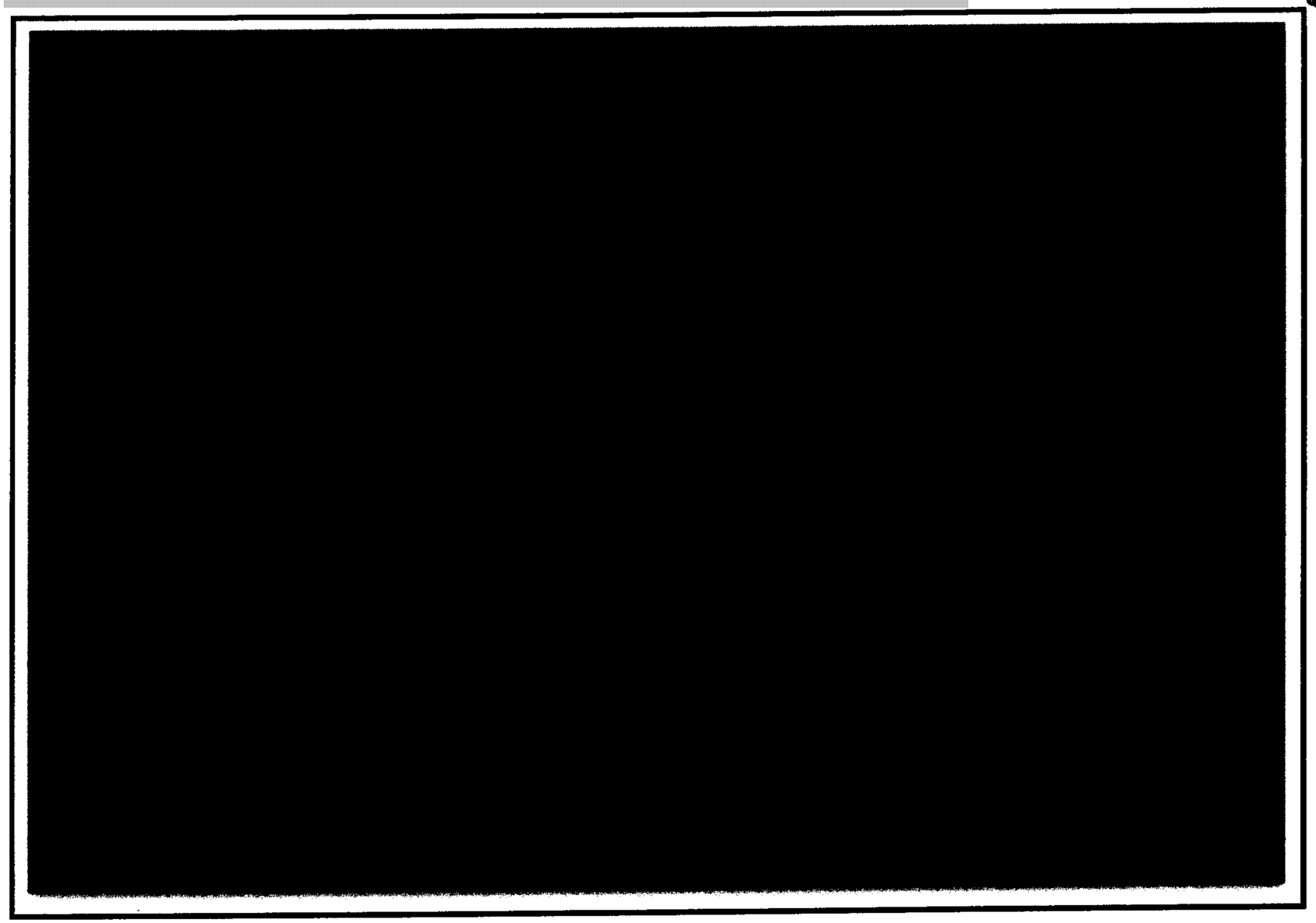
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

[redacted] Threat to CSEC

[redacted]

Corporate Security Directorate / Direction de la sécurité interne

Canada



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

s.15(1)

Russians seeking secrets in spy case

Sub-Lt. Jeffrey Paul Delisle, 40, faces two charges of violating the Security of Information Act and one Criminal Code charge of breach of trust by a public officer.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

At the Halifax Naval Base

Position afforded access to sensitive information

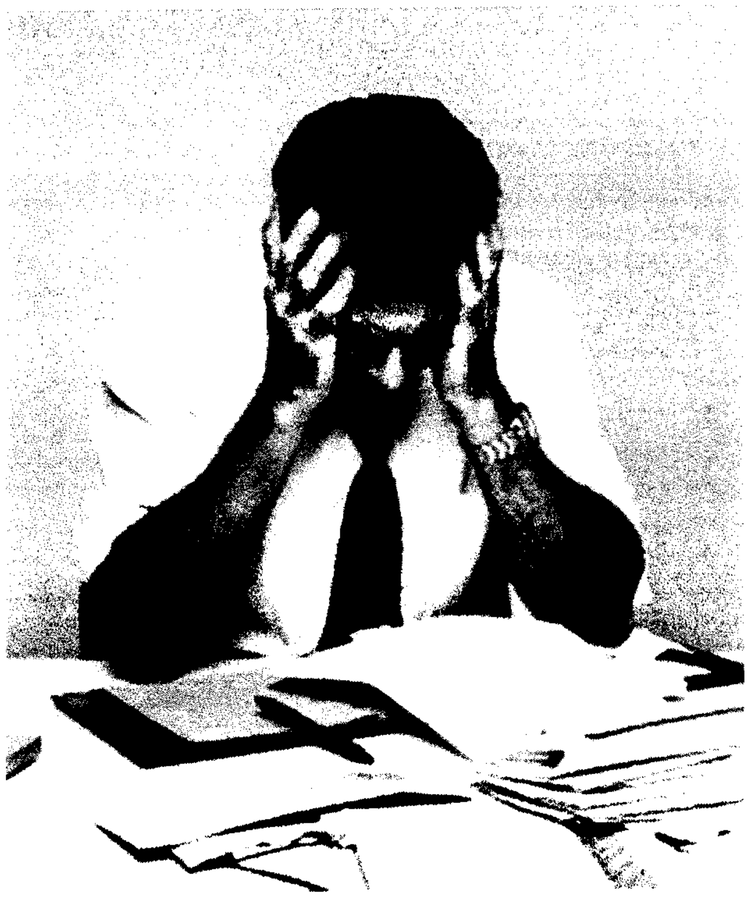
Corporate Security Directorate / Direction de la sécurité interne

Canada

Marriage and money problems

1997: Marries

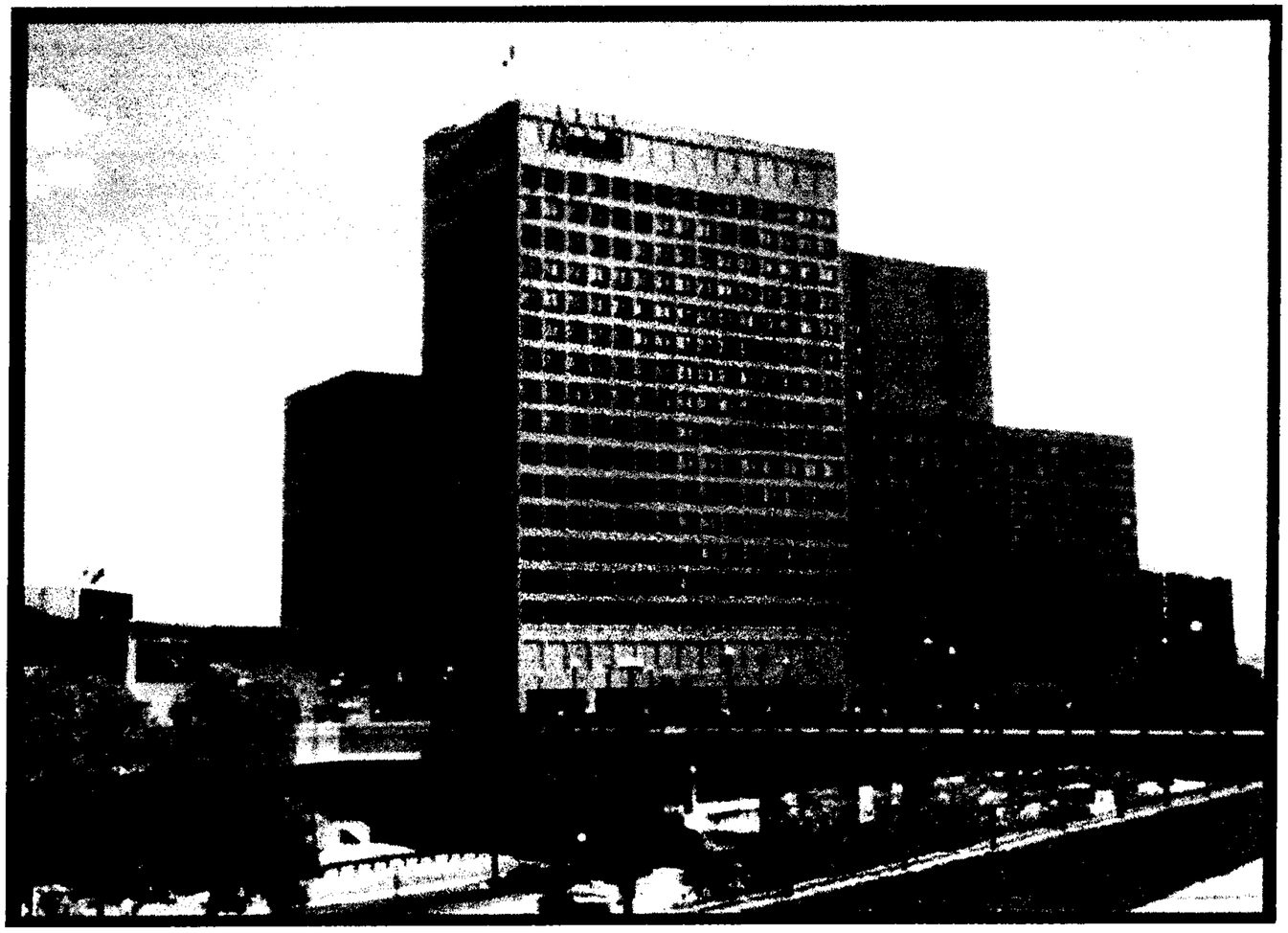
1998: Files for bankruptcy



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Transfer to Ottawa

Worked in the Chief of Defence Intelligence Office



Corporate Security Directorate / Direction de la sécurité interne

Canada

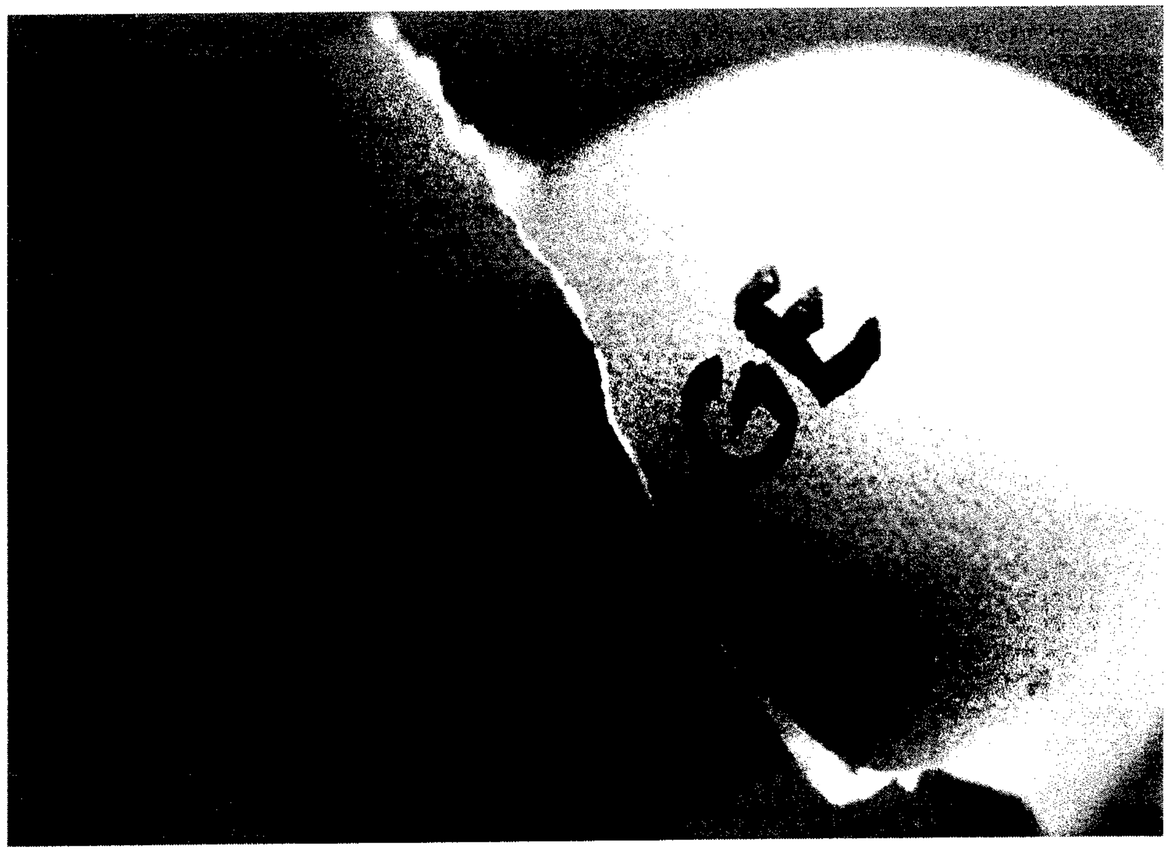
Personal life …

July 6, 2007

Accused spy Jeffrey Delisle's personal life 'fell apart' around time of alleged crimes

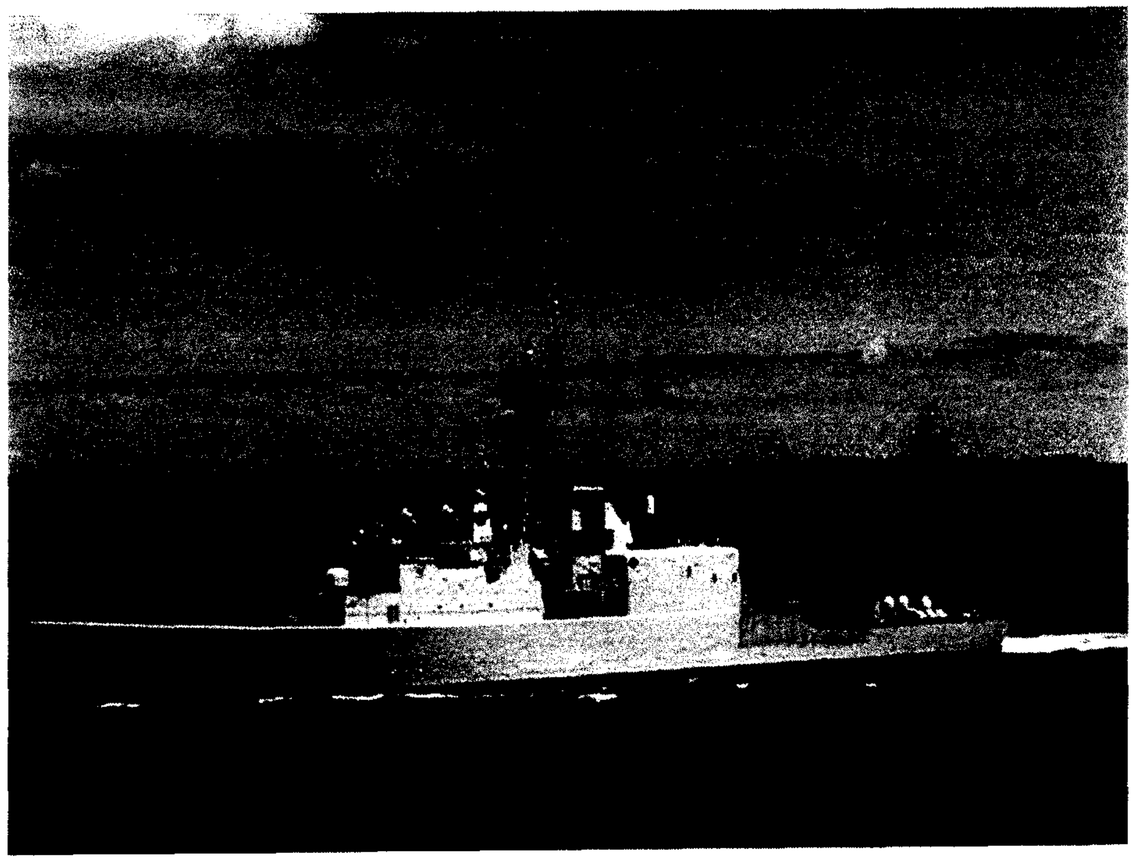
More debts …

Legal separation agreement stipulates that Delisle assumes the couple's debts



Back to Nova Scotia …

Delisle joins HMCS Trinity, an intelligence facility at the naval dockyard in Halifax



Arrest by the RCMP

Delisle is led out of a Halifax court on Jan 16

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

[redacted]

s.15(1)

s.16(2)(c)

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

[redacted]

- Employee security awareness

Document Handling

- Classification is critical to safeguarding
- Our "need to know" = problems for you
- Only those cleared with a need may access
- Wikileaks release of US State Department documents is an example of [redacted]

Lessons Learned

- Still a very hostile environment
- Business as usual for traditional and non-traditional adversaries
- Although the world is changing, trusted tradecraft remains successful
- Need to maintain and use good security measures

What Can You Do?

CALL US:

- When you encounter unusual situations.
- Someone shows undue interest in your job.
- Contact with foreign nationals;
  - Visits to Embassies

QUESTIONS

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

PERSONNEL SECURITY

Corporate Security Directorate

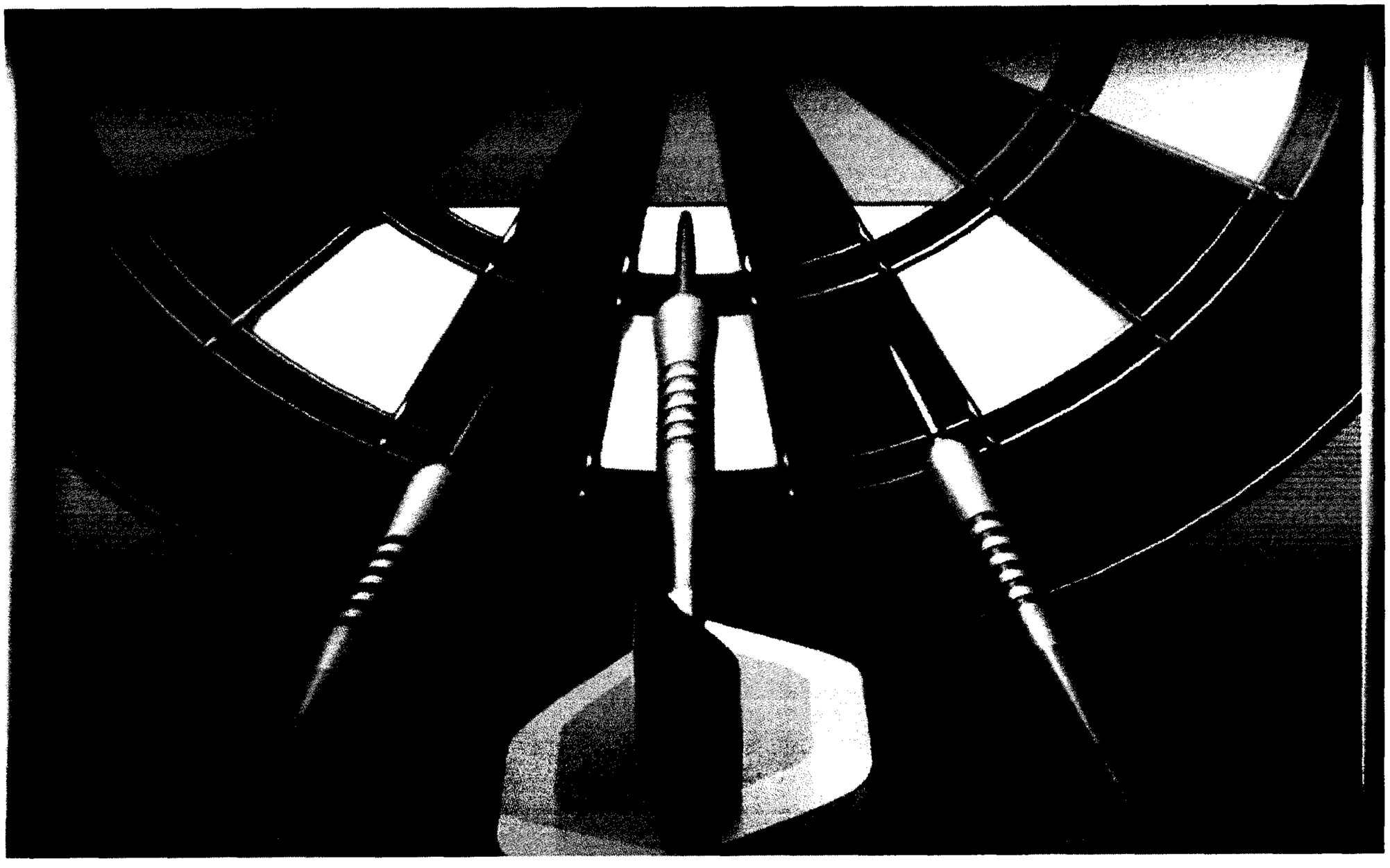
Direction de la sécurité interne

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Why is CSEC a target?



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Disclosure of Employment (SEC–205)

Where do you work?

- Limit the knowledge to those who truly have a "need to know"
- Ask family and close friends to say you work for the [redacted]

What do you do?

- Generic job titles
- Unclassified description

What is CSEC?

www.cse-cst.gc.ca

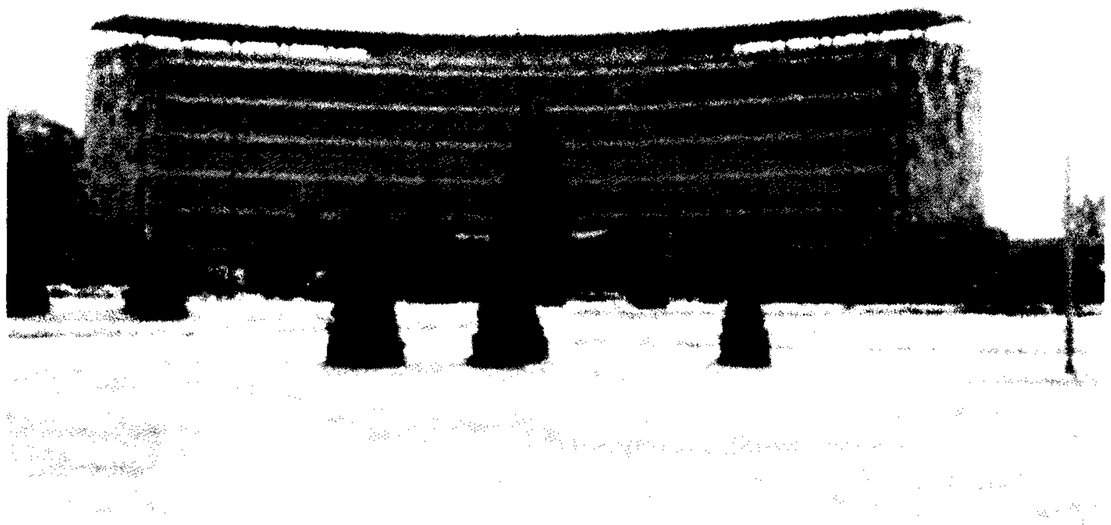
Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Discretion – It matters !

- **Be discreet both at home and at work**



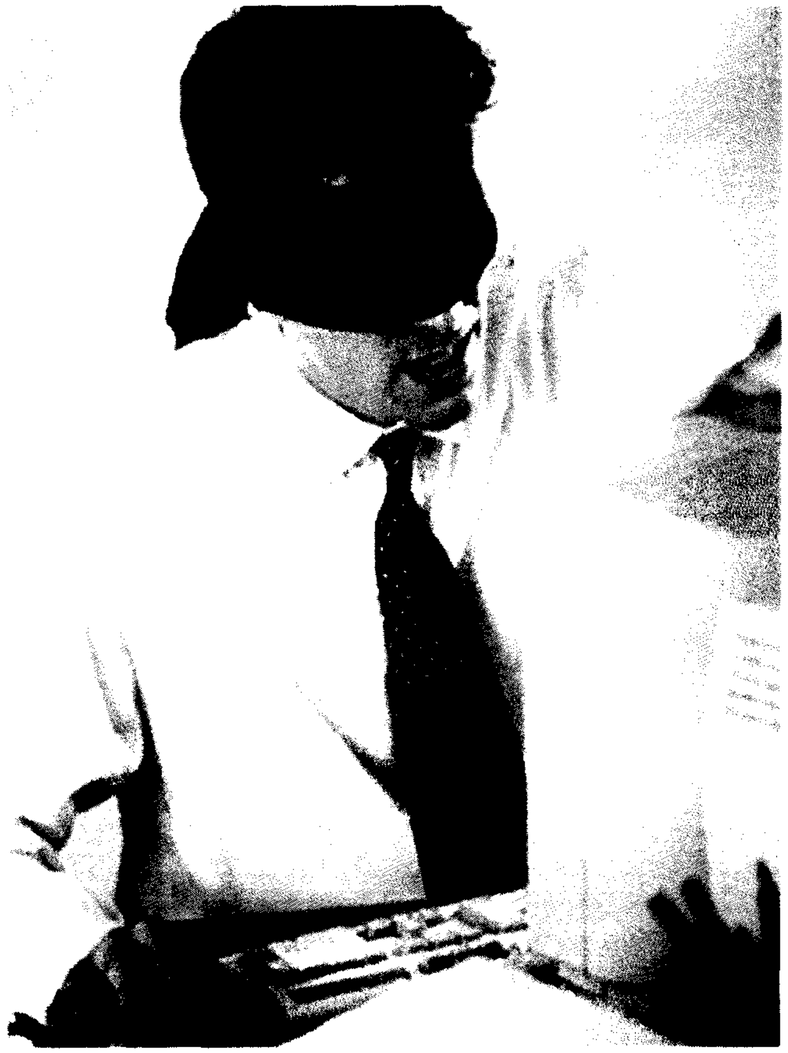
Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Need to know principle is key

- **Appropriate Clearance Level ?**
- **Need for the information**
- **Unauthorized Exposure to Compartment Intelligence (SEC 203) must be reported to your Group Security Officer …**



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Security Awareness

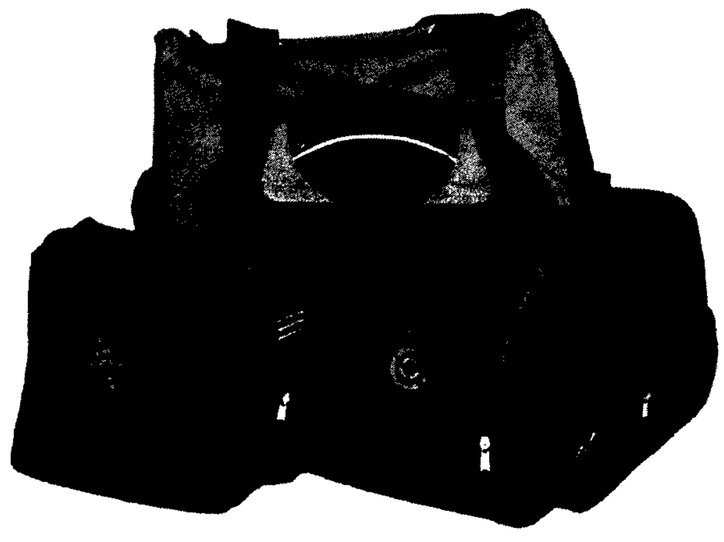
Amazing mind reader …?

nd reader reveals h

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

SEC–205 Disclosure of Employment 4.11 – Displaying logos, Awards, etc.

- Exercise caution and judgement about where and to whom you display items bearing these artistic identifications.
- Do not wear clothing or bring items visually associated with CSEC or the intelligence community with you when on personal travel abroad.



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Public Affairs and Communications Services (PACS)

- No Comment

- All inquiries about CSEC from the media should be directed to Public Affairs and Communications Services (PACS)

(613) 991-7248

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Suspicious Phone Calls

- 2011 – employees receiving phone calls at work and at home regarding [redacted]

- 2008 - CSEC employees receiving suspicious telephone calls at work from unidentified individuals [redacted]

- [redacted]: Service request "ticket" via "Service Desk" link on CSEC intranet page

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Travel

- **One-Stop Travel Request Page see CSEC intranet**
- **Lessen the risk to personnel, information and assets**
- **Condition of employment**
  (Letter of offer)
- **Travel restrictions**

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

SEC-204 Security and Foreign Travel

- **Register all <u>personal foreign travel</u> and <u>conventional foreign business travel</u>**

- **Exception: brief cross-border personal travel to the US (24-48 hours, long weekends)**

- **30 day advance notice**

- **Leave building pass in Canada**

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

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

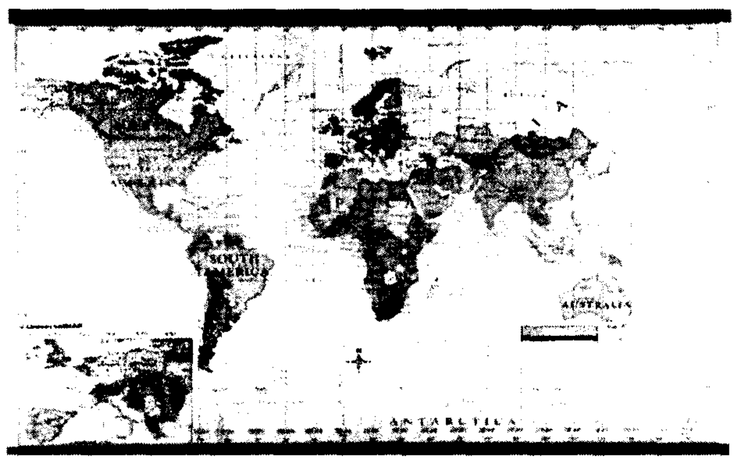
Border Crossings

- A Confirmation of Employment letter from Personnel Security is **not** necessary for Canadian-born employees but is **recommended** for employees on lengthy trips* and foreign-born employees**

- It's OK to state you work for CSEC

- Don't be reluctant to say that you're attending work-related meetings with counterparts at Fort Meade (i.e. NSA)

- Consult your manager or Group Security Officer



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Report Changes in Personal Circumstances

- **Changes to marital status**
- **Common-law, roommates, lodger, live-in nanny**
- **Address / telephone number**
- **Name change**
- **Application for dual citizenship**
  (before you apply)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Be Aware, Be Responsible

Effective Security means:

- **Understanding the threats**
- **Accepting the rationale for the programs and procedures in place to counter these threats**
- **Taking personal responsibility for CSEC Security**
- **Report security related incidences via Service Desk link or contact a guard station**

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

QUESTIONS?

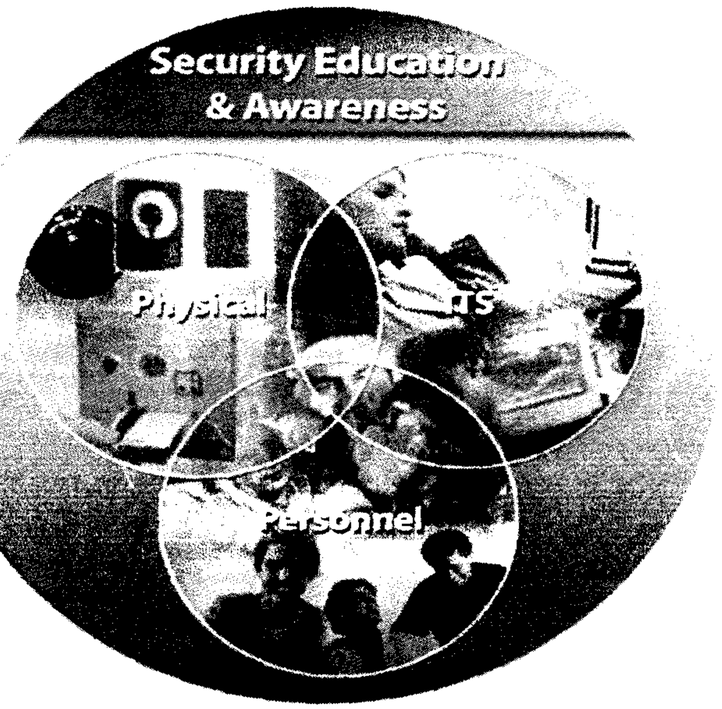
Send a Service Request or "ticket" via Service Desk link

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Corporate IT Security



Corporate Security Directorate

Direction de la sécurité interne

Canada

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

Information Security Threats

- Critical information is the target of cyber related attacks for criminal, political or other motives.

- The large number of potentially ill-intended perpetrators could include individuals acting on their own, hostile intelligence agencies and terrorists.

- Growing range of capabilities and tools, malicious cyber activities.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

How to Protect CSEC

- Follow policies and procedures
- Protect your computer databases and network lines from unauthorised access
- Properly store sensitive information
- Discuss sensitive company matters in secure locations
- Implement controls on employee and visitor access to sensitive facilities, material and so on, based on the “need to know”.
- Use caution when choosing the medium used for business communications
- Educate and sensitize your employees.

s.15(1)

s.16(2)(c)

SECRET

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

The Damage!

[redacted]

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Policies & procedures

- SEC-303 Random Inspection Program - Restricted Items at CSE
- SEC-400 CSEC Electronic Information Security Policy Framework
- SEC-401 Procedures for Portable Information Devices
- SEC-404 CSEC Certification and Accreditation Policy
- CSEC Internet Use Policy
- Government Security Policy (GSP)
- Policy on the Use of Electronic Networks
- OPS-5-1Operational Use of the Internet

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Passwords

s.15(1)

s.16(2)(c)

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

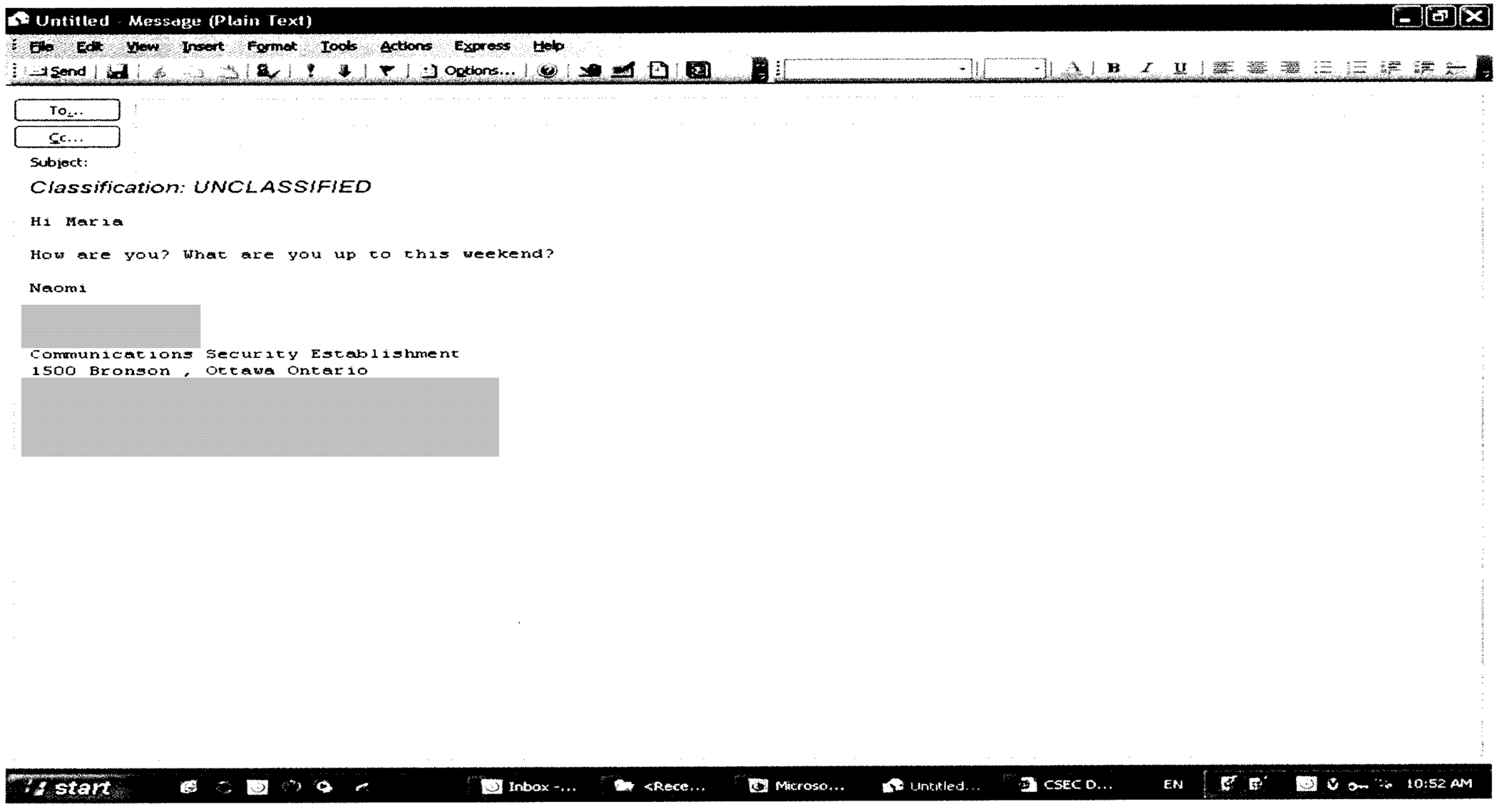
Emails

s.15(1)

s.16(2)(c)

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

Attribution to CSEC



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Things to Watch

- Use the appropriate security markings on your e-mails
- Ensure you have proper and approve encryption (ex. PKI) capabilities before transmitting sensitive information via e-mail
- *Important*: Be careful when using your personal email account on [redacted] attachments have not been screened by our email filter.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Downloads

Downloads

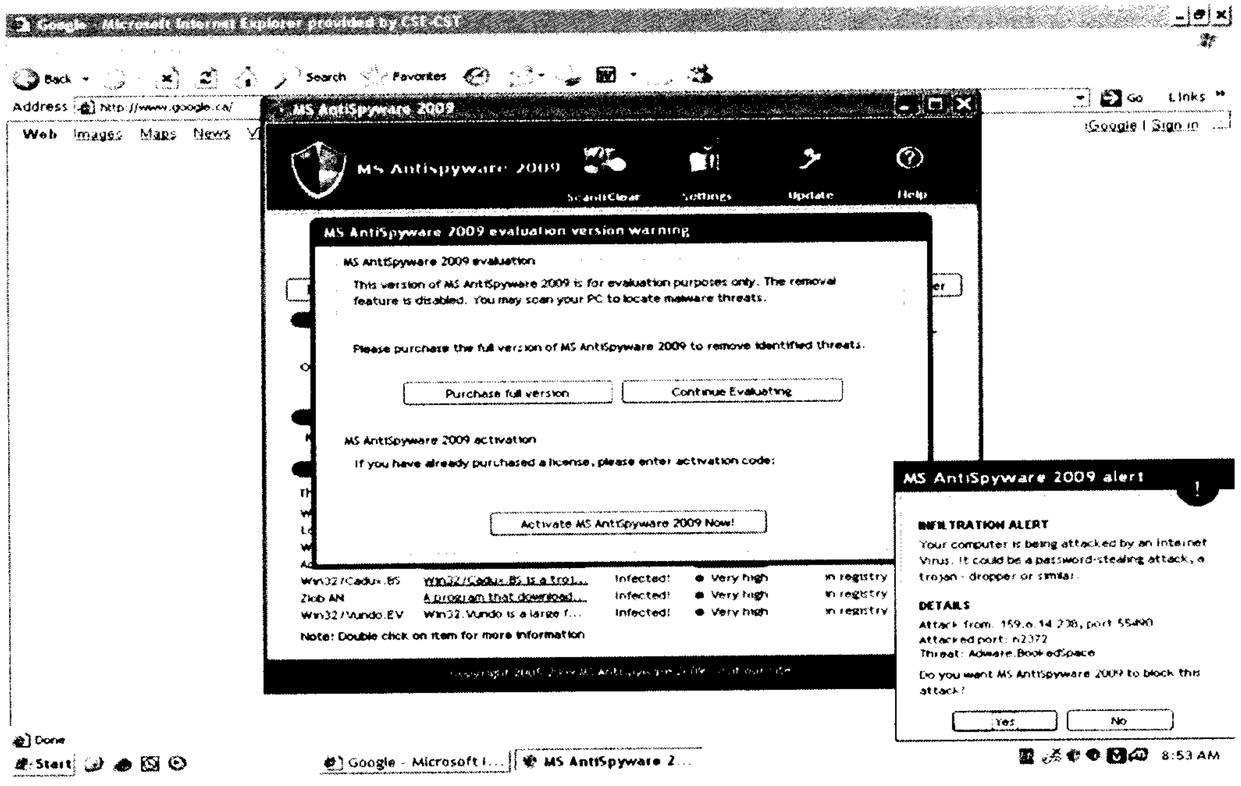
Downloads

- Permitted:
  - Information, such as “White Papers”, product information, etc. in format such as Word or PDF
- Prohibited:
  - Peer-to-peer software,
  - Games, music
  - Any executable

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

Malware

- Intrusion can happen, even at CSEC…
- Ex: SEO Poisoning



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Portable Information Devices

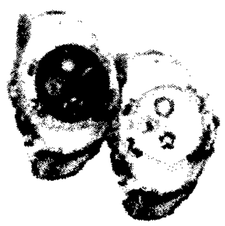
- Any personal device with transmitting, recording or connectivity capability is PROHIBITED on CSEC's campus (ex. Personal cellphones, blackberries, etc.)

- Personal "burned" CDs are not permitted on CSEC premises

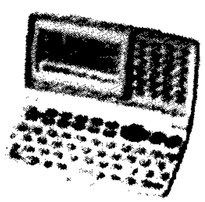
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Restricted Items at CSEC

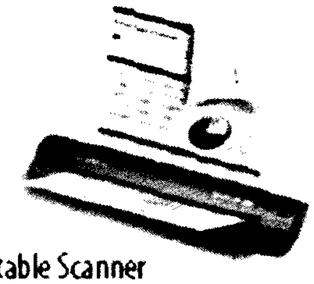
Do you have any recordable media or electronics with you?



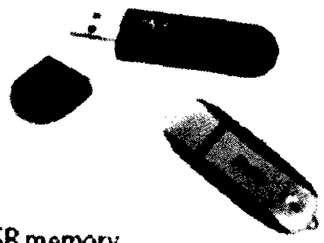
Photo/recordable watch



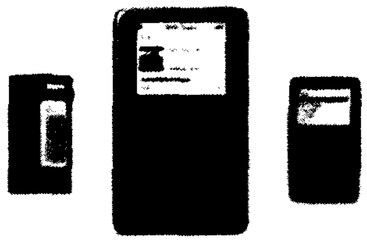
Electronic Agenda



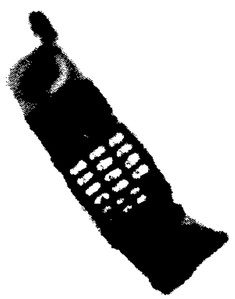
Portable Scanner



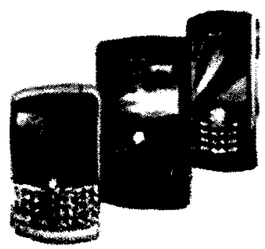
USB memory



Digital music player



Cell Phone



Wireless
Personal Digital Assistant (PDA)

Laptop

Corporate Security Directorate / Direction de la sécurité interne

Canada

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

Blackberry

- CSEC Blackberry

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Internet Use

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

Permitted Non-sensitive Browsing

- CSEC employees may make personal use of corporate internet access for purposes of enhancing their professional growth, general knowledge, and general health and well-being. Ex:
  - Administrative use
  - Product research
  - Global news & events
  - Academic & research institutions
  - Computer trends & technologies

- *Important:* Since it is not possible to use technology to only allow permitted activities. DO NOT ASSUME that an activity is permitted simply because it is not blocked! If in doubt, ASK!

Prohibited Browsing

- [redacted]
- Web surfing of sites that are not directly related to [redacted]
- Any communication of a classified nature.
- Any use in support of any business other than CSEC business, or for personal gain.
- Any use that causes network or system congestion.
- Client-server connections to external services such as real-time chat.

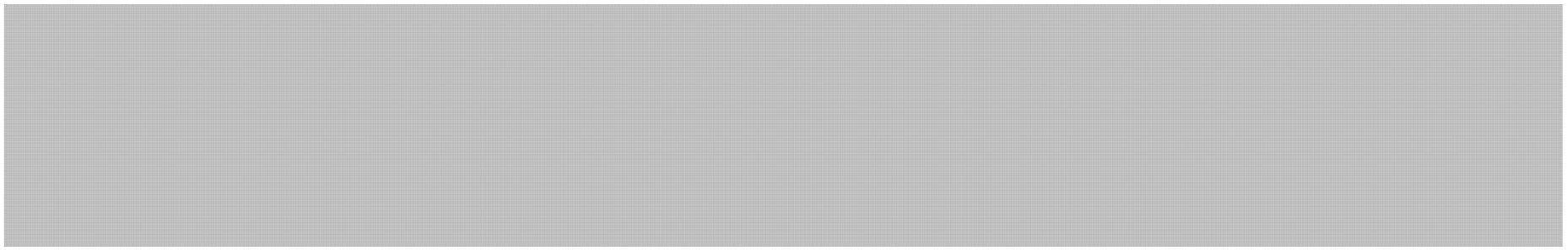
Use of Forums, Blogs and Wikis

- Permitted
  - Participation in web-based discussion groups of personal interest with [redacted]
- Prohibited
  - [redacted]
  - Representation of personal opinion as CSEC position in any forum.

s.15(1)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Internet Use,



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

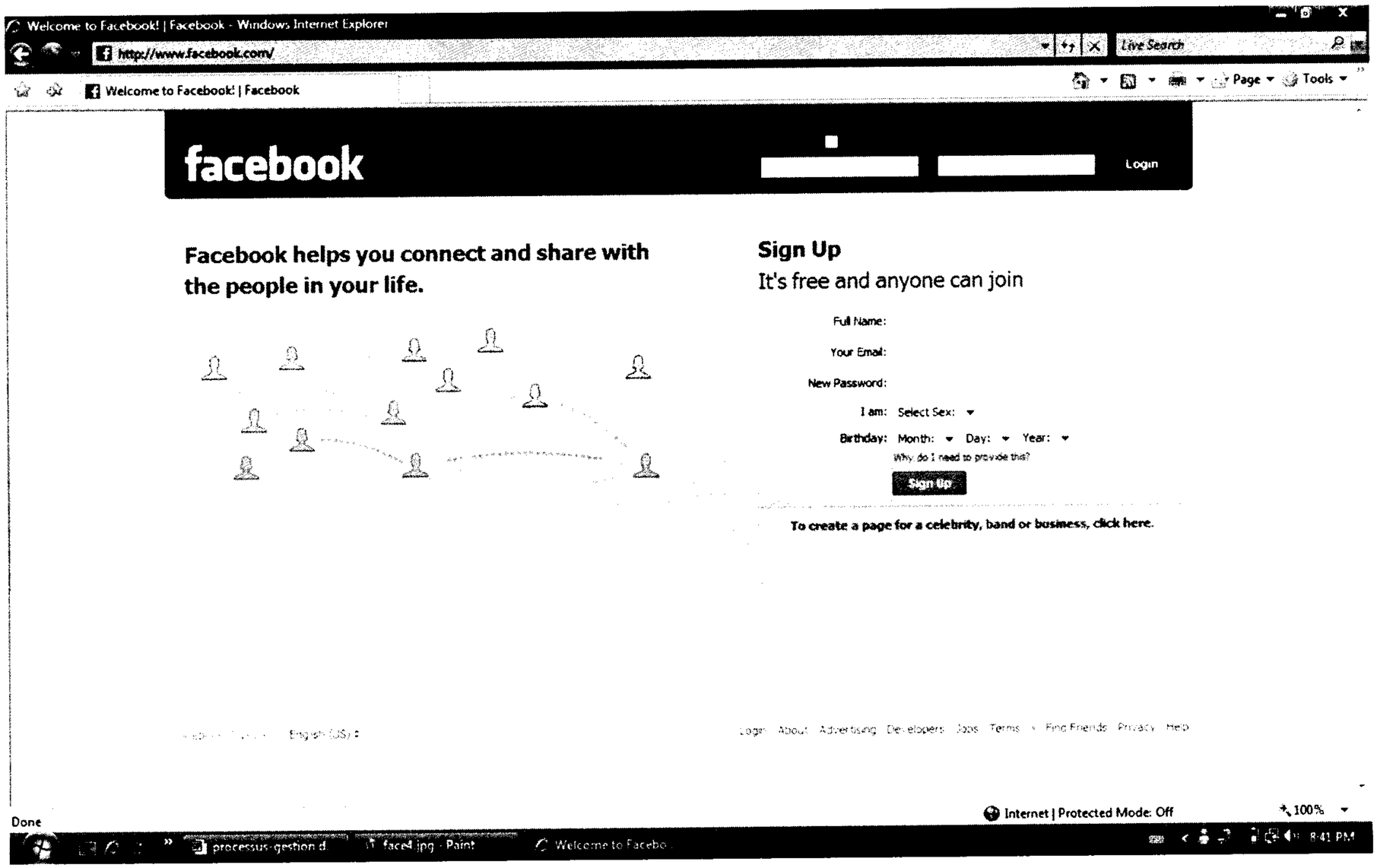
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Server Logs

[redacted]

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

Social Websites



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

Security is Your Responsibility

- If necessary to bring in restricted items - remember to fill out the appropriate forms
- CSEC 's security safeguard resides with each employee and their adherence to the process put in place:
  - Do not compromise IT material
  - Do not put our environment at risk
  - Sign acknowledgment of responsibility
  - Return borrowed material
  - No hand off to another colleague
- Remember CSEC retains the right to confiscate any material when abuse is suspected.

s.15(1)

Report Incidents/Seek Advice ?

- Corporate Security
  - Send a ticket via [redacted]
- IPC-[redacted]
- ISSO-dl
- Your Group Security Officer

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

A chain is as strong as its weakest link

- **Don't be the failing link... Practice and promote good IT security**

  - ☑ **Lock your computer when absent**
  - ☑ **Observe IT security policies, procedures and guidelines**
  - ☑ **Use and protect strong passwords**
  - ☑ **Observe the need-to-know**
  - ☑ **Avoid error --- when in doubt, ask your: Group Security Officer (GSO), Manager, or an IT Security Specialist**

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

Report Incidents/Seek Advice ?

- Corporate Security
  - Send a ticket via ARS
- IPC-[redacted]
- ISSO-dl
- Your Group Security Officer

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Questions?

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Introduction to SIGINT

CSEC Foundational Learning Program

Learning Advisor, [redacted]

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

What We'll Cover

- What is SIGINT and why we do it
- Historical events and what we've learned from them
- A "surprise" group activity
- How SIGINT works and is structured
- A product of SIGINT
- Some cool SIGINT stuff

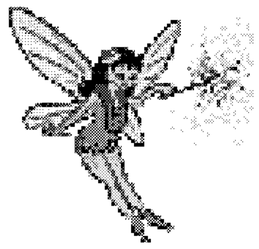
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

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

What is SIGINT?

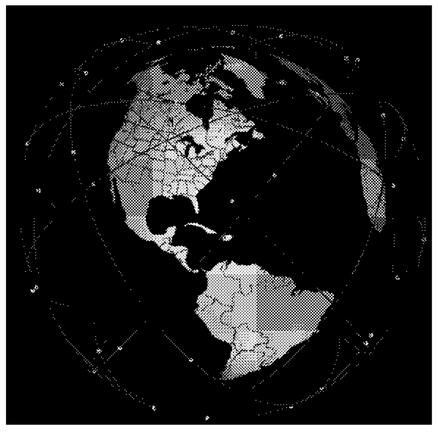
- SIGINT is **NOT** what you see in Hollywood!

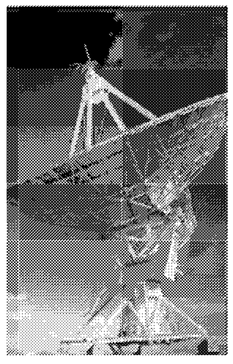
The most famous SIGINTer is the Traffic Fairy

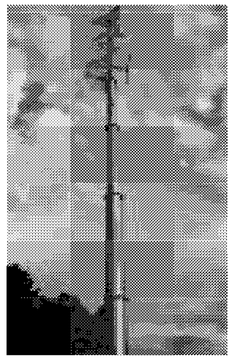


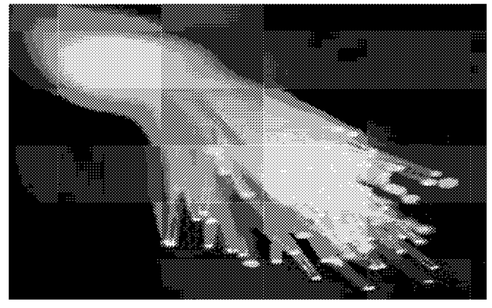
What is SIGINT?

- Intelligence acquired through the collection of electromagnetic signals, including
  - communications i.e. telephony, digital data networks
  - non-communications signals i.e. radars or telemetry









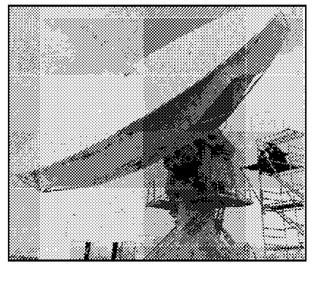
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

SIGINT is a Combination of …

COMINT
Communications Intelligence
• think **Talkers!**

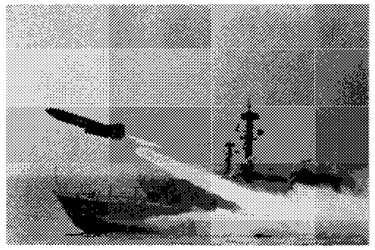
Digital/Analog

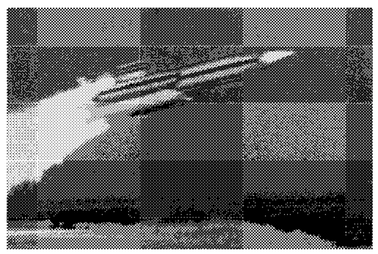
Satellite



FISINT
Foreign Instrumentation
Signals Intelligence
• think **Meter readers/trackers!**

Missile Tests

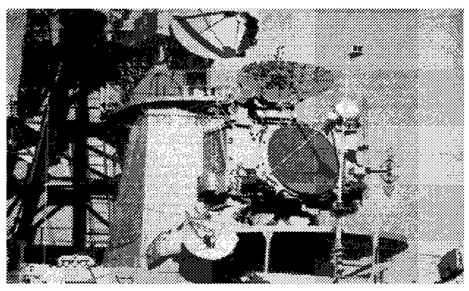




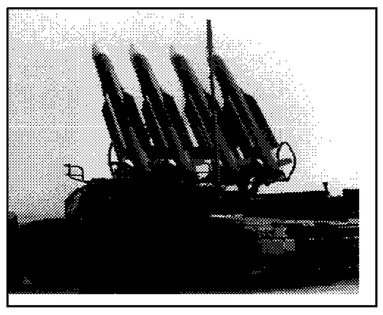
- Data links
- Telemetry
- Beacons

ELINT
Electronic Intelligence
• think **Radars!**

Shipboard Navigational Radar



Fire Control Radar



-
-

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Some ELINT Examples

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

SIGINT is …

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

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

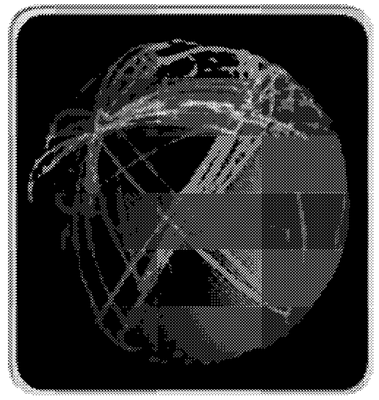
So, Why do SIGINT?

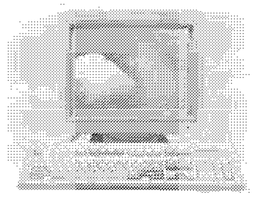
Many Others

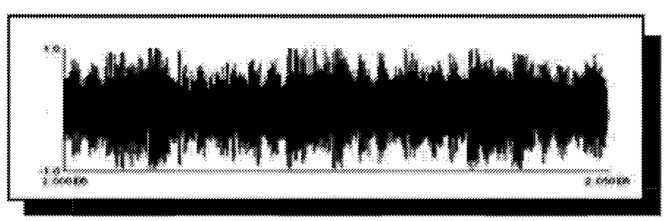
[redacted]

RCMP

PS







[redacted]

CSIS

DFAIT

DND

- Supports Government of Canada decision making
  - In support of the health, safety and the prosperity of Canadians
  - For the betterment of Canada's position on the world stage

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

Brief History: Post-War

- 1945: Igor Gouzenko affair

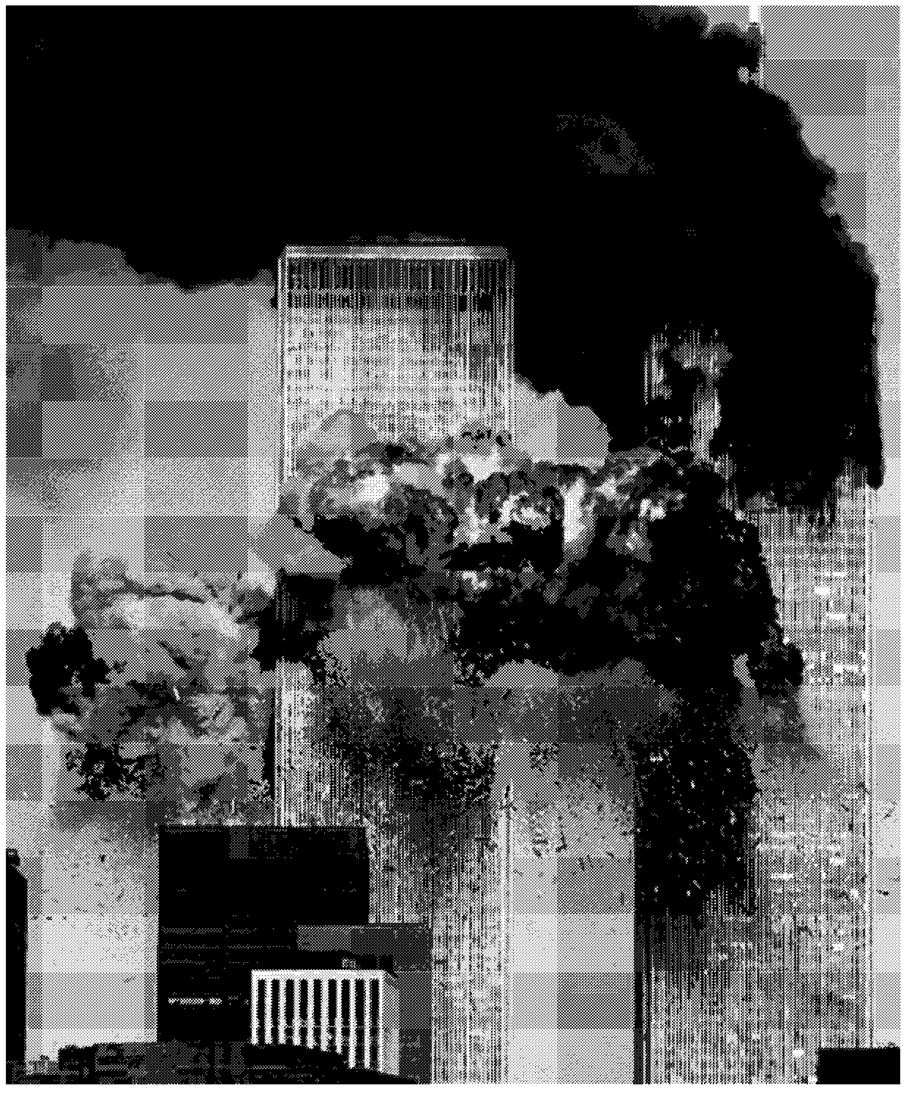
Brief History: Cold War

- 1989: Fall of the Berlin Wall & Soviet Union

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

Brief History: 9/11

- 2001: Aftermath of the 9/11 attacks



Brief History: 7/7

- 2005: July 7 London bombings

What We've Learned From History

- Threats are a constant
- Technology continually changes; we must always keep up with it and readily adapt
- SIGINT has always been critical to meeting GC intelligence requirements supporting GC decision making

How Would You Construct a SIGINT Agency?

Task: Get into groups and through discussion come up with your group's ideal SIGINT agency structure. Be prepared to explain your creation!

<u>Some things to consider:</u>

How would you structure your organization?

How do you decide what to focus on?

What rules are needed?

Who runs the place?

How do you get data; what happens to it?

What organizational structure would you need to analyse/process it?

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

[redacted]

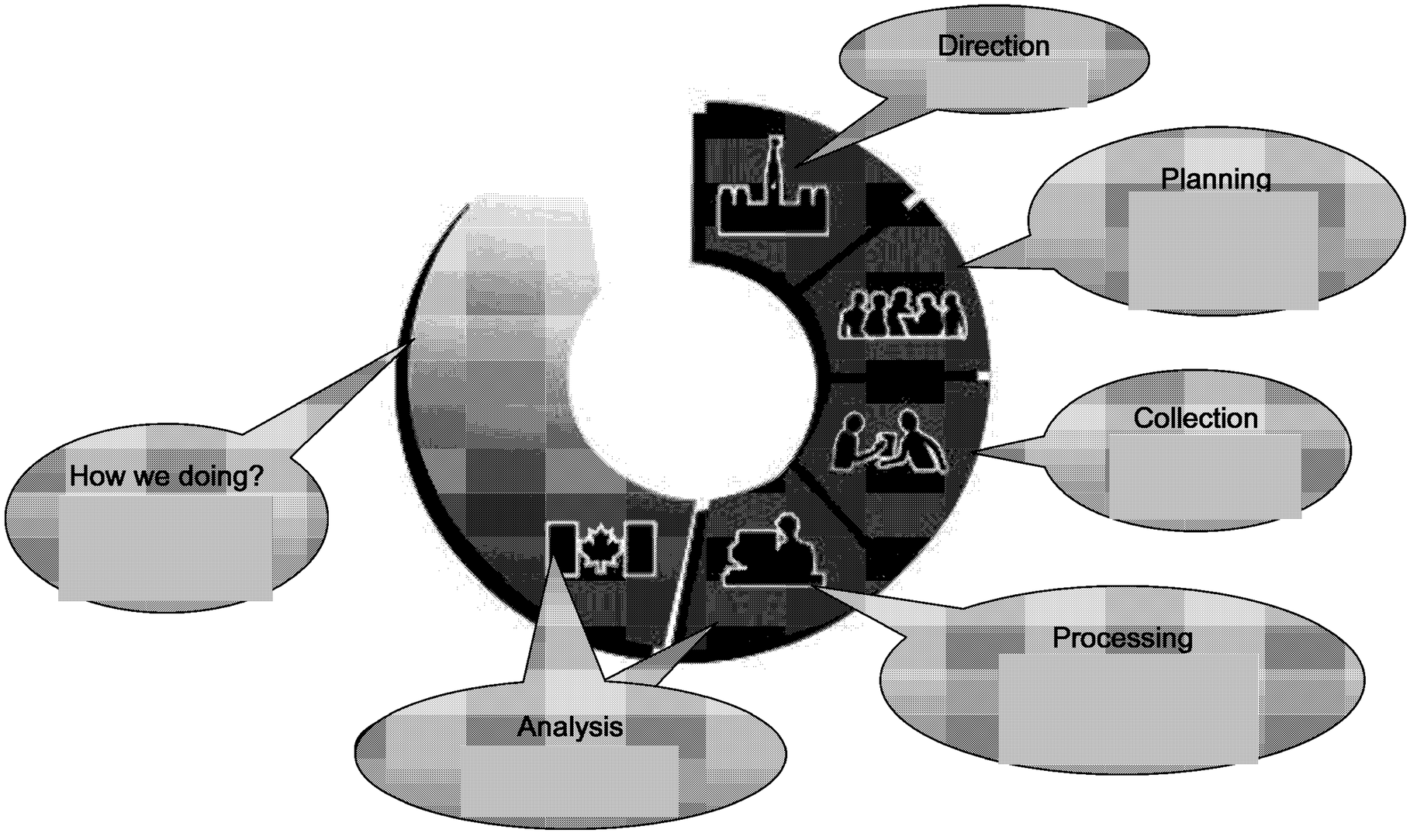
s.15(1)
s.16(2)(c)

SIGINT Requirements

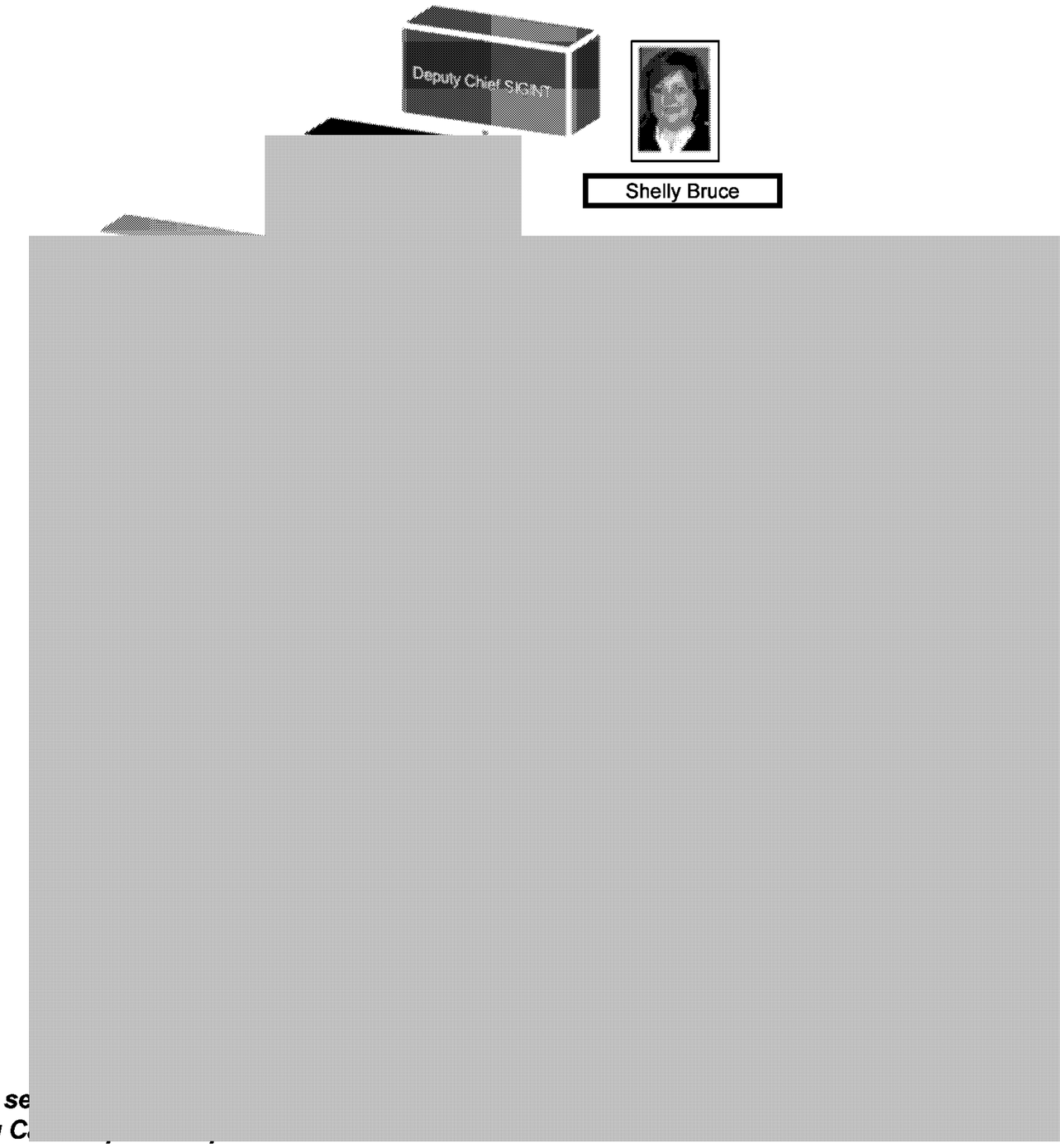
- The **National SIGINT Priorities List** a.k.a. the **"NSPL"**
  - is SIGINT's reflection of GC Intelligence priorities
  - NSPL drives the entire SIGINT process
  - *All NSPL items are mapped to a* **"GCR"** *a government of Canada requirement*
  - NSPL is tier based, 0 is the highest and 4 lowest priorities
  - NSPL includes *Standing Issues* and *Watch Briefs*

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

CSEC SIGINT is

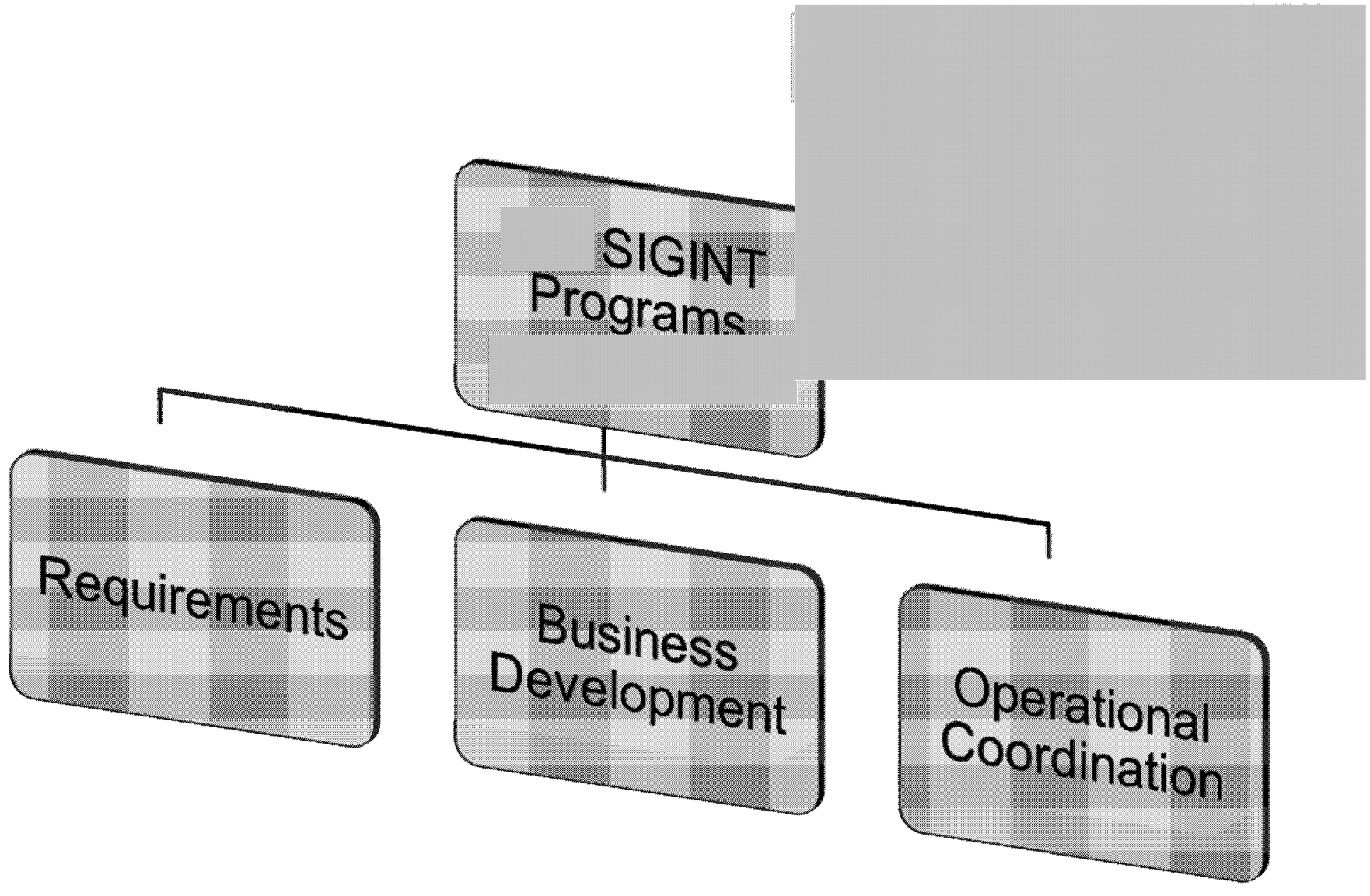


Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



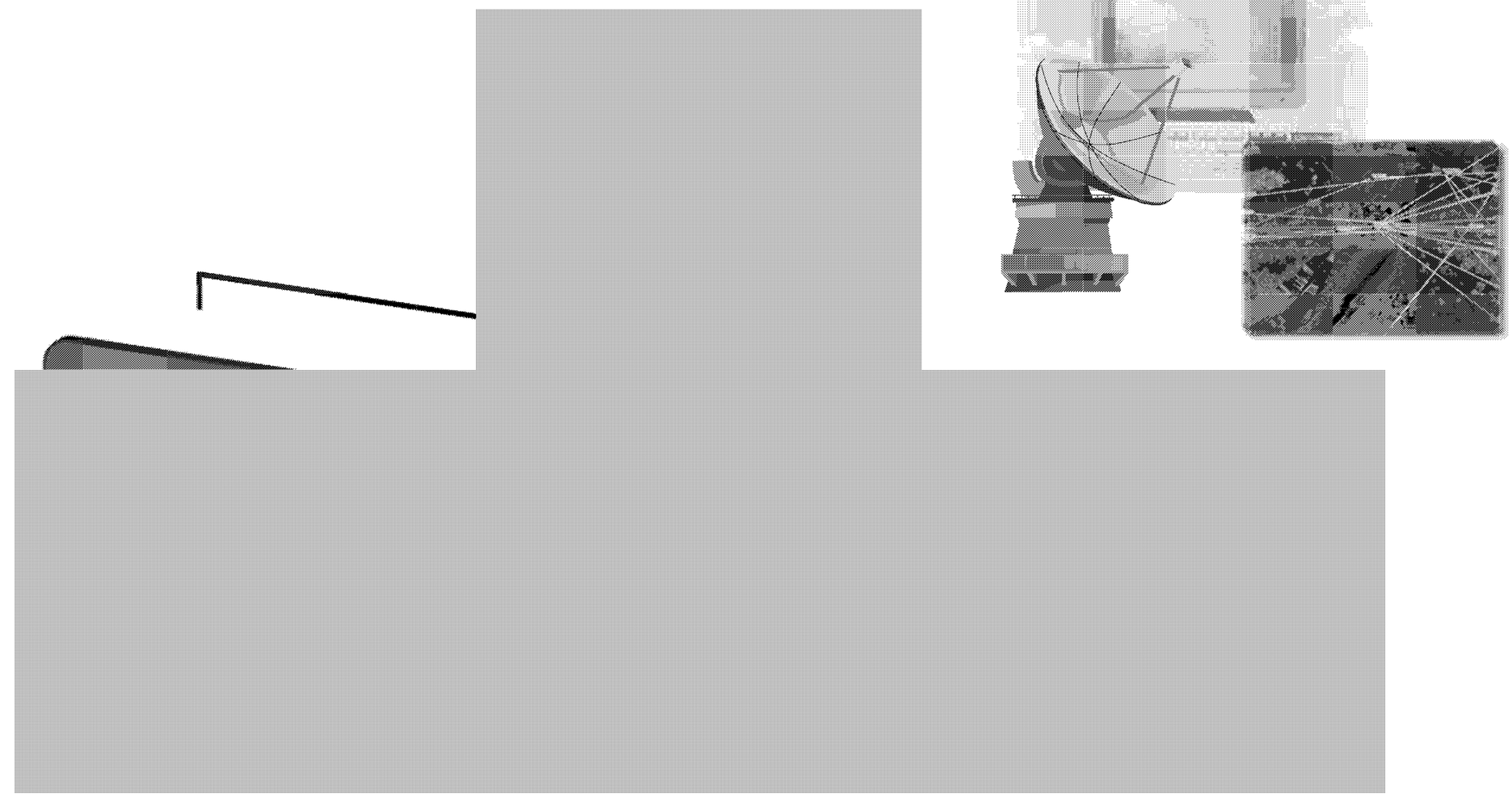
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

SIGINT Programs



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

SIGINT Access

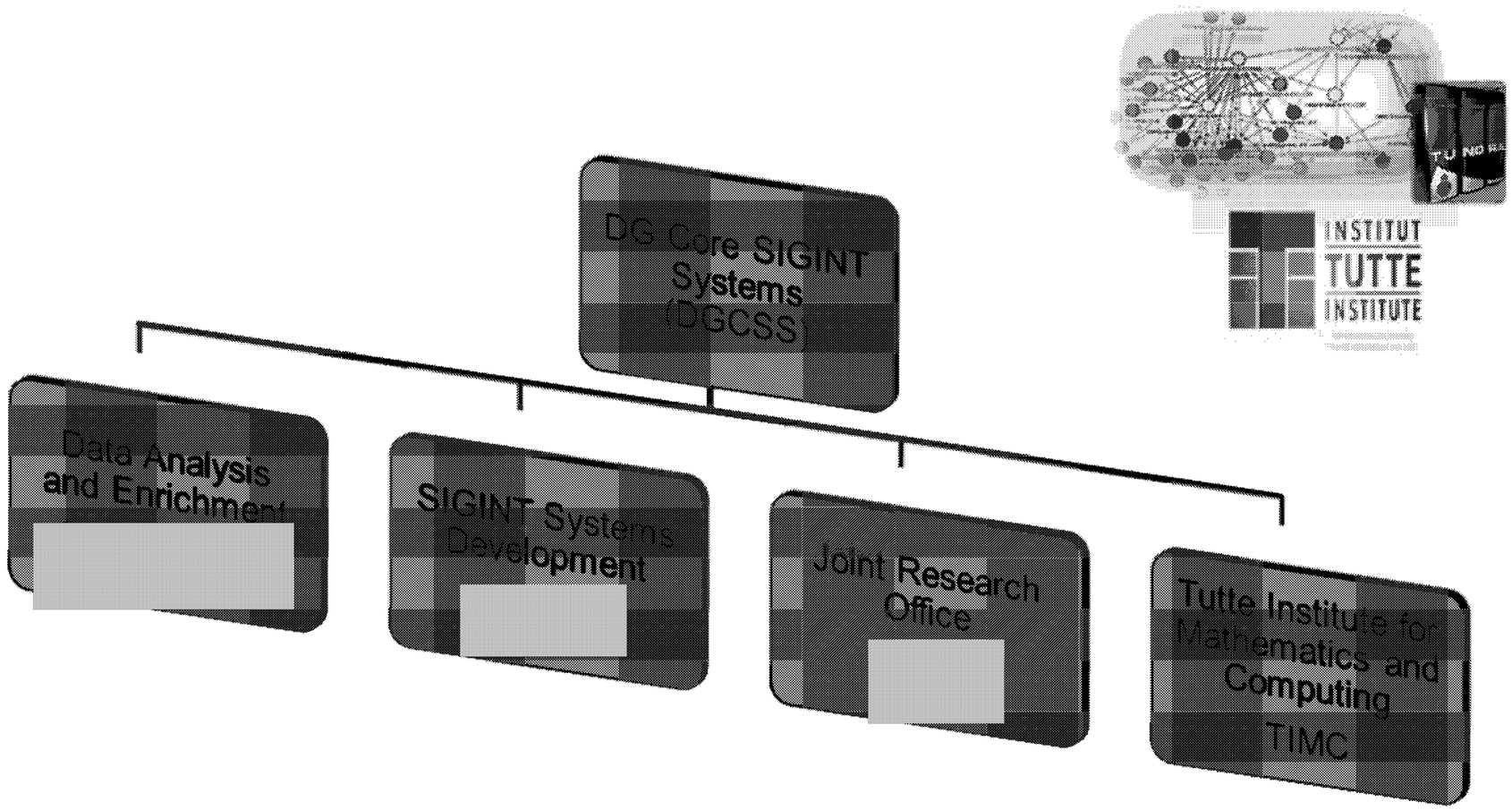


Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

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

[redacted] SIGINT Systems



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

Intelligence

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Capability Snapshot

- Engineers
- Mathematicians
- Computer Scientists
- Intelligence analysts

s.15(1)

s.15(1)

s.15(1)

s.15(1)

s.15(1)

Conclusion

[redacted]

- CSEC SIGINT collaborates with partner agencies to leverage resources

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC's International Partnerships
The 5-Eyes Relationships

CSEC 101:
Foundational
Learning Curriculum (FLC)

May 2012
Cerrid# 810545

Presenters:

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

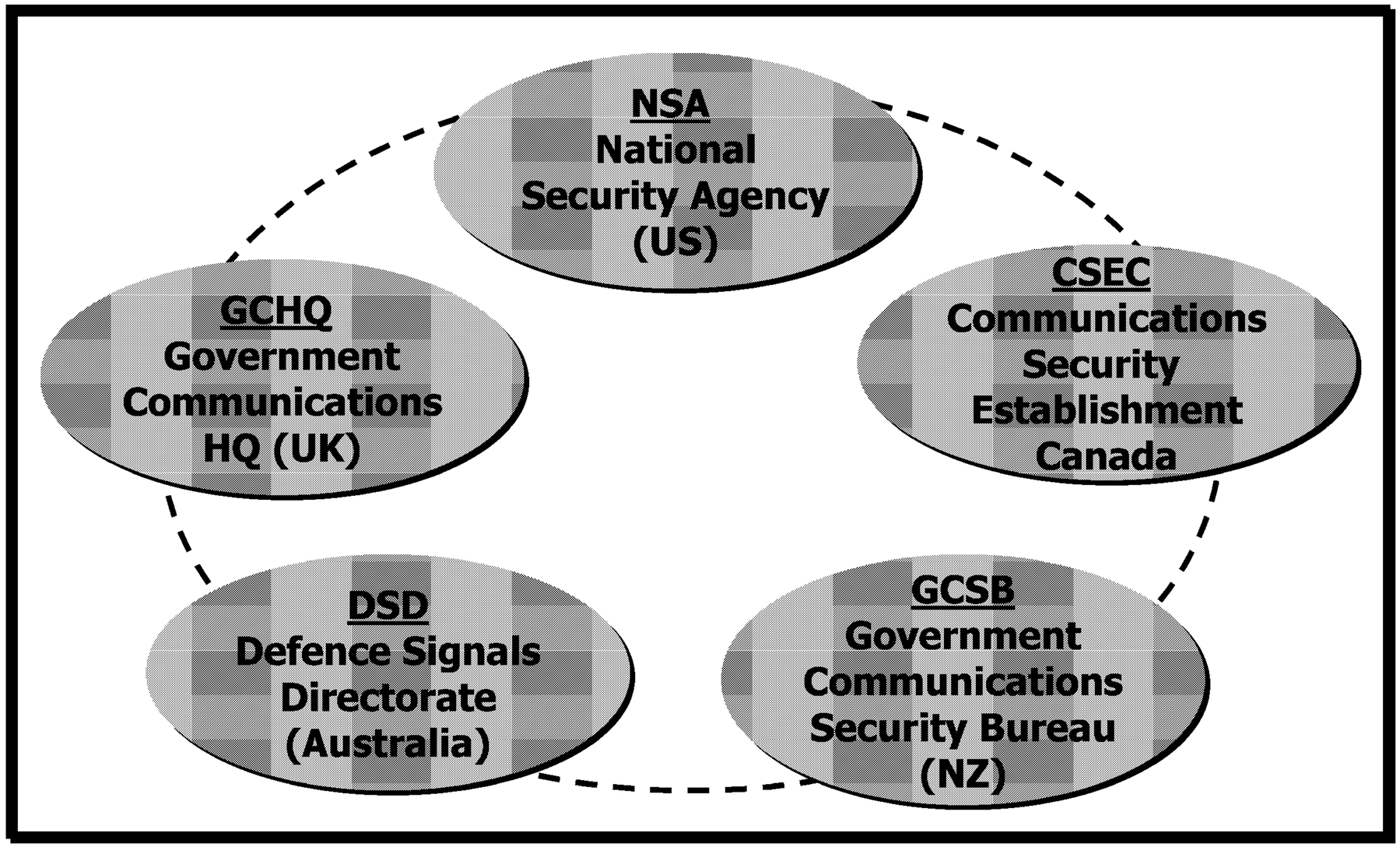
Canada

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

We will discuss:

- Who and where are these partners?
- History of the partnership (briefly)
- The importance of the partnership
- How/why we collaborate

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



We've been partnering a long time…

- Canada and UK collaborate to initiate or first intercept operation in British Columbia (1925)
- UK and US cryptologic exchange (1940)
  - Canada and US cryptologic exchange (1942)
  - UKUSA (1946): UK and US agreement
  - CANUSA (1949): Canada and US agreement
  - First Canadian Liaison posted to GCHQ (1949)
  - Canada produces NATO cryptographic material (1955)

Importance of Sharing

A part of our ability to access intelligence derives from our intelligence alliances and relationships. For many years Canada has exchanged information with key allies. … These relations are enormously beneficial to our country. Canada alone could not replicate the benefits gained through these international arrangements. But we are also a significant contributor of intelligence. These contributions are recognized and appreciated by our allies.

Securing an Open Society: Canada's National Security Policy, 2004 (p. 17)

s.15(1)

How we Collaborate

- Across the Board – SIGINT, IT Security, Corporate Services, DGPC, CIO…
- Operational and Strategic level co-operation
- Crisis collaboration
- Reach into each others' respective Security and Intelligence Communities
- [redacted]

s.15(1)

Collaboration – *not always easy (but worth the effort)*

- Different time zones, cultures and languages
- Different policy and legal environments
- Different sizes of workforces and budgets
- [redacted]
- Technology platforms and infrastructure
- Cost of travel
- Personal relationships important!

Liaison Offices

- CANSLO = Canadian Special Liaison Officer
  - CSEC's representative to the foreign partner

  - Keeps CSEC informed of events, plans, policies, trends

- BRLO = British Liaison Officer
- SUSLO = Special US Liaison Officer
- AUSLO = Australian Liaison Officer
- NZLO = New Zealand Liaison Officer

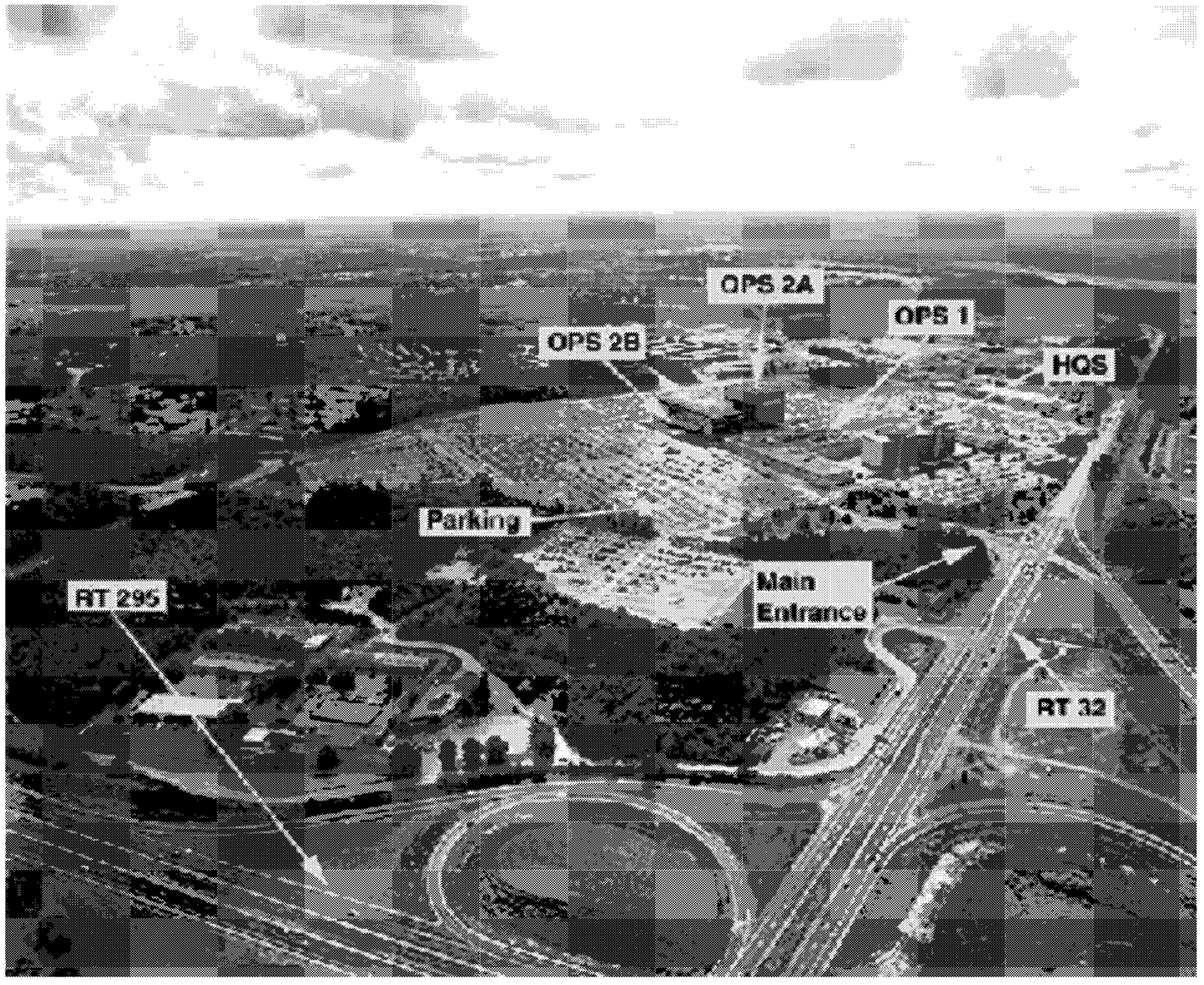
s.15(1)

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

NSA – Ft. Meade, Maryland

- civilians
- military staff

Total: ~ !!!!!



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

000464

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

SUSLOO

Special United States Liaison Office Ottawa

- SUSLOO –
- SUSLOO Office:
  Email: cse-cst.gc.ca

s.15(1)

s.19(1)

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

CANSLO/W

Canadian Special Liaison Office Washington

- CANSLOW –
-
- Office staff – CANSLO, Deputies, office assistants, communications officer
- Integrees – up to at any one time

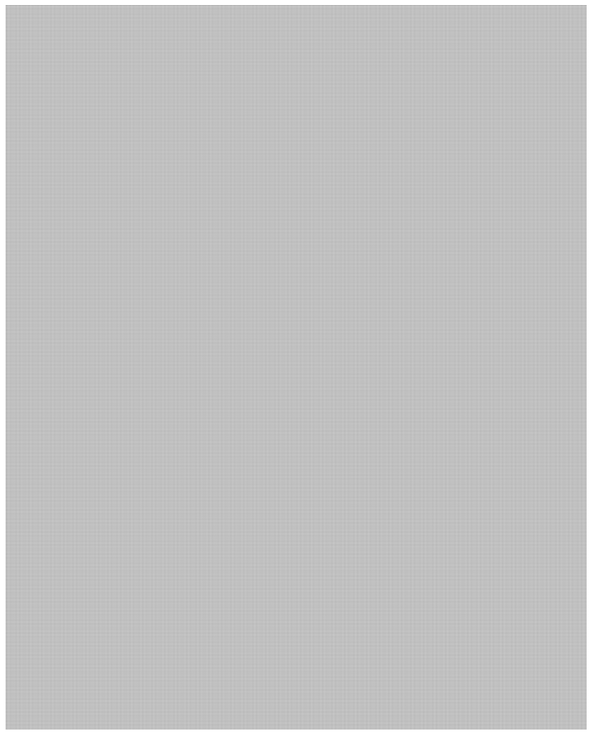
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

GCHQ – Cheltenham, UK

employees

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

BRLO
British Liaison Office



- BRLO –
- BRLO Office:
  Email: @cse-cst.gc.ca

CANSLO/L

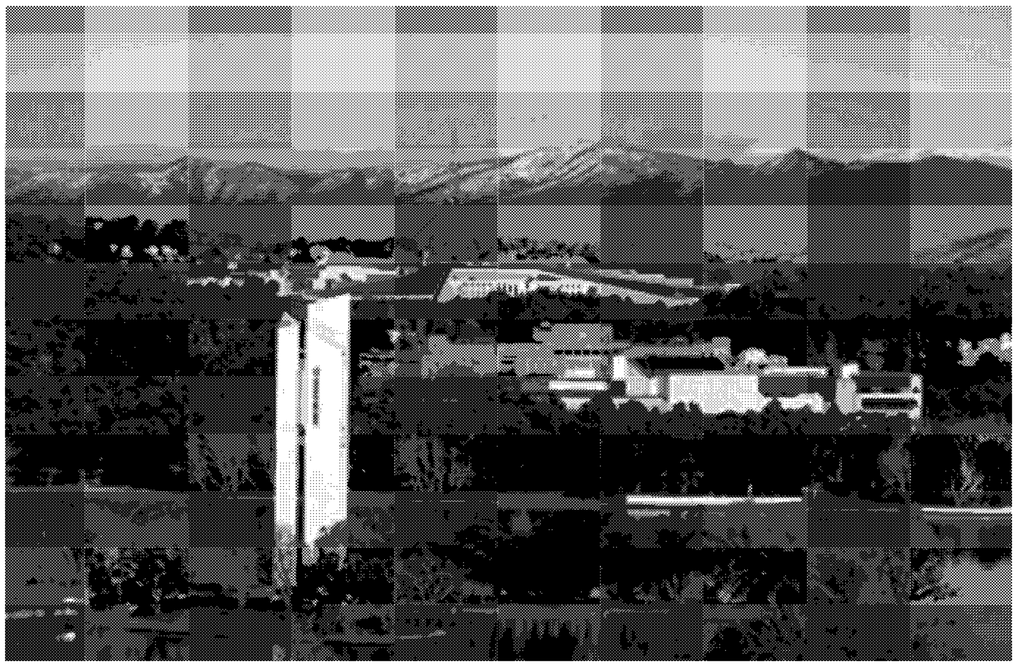
Canadian Special Liaison Office London

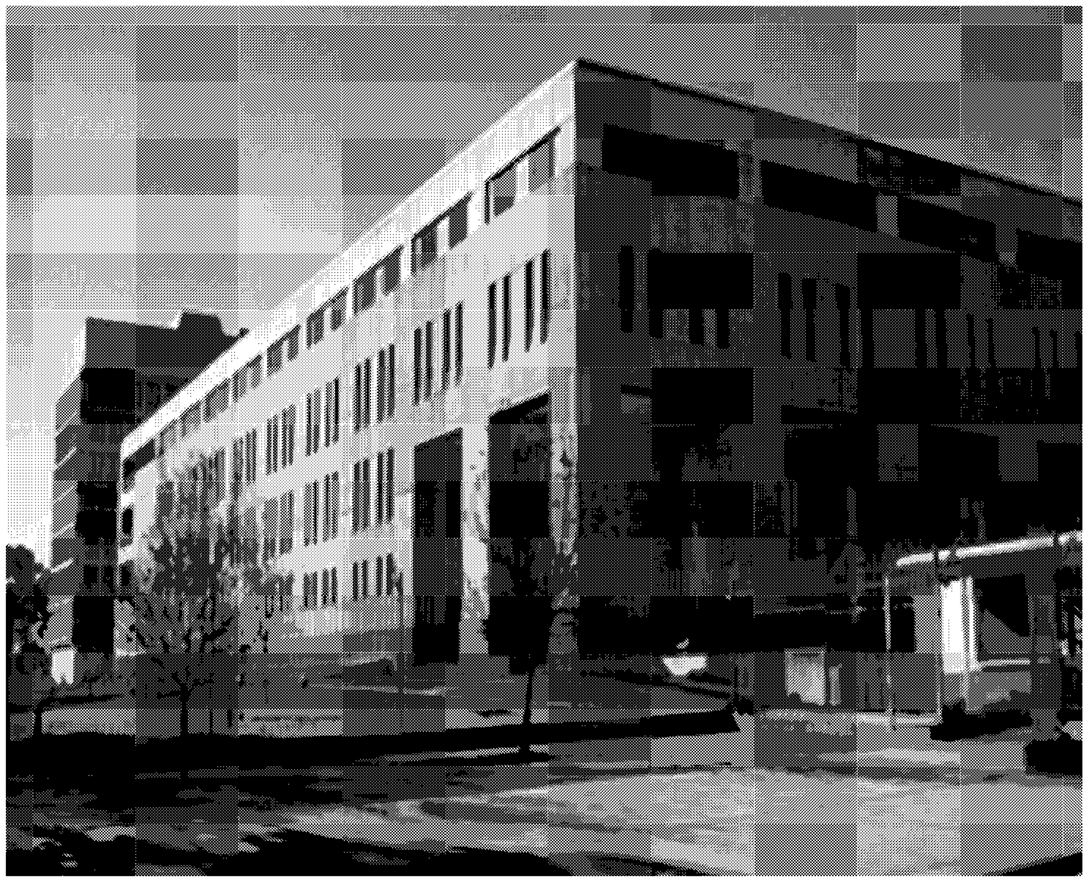
- CANSLOL –
  Email: @cse-cst.gc.ca
- Office staff – CANSLO/L, Deputy CANSLO/L, administrative officer
- CFIOG integrees at GCHQ
- CSEC integrees at any one time

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

DSD – Canberra, Australia

- [redacted] civilians
- [redacted] military staff (Australian Defence Force)





Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

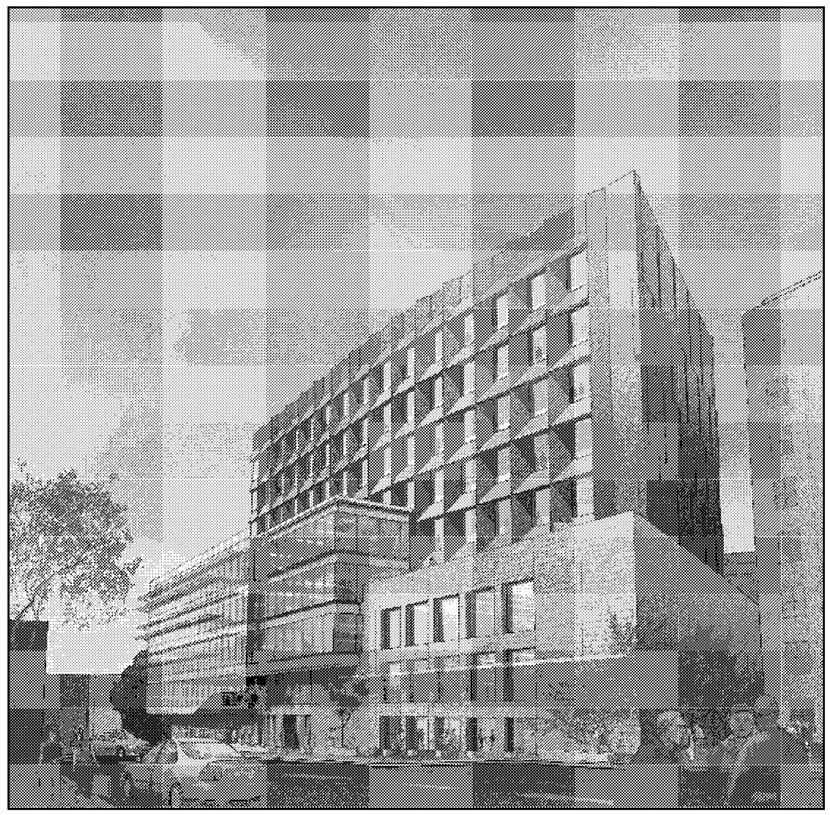
Canada

s.15(1)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

GCSB – Wellington, NZ

about [redacted] employees



s.15(1)

s.19(1)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

AUSLO
Australian Liaison Office

[redacted]

- AUSLO - [redacted]
- AUSLO Office: [redacted]

Email: [redacted]@cse-cst.gc.ca

s.15(1)

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

GCSB/NZLO

- [redacted]
- [redacted]

(nzlow@gcsb.govt.nz)

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

CANSLO/C-W

Canadian Special Liaison Office Canberra

- First CSEC liaison office in Australia opened in 2009 at DSD in Canberra
- CANSLO/C-W is
- Also CSEC's representative to GCSB in New Zealand.
- Accredited to Canadian High Commissions in Canberra and Wellington

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

The Partnership in Action

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Why do we work together?

- Shared missions and objectives
- History
- Geography
- Different strengths and weaknesses

s.15(1)

[redacted]

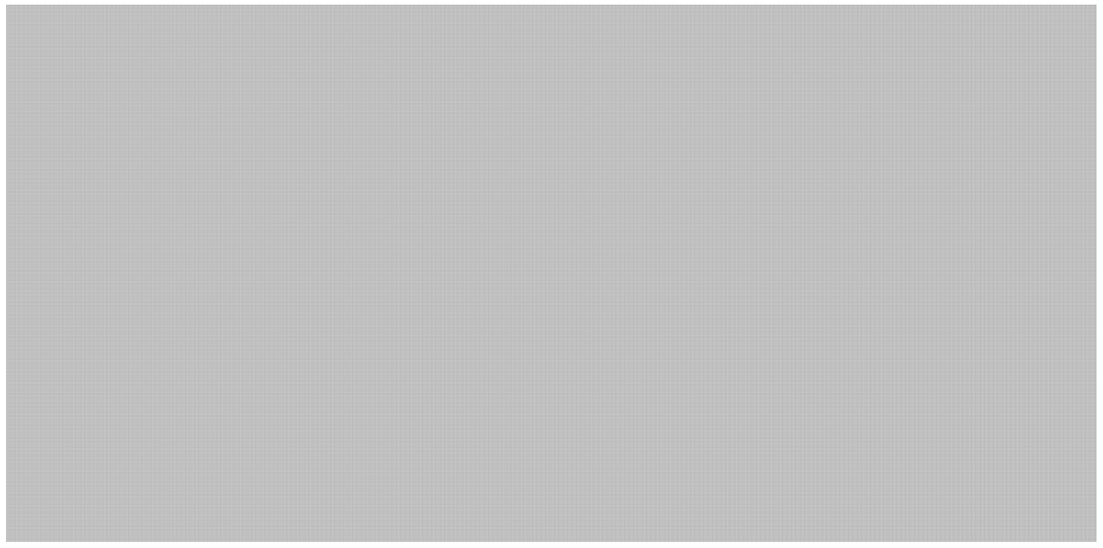
- Heads of 5-eyes agencies committed to helping each other to defend our national and mutual interests in cyberspace.
- [redacted]

What benefits do the partners have from working with CSEC?

- Agility
- Size
- Innovation/Creativity
- Unique skills
- Insight

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

How does CSEC benefit from working with the partners?



Take aways…

- The 5-Eyes alliance is critical to CSEC's ability to fulfill both its foreign intelligence and information security mandates.
- It has evolved since WWII into the most robust relationship in the international S&I community.
- [redacted]
- Canada benefits tremendously.

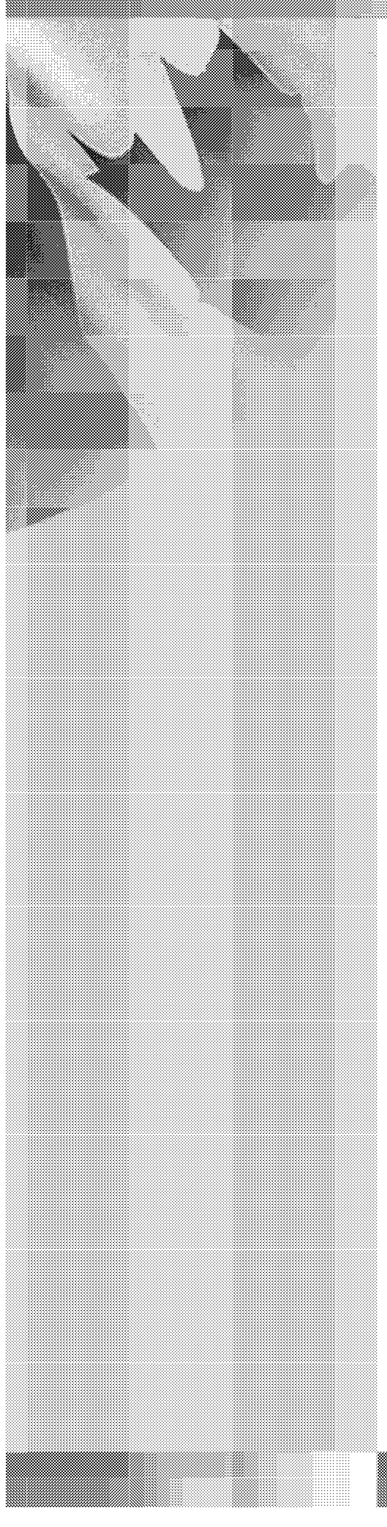
- *It is precious - Treat it with Care*!

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Questions?

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada



Introduction to the Security and Intelligence Community

SIGINT Programs, Oversight and Compliance

Objectives

- Identify primary "players" within S&I Community
- Outline roles within the community
- Delineate where CSEC fits
- Discuss how the S&I Community Works

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

Government of Canada Privy Council Office | Gouvernement du Canada Bureau du Conseil privé

Solicitor General of Canada

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Royal Canadian Mounted Police | Gendarmerie royale du Canada

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

National Defence | Défense nationale

Department of Justice Canada | Ministère de la Justice Canada

Foreign Affairs and International Trade Canada | Affaires étrangères et Commerce international Canada

Canada

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

Canadian Security Intelligence Service / Service canadien du renseignement de sécurité

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

Department of Justice Canada / Ministère de la Justice Canada

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Government of Canada / Privy Council Office — Gouvernement du Canada / Bureau du Conseil privé

Foreign Affairs and International Trade Canada / Affaires étrangères et Commerce international Canada

National Defence / Défense nationale

Canadian International Development Agency / Agence canadienne de développement international

Natural Resources Canada / Ressources naturelles Canada

Transport Canada / Transports Canada

Financial Transactions and Reports Analysis Centre of Canada / Centre d'analyse des opérations et déclarations financières du Canada

Canadian Food Inspection Agency / Agence canadienne d'inspection des aliments

Public Health Agency of Canada / Agence de la santé publique du Canada

Canada Border Services Agency / Agence des services frontaliers du Canada

Citizenship and Immigration Canada / Citoyenneté et Immigration Canada

Public Works and Government Services Canada / Travaux publics et Services gouvernementaux Canada

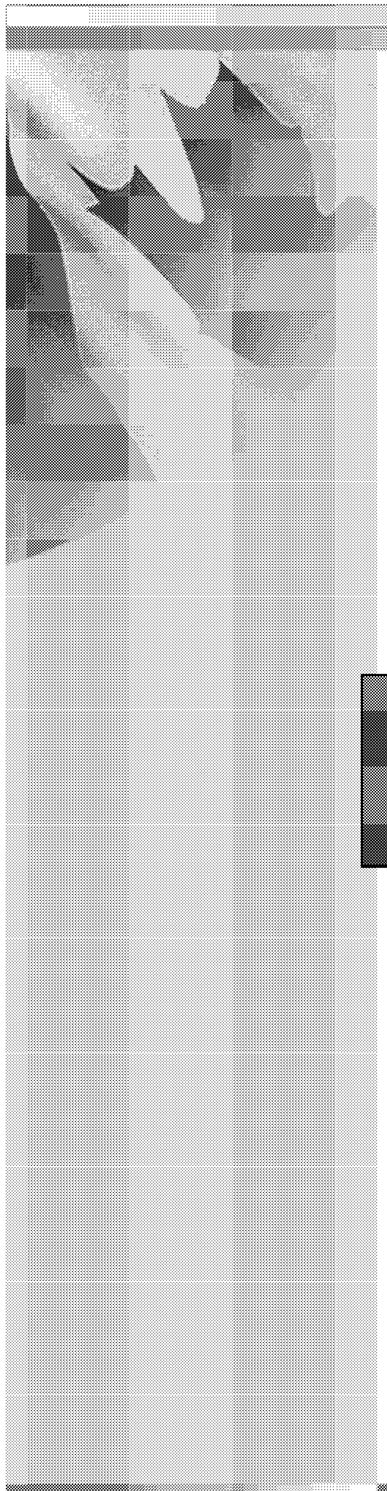
Canada Revenue Agency / Agence du revenu du Canada

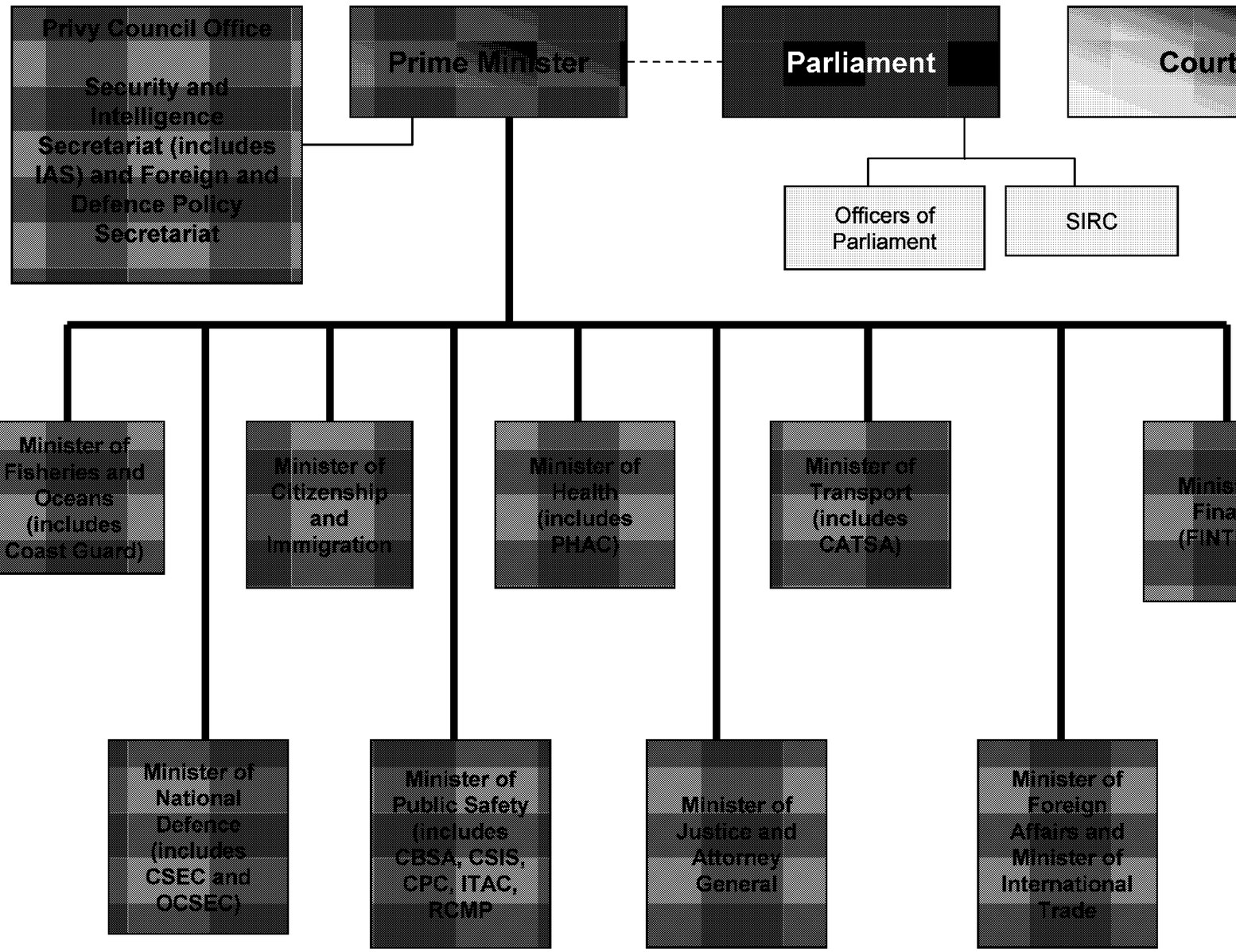
Public Safety Canada / Sécurité publique Canada

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

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada





Canada

Roles within the Community

PRODUCERS

CSEC: Communications Security Establishment Canada
CSIS: Canadian Security Intelligence Service
DFAIT: Department of Foreign Affairs and International Trade
DND&CF: Department of National Defence & Canadian Forces
FINTRAC: Financial Transaction and Reports Analysis Centre of Canada
RCMP: Royal Canadian Mounted Police

PRIMARY CONSUMERS

CBSA: Canada Border Security Agency
CIC : Citizenship and Immigration Canada
CSIS: Canadian Security Intelligence Service
DFAIT: Department of Foreign Affairs & International Trade
DND&CF: National Defence & Canadian Forces
FINTRAC: Financial Transaction and Reports Analysis Centre
PCO: Privy Council Office
TC : Transport Canada

SECONDARY CONSUMERS

AEC: Atomic Energy of Canada
CFIA: Canadian Food Inspection Agency
CIDA: Canadian International Development Agency
CG: Canadian Coast Guard
CNSC: Canadian Nuclear Safety Commission
CRA: Canada Revenue Agency
CSA: Canadian Space Agency
DFO: Department of Fisheries and Oceans
EC: Environment Canada
EDC : Export Development Canada
HC: Health Canada
IC: Industry Canada
PHAC: Public Health Agency of Canada
PSC: Public Safety Canada
NRCan: Natural Resources Canada

Canada

How the S&I Community Works

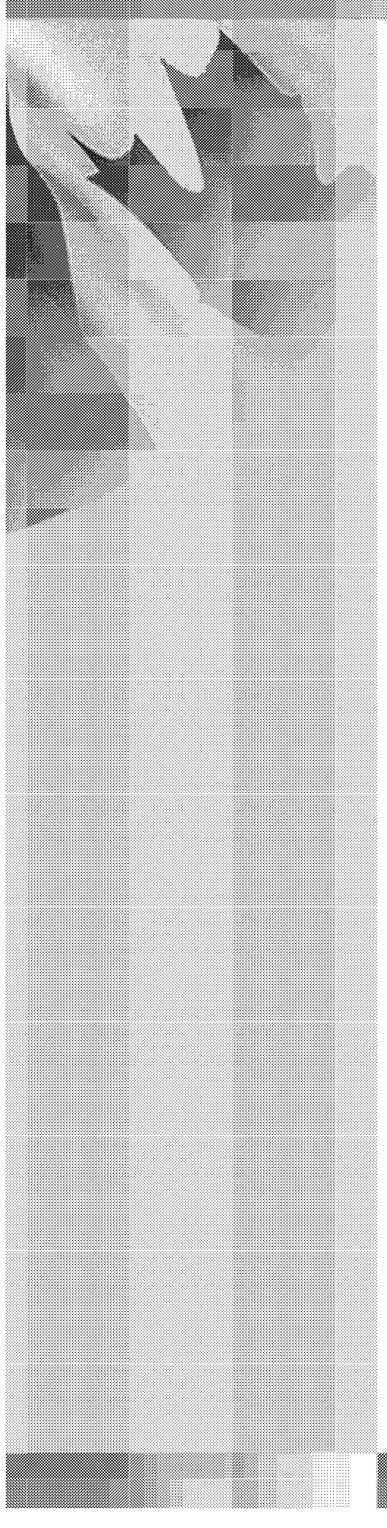
Intelligence Priorities

- Sets intelligence priorities for the Government of Canada
-
-
- Used as a basis in drafting NSPL

How the S&I Community Works (cont'd)

Policies and Programs

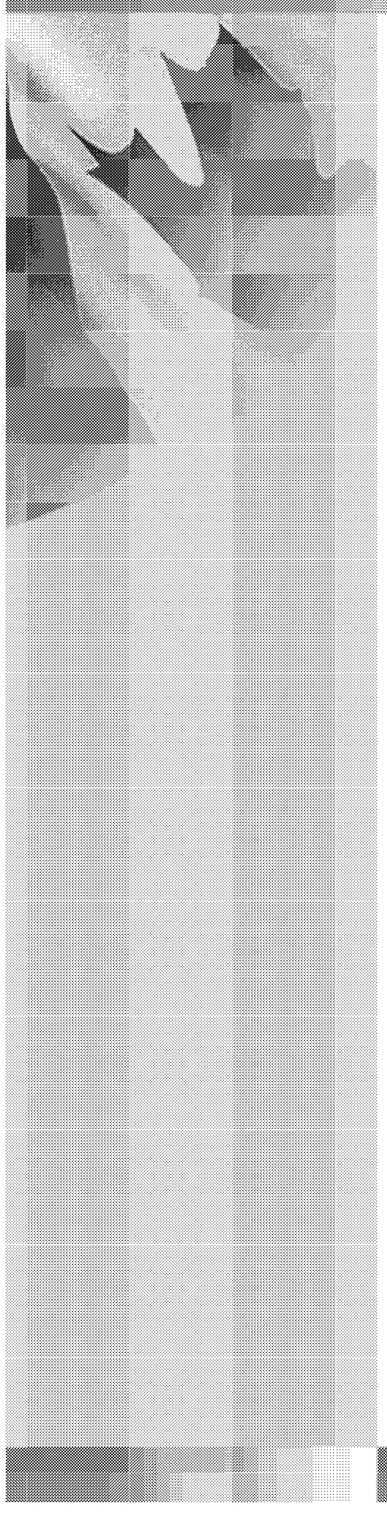
What do you think were the major issues (in 2009-2010) that the FAS Cabinet Committee approved and were seeking funding in Budget 2010?



[redacted]

How the S&I Community Works (cont'd)

Balancing competing priorities



Questions???

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Canada

Overview

- JENGA!
- IM…Why bother?
- What is information management (IM)?
- IM Roles and Responsibilities
- Key IM Concepts
- Why is IM important? / What's in it for you!
- IM Services at CSEC
- Questions?

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

Why Bother?: An IM True Story!

RE: Helloooo - Message (Plain Text)

RE: Helloooo - Message (Plain Text)

RE: Helloooo - Message (Plain Text)

RE: Helloooo - Message (Plain Text)

RE: Helloooo - Message (Plain Text)

File Edit View Insert Format Tools Actions Express Help

Reply | Reply to All | Forward

From: Sent: Fri 08/04/2011 12:05 PM

To: @forces.gc.ca'

Cc:

Subject: RE: Helloooo

-----Original Message-----
From: @forces.gc.ca [mailto: @forces.gc.ca]
Sent: April 8, 2011 11:52 AM
To:
Subject: RE: Helloooo

Found it! under "Training" called "Training for Alerts" - which is where we would expect it to be! It was that "Alerts Workflow" doc that got me confused (must have been Angela's from way back!)

thanks, and have a good weekend,

Canada

What is Information Management?

Information

Information is records, documents, files, resources, and data used by CSEC in the course of its daily operations, regardless of medium, format or topic.

Information Management

A discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal or long-term preservation.

Canada

Basic IM Precepts – Documents & Records

Information formatted for human interpretation. Can be any media or form. Examples are emails, photos, reports, memos, diagrams, videos, recordings, etc.

Can be altered or destroyed

Any document communicated to another person, other than a publication, regardless of media or form, **having operational, business or archival value**

Must be **inventoried**

Must be **managed**

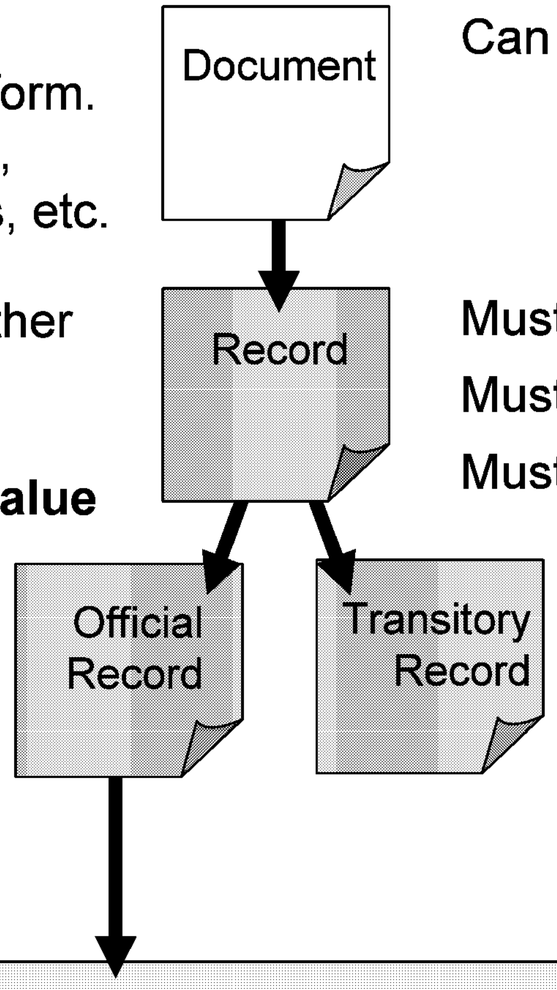
Must **not be altered**

Record created, collected or received by CSEC employees & used for operational, business or legal purposes

Must be **retained until the end of its retention period**

Required for a limited time to ensure the completion of a routine action or the creation of a subsequent document

May be **routinely destroyed**



Disposition - records of historical but no further operational or business value are either transferred to Library and Archives Canada, destroyed, or alienated from the control of the GC.

Canada

IM Roles and Responsibilities – What?

All Government of Canada Employees are:

responsible for managing information they collect, create and use as a valuable asset to support the outcomes of CSEC's programs, services, operational needs and accountabilities.

(Directive on IM Roles and Responsibilities, Communications Security Establishment Canada and Treasury Board Secretariat, 2007*)*

Your key IM Roles and Responsibilities – How?

- **Manage** information as a key corporate resource.
- **Identify**, **file** and **organize** information for quick and easy retrieval.
- **Provide access** to information, as appropriate.
- **Retain** and **dispose** of information appropriately.
- **Take responsibility** for your performance in the management of information.
- **Comply** with information policy and legal requirements.

Staying Compliant - The Goals of Sound I.M.

- **Quality** information is created and provided;
- Program service and delivery is **efficient;**
- **Decisions** are documented;
- Information is **available** (captured, organized, accessible, maintained, and preserved);
- Information is **protected** in accordance with legislation and policy requirements; and
- Information is **disposed of** in accordance with legislation and policy requirements.

GC Legal and Policy Requirements

When dealing with information we must always be aware of and respect GoC legislative and policy requirements.

Examples:

- ATI and *Privacy Acts*
- *Library and Archives of Canada Act*
- *Financial Administration Act*
- TBS *Policy on Information Management*
- TBS Directives:
  - Directive on IM Roles & Responsibilities
  - Directive on Record Keeping

Key IM Concepts - Official Records

In order to ensure that the Government of Canada can **provide documentary evidence** of all of its **activities**, all federal government employees must be diligent about **saving official records** (Information Resources of Business Value).

Key IM Concepts – Official Records

Official Records **document** or provide evidence of a department's **business activities**.

You **must save** all of your official records.

Examples:

- Briefing notes;
- Policies and Directives (including materials that would allow for reconstruction of a policy);
- Final reports, Performance Results, business deliverables (including those from outside sources);
- Materials of historical or research importance; and
- Documents that result in or influence a business decision or that require a signature.

Key IM Concepts – Transitory Documents

Transitory records are information sources that are only required for a **limited period of time**, in order to complete a routine action or to prepare a subsequent record.

Examples:

- Duplicate copies or Photocopies of departmental pubs;
- Casual communications, misc. FYI notices;
- Information received as part of a distribution list; and
- Draft documents (changes have been incorporated into a subsequent document or final version).

Key IM Concepts – Transitory Documents

In order to ensure that the Government of Canada can **support** its information **systems** and **produce relevant information** with ease and accuracy upon its request, all GoC employees must be diligent about deleting or destroying transitory records.

Check Your Knowledge – Official and Transitory

OFFICIAL

CSEC Business Continuity Planning Policy

Ink signed Memorandum of Understanding

Signed project charter

Cyber Defense SIGINT reports

Budget records

Report for CSEC done by a consultant

Email SENT to a dist. list regarding a decision

Meeting Minutes

Annual Personal Performance Report

Cyber Protection Priorities progress reports

Staffing & Recruitment Policy

CSEC Chief's notes to staff - 2003

An original or master copy of a CSEC publication

Transaction-orders or receipts (requests and confirmations)

Equipment inventory

Correspondence b/w clients/vendors/partners

Corporate Services business plan

Notes in lab books

Results from a survey

Organization Charts

TRANSITORY

Blueprint copy of CSEC's new building

Grand & Toy Catalogue

Email RECEIVED via dist. list regarding a decision

Photographs of CSEC's new building

Final results of the first division beach volleyball league

Blackberry pin-to-pin messages

Printed user manual

Supporting data used to update processes

Your copy of the ITS Learning Catalogue

Blogues

Email invitation to meeting to discuss project

Email invite RECEIVED to attend corporate event

Tweets

Canada

IM Supports Transparency, Collaboration and Informed Decision Making

- We must be able to **easily** produce **all** of the appropriate information when the public, or other departments (internal and external review bodies), ask for it – **transparency**.

- We must share information (make it accessible) appropriately among our colleagues, between departments and across government to facilitate, enhance and make our work more efficient – **collaboration**.

- We must be able to use the information that we have to make effective and **informed decisions**.

Canada

Managing Information: What's in it for you?

You'll be able to:

- Find the right information faster and easier - when it's needed;
- Reduce 'level of effort' by minimizing duplication of work;
- Easier to share information with your colleagues;
- Provide easy access to quality, reliable information to others;
- Make informed decisions based on up-to-date information;
- Increase your ability to meet business, legal and accountability requirements (e.g. ATIP requests); and
- Demonstrate legal and policy compliance.

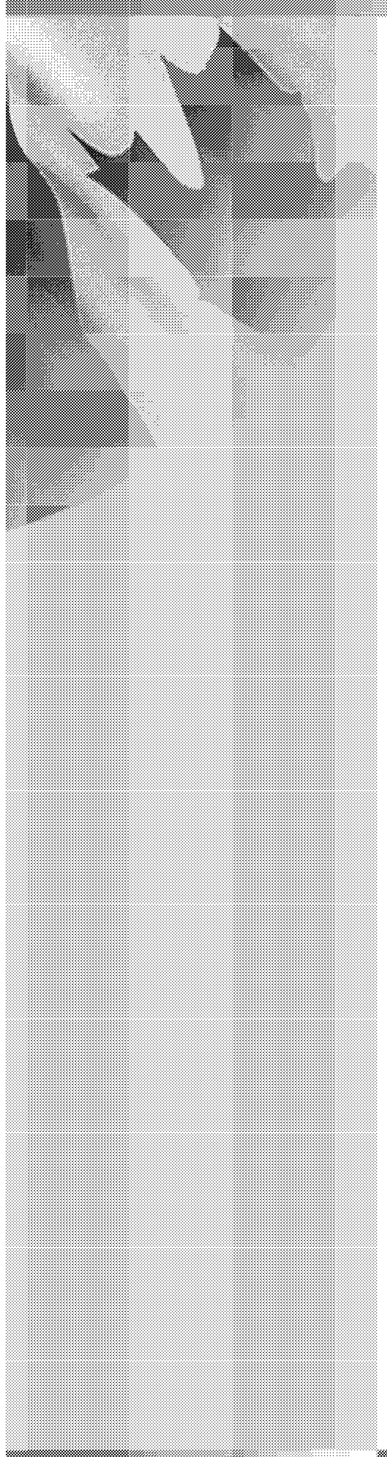
IM Services at CSEC

Information Management Directorate

- CERRID
- Information Management Advisors
- Information Management Training
- Information Holdings Services
- Information Management Awareness

Questions?

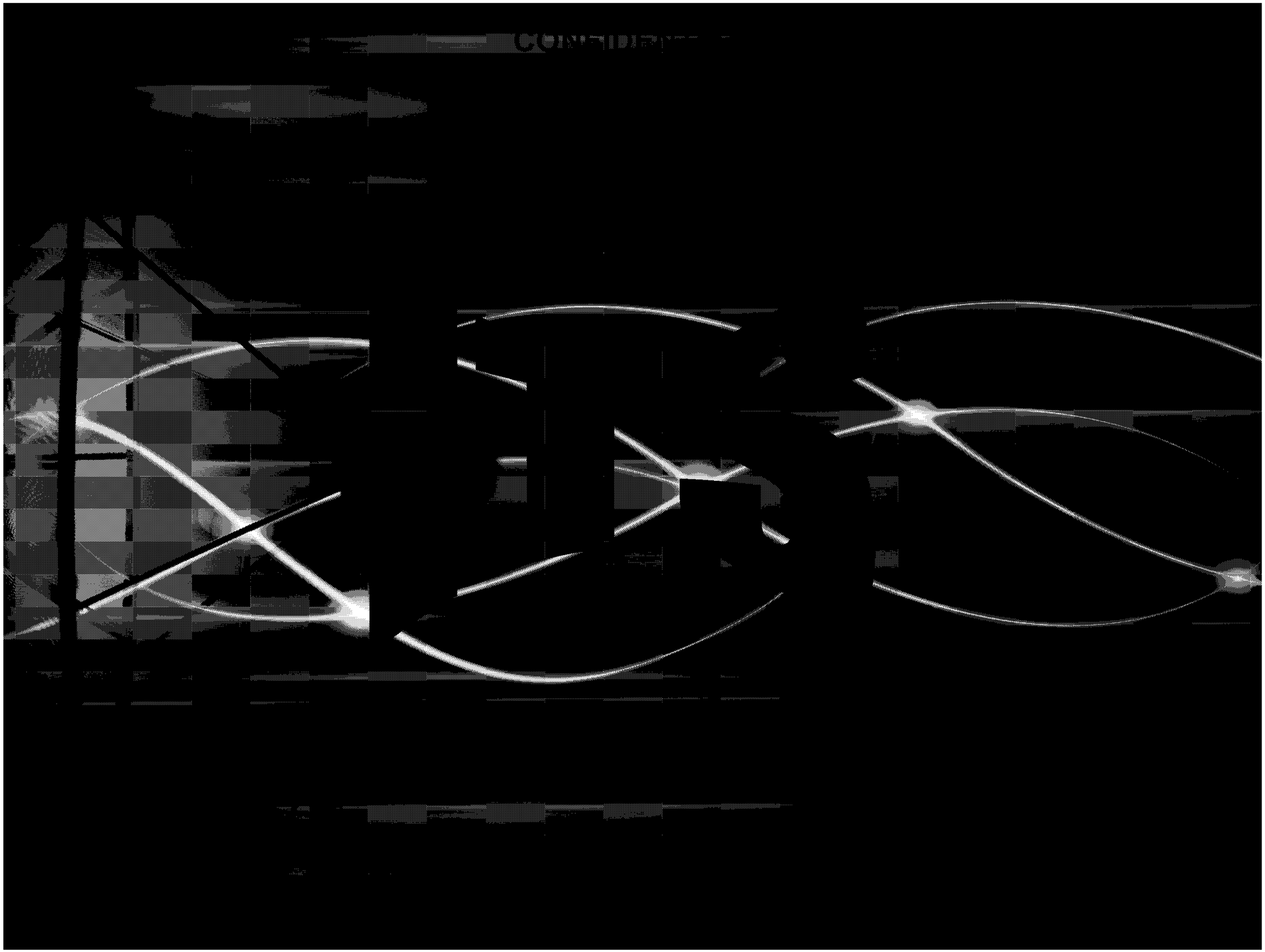
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

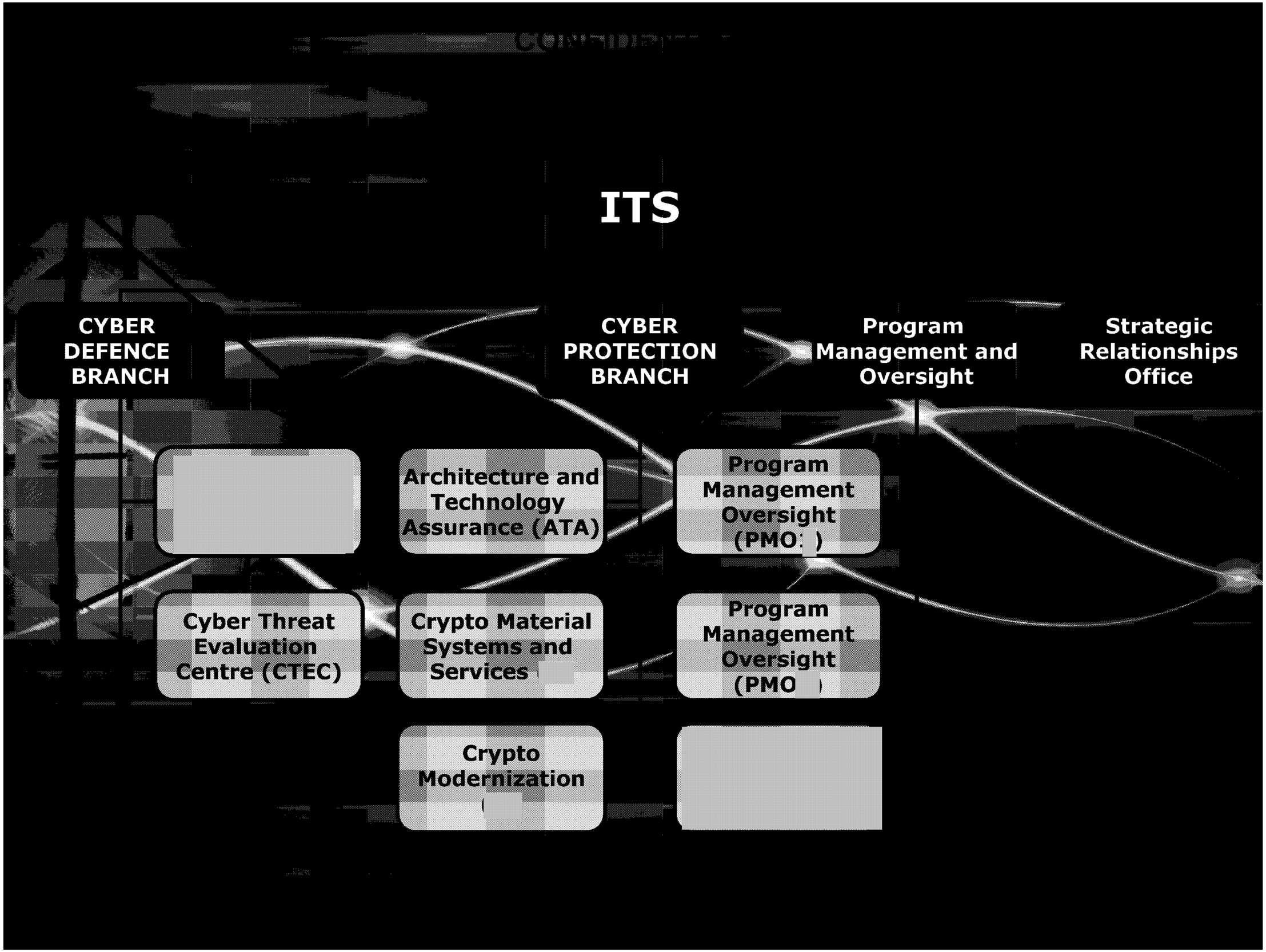


Foundational Learning Curriculum

The Information Technology Security (ITS) Organization

Canada





Cyber Defence Branch Mission

"To detect and mitigate sophisticated cyber threats and attacks against information systems of importance to the GC"

Cyber Defence Branch

- Monitor GC systems

- Tactical advice / guidance to GC Depts
- Distribute warning, flashes, cyber info
- In-depth technical analysis on data
- Develop defensive plans against specific threats

CTEC

Cyber Protection Branch Mission

"to protect Government of Canada electronic information"

Cyber Protection Branch

- Wireless and Emission security testing
- Onsite assistance to depts. after security incident
- Work with PWGSC and TBS on COTS policy & requirements
- Work with industry to evaluate/certify commercial IT security products

ATA

- enable GC departments to conduct operations and protect GC most sensitive information
- CSMI – will provide the foundation for the next generation of systems for key management

Electronic Key Management System

- Ordering, Generating, Distributing keys
- Distribution of COMSEC material to GC
- National COMSEC Incidents Office (manage incidents)
- National COMSEC Audit Team

s.15(1)

ITS Program Management and Oversight

"PMO coordinates & analyzes any external requirements on behalf of the IT Security program"

PMO

- Strategic and Business Planning
- Human Resources development and tracking
- Financial planning and program monitoring
- Tracking and vetting deliverables

PMO

PMO

ITSLC

- Develop and provide effective and efficient IT Security Training, Education and Awareness for all GC IT security professionals and employees
- PoS /38 courses

- Provide operational policy advice and guidance to operators to ensure ops are conducted lawfully and protect the privacy of Canadians
- Verify compliance (spot testing, documentation, procedures)

IT Security Strategic Relationships Office

"establish and maintain effective relationships to realize CSEC objectives"

Strategic Relationships Office

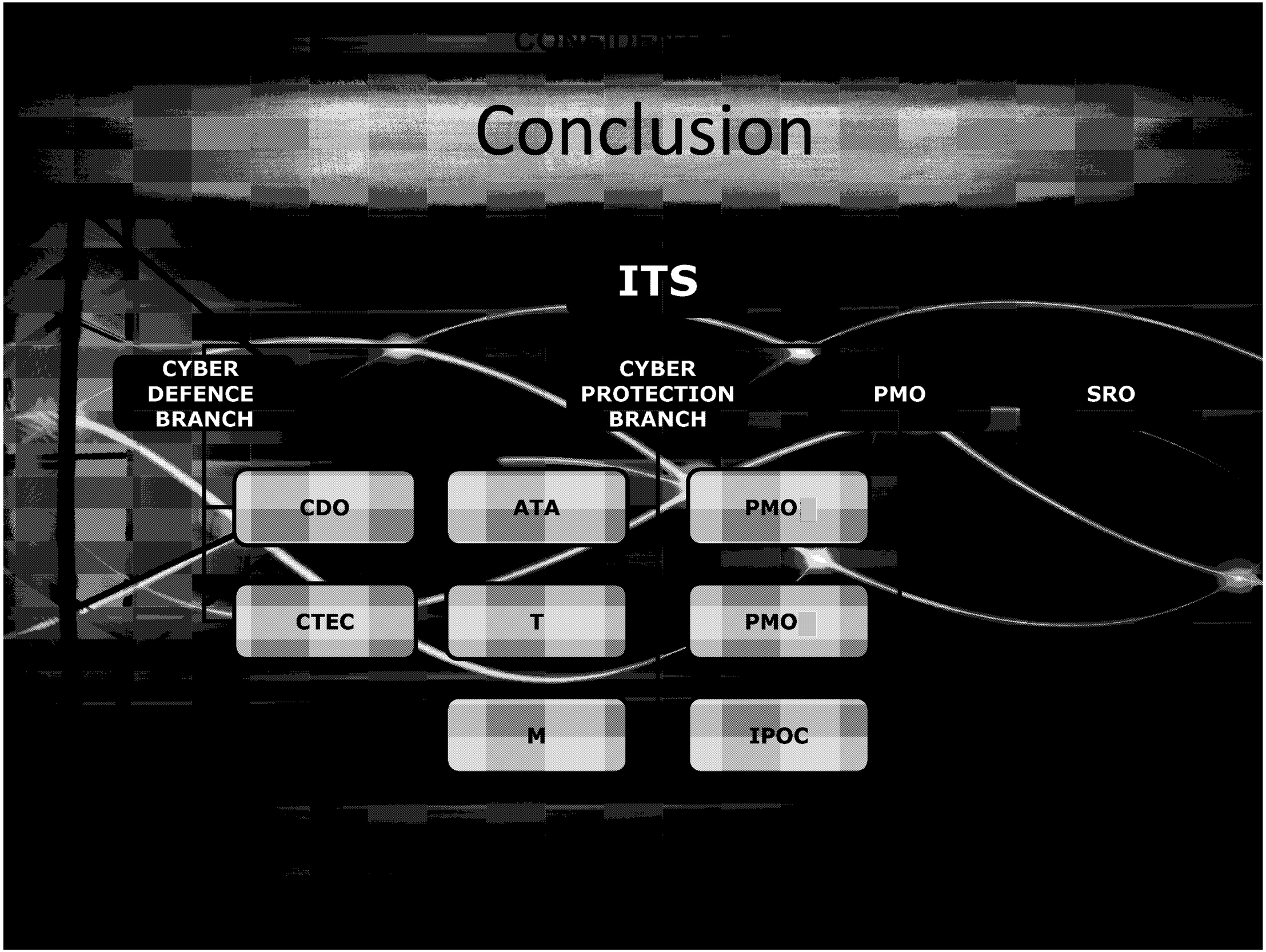
- Develop strategic cyber-security relationships with Industry, SSC and TBS

[redacted]

ATA	- Emission Security [redacted]
T	- Provide Crypto equipment (Taclane, SCIP- STE) from National reserve - Issue and manage related crypto key
ITSLC	- Conduct on-site training on Crypto equipment (STE and Taclane) [redacted]
CDO	- [redacted]
CTEC	- Issue warnings on the increased threats - Analyse available data and if threats exist set up a plan to counter, coordinate incident response as req'd
IPOC	- Brief the analysts (CDO) with regards to Privacy issues involving Canadians, rules of engagement etc - Monitoring operations for compliance
PMO [redacted]	- Wallet…PMO [redacted] will be tracking all expenses incurred (overtime, equipment purchases etc.)
SRO	- Initial and continued liaison with other gov't departments and engaged private sector partners
M	- Their mission will take fruit in the future

[redacted]

Conclusion



Questions

Questions

Canada

COMPENSATION

AND

BENEFITS

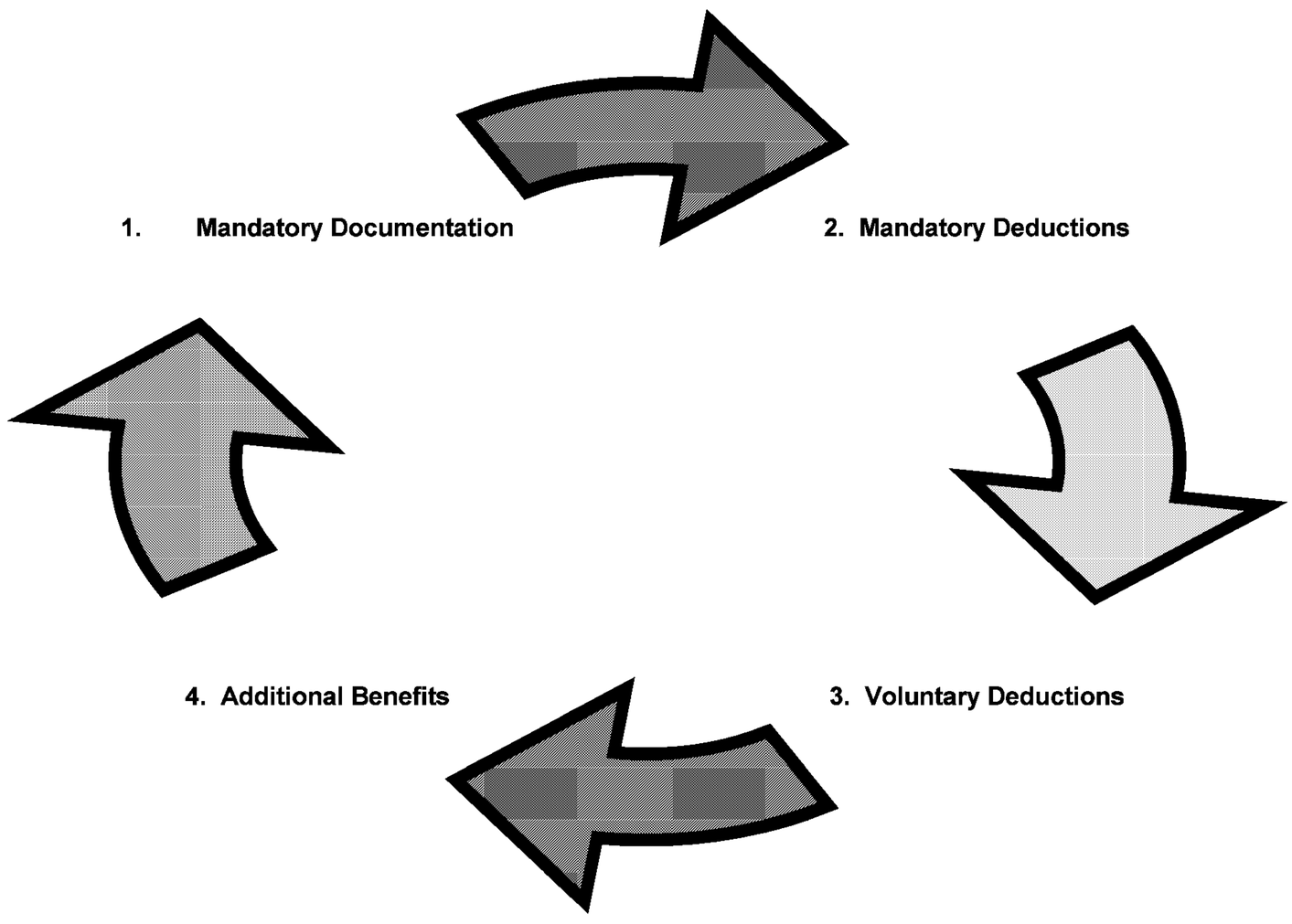
Compensation and Benefits Unit

- You are assigned a Compensation Advisor based on your group within CSEC.

- Your advisor will provide you with compensation, insurance and pension information throughout your CSEC career.

- Life events:
    - Hire
    - Retirement
    - Promotion
    - Marriage
    - Illness

HOW WILL WE PROCEED?



Personal Record Identifier (PRI) and Pay List

- **PRI**
  - Personal and confidential number
  - To identify you on all CSEC forms
  - May be the same as previous department or may be a new one
  - Can be found on your pay stub

- **Pay List**
  - Can be found on your pay stub
  - Identifies your Compensation Advisor

Mandatory Documentation

- Personnel Questionnaire
  - Required information to start your pay

- Tax Forms (TD1 – TD1ON)
  - Determine accurate tax bracket

- Direct Deposit
  - For indeterminate or > 6 months term
  - possibility of two accounts (regular pay/supplementary pays)

General Pay Information

- One collective agreement
- Paid on a current bi-weekly basis (basic pay and allowances)
- Each pay period begins on a Thursday and ends two weeks later on Wednesday (pay day)
- Pay Stubs - we do not have access to the Compensation Web Application
- Increments

Mandatory Deductions

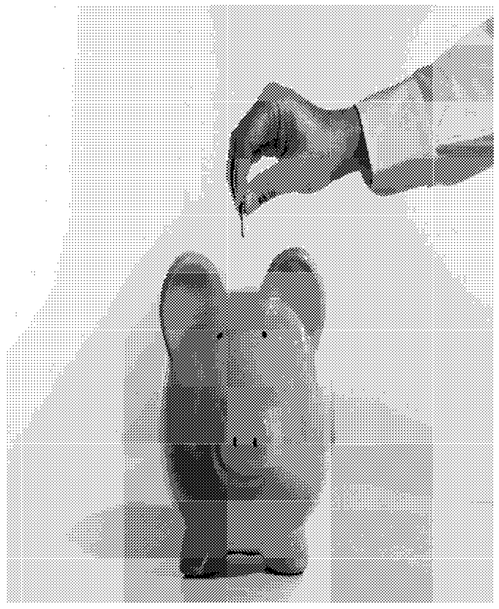
- Federal Income Tax based on province of work
- Canada Pension Plan (CPP)
- Employment Insurance (EI)
- Public Service Superannuation (PSSA)
- Supplementary Death Benefit Plan (SDB)
- Disability Insurance (DI)
- Union Dues
- Sales tax (employee premium paid for insurances)

Canada Pension Plan

- Federal mandatory pension plan
- 18 years of age to 71 years of age
- Bi-weekly deductions until you reach the yearly maximum amount.

2012: $2,306.70

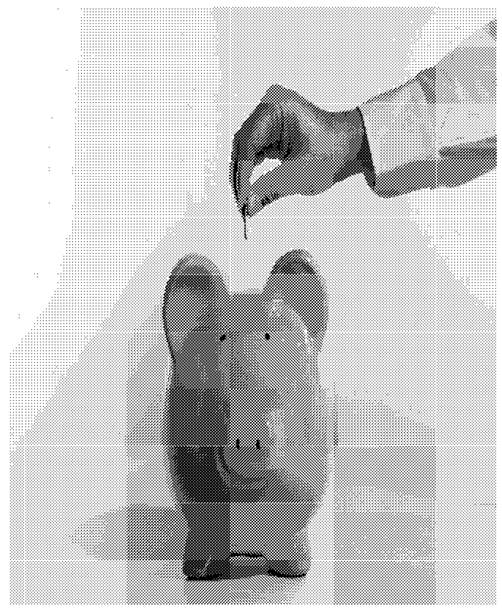
- Are you in receipt of CPP?
  - (need letter of entitlement)



Employment Insurance

- Provincial mandatory Employment Insurance plan

- Bi-weekly deduction until you reach yearly maximum amount
  - 2012: $839.97



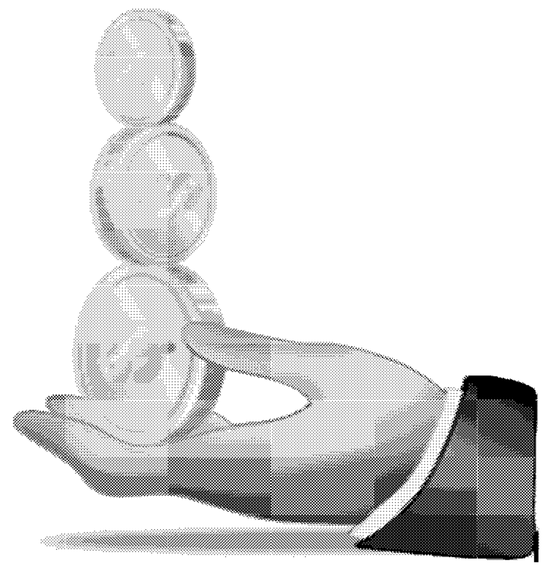
You
and
Your Pension Plan

– Indeterminate and Term > 6 months

- Log on the www.pensionandbenefits.gc.ca (access from work and home)
- Review information for new employees
- Review the 16 video series

Public Service Superannuation (PSSA) (cont'd)

- Provide employee with retirement income - calculation is based on contributory years of service, age and salary
- Low rate and High rate
  2012: 6.2 % (Low) (up to YMPE $50,100)
  8.6 % (High)
- Plan is integrated with CPP
- Vested after 2 years of pensionable service
- Contribute to a maximum of 35 years of service. After 35 years, contribute 1% to SRBA (indexation)
- Mandatory copies of documents: Birth Certificate, Marriage Certificate etc.....)
- Additional information in package

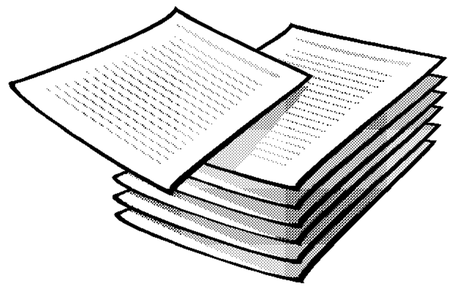


- **Purchase of Prior Service**
  - Prior employment with PS or other employers
    - » (ie: terms, COOP, other pensionable employment…)
  - Less expensive if done within first year
  - Additional information in package

- **Supplementary Death Benefit**
  - Life insurance
  - Twice your annual salary rounded up to the next $1000.
  - Monthly deduction based on salary and pensionable allowances
  - If CFSA recipient of annuity – need to cease coverage
  - Naming of beneficiary (SDB)
  - You can change beneficiary at any time
  - Monthly cost: .15 ¢ per $1000 coverage + sales tax

Pension Benefit Statement

- A statement is provided once a year to all employees detailing pension benefits

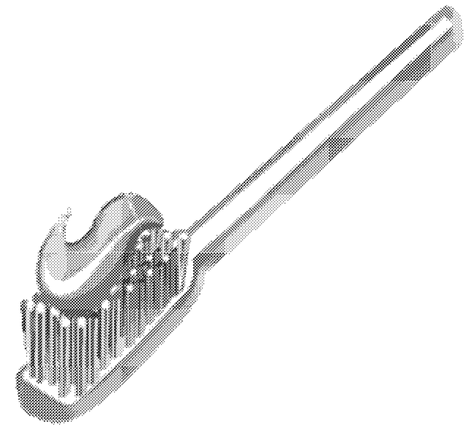


Disability Insurance (DI)

- Disability plan offered by Sun Life of Canada
- Monthly benefit may be paid for employees unable to work due to illness or injury
- 70% of your insured salary
- Monthly cost: $0,2415 per $1,000 of annual salary + sales tax
  - (Premium Holiday January 1st, 2011 to March 1, 2011)
- Waiting period – 13 weeks
- Additional information in package

Dental Plan

- **Employer Paid**
- Great West Life is the administrator
- Terms of > 6 months/indeterminate
- Eligibility: 3 month waiting period
- Coverage is extended to the employee's spouse and children under 21 years of age (25 years of age if attending school full-time).
- Annual deductible: $25 single and $50 family
- Certificate plan number – card in approximately 3 months
- Taxable benefit for Quebec residents
- Great West Life Website – sign up
- Co-ordination of benefits
- Additional information in package



Public Service Alliance of Canada (PSAC)

Public Service Alliance of Canada
Alliance de la Fonction publique du Canada

- Support unionized employees

- Additional information at fair (insurance, etc.…)

- Form to be completed

Monthly flat rate (March 1, 2011)	
UNI-01 to UNI-05	$ 42.90
UNI-06 to UNI-11	$ 77.08

Deduction Adjustment

First Pay Cheque / month	Second Pay Cheque / month	Third Pay Cheque / month
•PSHCP •Parking •OC Transpo Ecopass	•DI •SDB •Union Dues •Prior Pensionable Service	• Twice a year - fewer deductions

Deduction Adjustment – Accounting mechanism used by the pay system to equalize the net amount of your cheques

Voluntary Deductions

- Public Service Health Care Plan (PSHCP)
- Canada Savings Bonds Campaign
- Government of Canada Workplace Charitable Campaign
- Recreation Association (RA)
- Union sponsored insurance
- Fonds de solidarité FTQ
- Alterna Bank

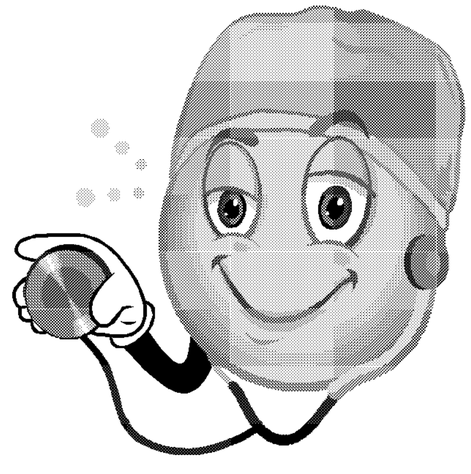
Public Service Health Care Plan (PSHCP)

- Optional insurance – Sun Life

- Provides coverage for the cost of prescription drugs, certain medical expenses and most hospital expenses

- Requirement: Provincial Health Plan

- Additional information in package



Public Service Health Care Plan (PSHCP)

- 3 Levels (Level I, II and III)
  - All the same for regular benefits (prescriptions ……
- Difference is hospital coverage

Public Service Health Care Plan

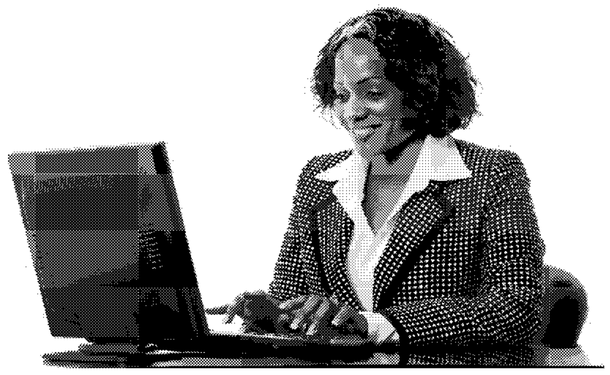
(premiums – June 1, 2012)

Levels and Daily Coverage	Level I $60.00 / day		Level II $140.00 /day		Level III $220.00 / day	
	Employee's Share	Employer's Share	Employee's Share	Employer's Share	Employee's Share	Employer's Share
Single	$0.00	$113.69	$1.10	$113.77	$5.31	$113.77
Family	$0.00	$113.70	$3.53	$113.77	$10.34	$113.77

- Application required – coverage 1st of month following application within 60 days of being eligible
- Certificate plan number – card in approximately 2 months
- Taxable benefit Quebec residents
- Apply today or sign waiver
- Co-ordination of benefits

PSHCP (Positive Enrolment)

- Mandatory to go on line to register yourself and your dependents
- Coverage will be refused if not done



OC Transpo Ecopass Program

- Program available at CSEC
- Cost savings
- Additional information in package

Benefits

- PeopleSoft
- Annual Leave
- Sick Leave
- Other Leave
- Designated Paid Holidays
- Leave Without Pay

PeopleSoft

- **Human Resource system at CSEC**
  - Personal Information (self-service)
    - Emergency contact
    - Change of address
  - Register your leave
    - Annual leave
    - Sick leave
  - View leave balances

Annual Leave

- Leave credits are based on your continuous /discontinuous years of service
- Advanced for current fiscal year - earned for months in which you receive at least 10 days pay
- Carry forward at year end to maximum 35 days
- For the first 6 months of employment, you may only apply for leave, which you have earned

ANNUAL LEAVE	
O to 7 years	15 days - 112.50 hrs
8 to 15 years	20 days – 150 hrs
16 years	22 days – 165 hrs
17 years	23 days – 172.50 hrs
18 years	25 days - 187.50 hrs
27 years	27 days – 202.50 hrs
28 years	30 days – 225 hrs

Leave

Sick Leave

- 9.375 hours per month for each month in which you receive at least 10 days pay (15 days per year or 112.5 hours)
- Accumulated each month
- Carry forward at year end

Designated paid holidays

- Entitled to pay for a designated holiday provided you are not on leave without pay the day before and the day after the holiday

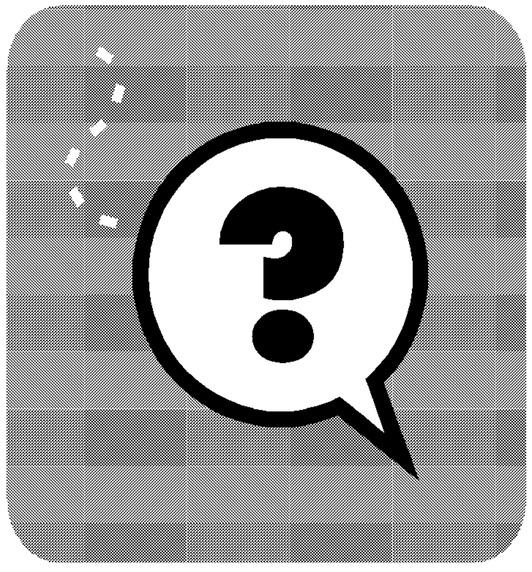
• Personal Needs Day
•Volunteer Day
• Family Related Responsibilities
• One Time Entitlement - 1 extra week

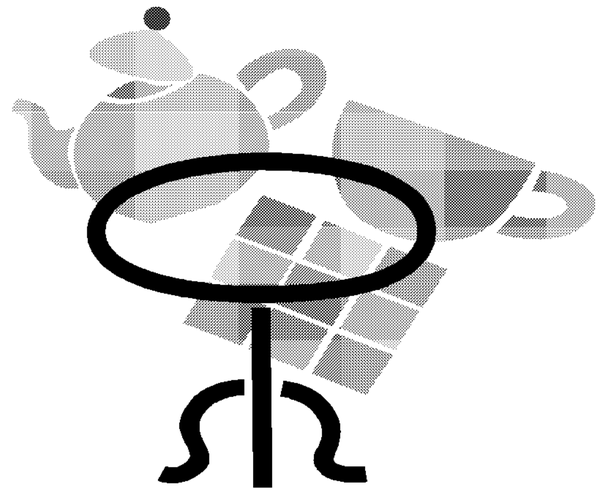
Leave Without Pay

- Different types of leave without pay are offered to CSEC employees
- All types are described in the collective agreement (maternity leave, parental leave, care of immediate family …..)
- Please contact your Compensation Advisor when you are considering any type of LWOP

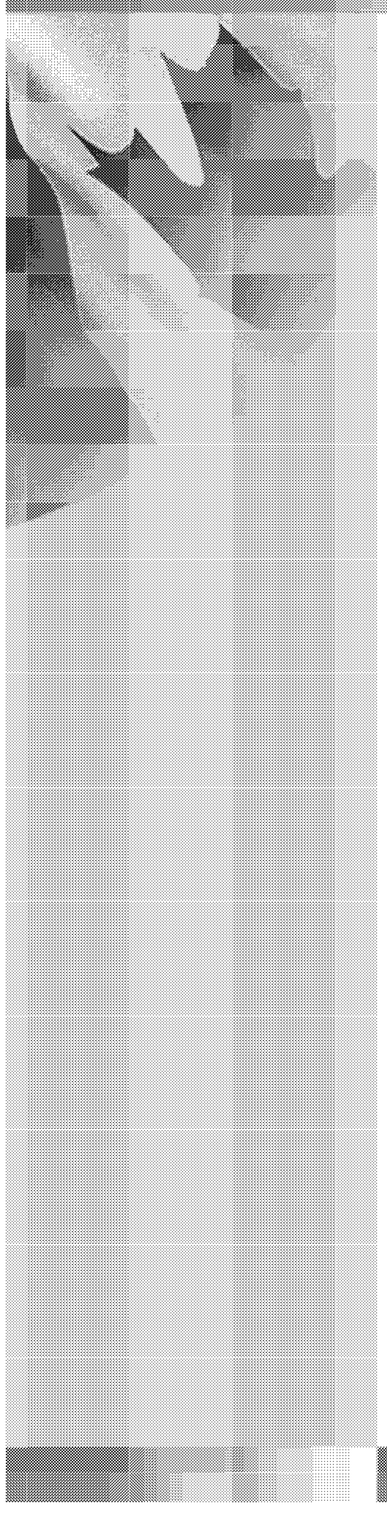
Reminder

- Any life events:
  - Marriage
  - Baby
  - Divorce
  - Resignation
  - New department
  - Etc.





Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



OPSEC Briefing

For New CSEC Employees

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

OPerations SECurity

- analytical process aimed at protecting information - generally **unclassified** - about your intentions and capabilities.
- affects activities or info that is observable to the public.
- requires identifying, controlling, and protecting indicators associated with our operations and plans.

Why OPSEC?

Some examples of OPSEC failures

- Purple Dragon: US bombing aircraft in Korean war downed because of pilots talking in mess halls, etc.
- Waco disaster: 200 uniformed and armed ATF officials show up at the local McDonalds for breakfast before heading off to the compound. (It just so happens, a Waco member was working in the restaurant when they showed up!)
- U.S. soldiers in Iraq suffering increased casualties after other soldiers post pics of damage to their vehicles on the Internet.
- Turkish military attache shot on Island Park Drive after taking exact same route, every day, at the same time.
- CNN's raw data feeds from Middle East back to Atlanta containing discussions between the reporters and Atlanta, indicating things like "Schwarzkopf told us we can film this info, but can't release it until after 2300hrs, when the troops will begin invading [Iraq]."

Why OPSEC?

Some examples of OPSEC success

- George W. Bush's first visit to Iraq! Didn't even tell his father why he wouldn't be coming over for Thanksgiving!
- Prince William spends night on London streets as a homeless person (reported by Guardian 1 week after the fact!)
- PM Harper's surprise visit(s) to Afghanistan

The Process:

- **identify the critical info**
- **identify the threat**
- **identify your vulnerabilities**
- **assess the risk**
- **recommend counter measures to reduce your *indicators***
- **then go back and look at the critical info and repeat the process.**

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

Indicators!

These are the organization's observable or detectable activities or information that can be pieced together to reveal sensitive info – clues to an activity:

Patterns: how we organize our equipment, relationships with other organizations, associations between events and individuals

Stereotypes: indicators associating certain names, insignia, etc, with specific events. (A bunch of women/men in dark suits, sunglasses, earpieces = ?)

Predictable actions: a quarterback blowing onto his hands every time he is about to throw a pass; a poker player who rubs her/his temple before every bluff.

Caveat!

- There is no such thing as an "OPSEC Violation"
- This presentation **does** provide guiding principles so that employees can judge for themselves how best to behave in contexts touching on the public venue
- This presentation **does not** provide concrete "do's" and "don'ts"

- *Key: Every situation is different:*
  - *Varying sensitivity levels of your critical information (travelling as a CSE employee, DND employee, as a private citizen)*
  - *Different adversaries (FIS, criminals, little-known neighbors)*
  - *Different contexts (shopping downtown, business travel to [redacted] business travel to [redacted] personal travel to [redacted]*

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

Online Work-related Activities

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

Google groups [ ] Search

hacking_sp

Description: hacking, exploit, bug, vuln, backbrack

Discussions: all 17 messages

Ref: Hacking past a password prompt
By Jack Bauer - Nov 6 2009 – 1 author – 0 replies
Can anyone tell me how I can hack past a password prompt? Just curious. Thanks.

Jack.Bauer@cse-cst.gc.ca

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

SpyNet!©

The place where spies meet!

Name: Bill Jones

Employer: Communications Security Establishment Canada

Work phone: 613-991-5555

Occupation: If I told you, I'd have to kill you…

Interests: [redacted]

Age: 49

Blood type: O pos.

Credit card number: Master Card – 8640 3123 9644

IQ: 49

Bill's friends:

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

A good idea?...from a CSEC [redacted] account?

Google

[redacted]

Search

Online [redacted] activities

- Maintain discretion on the Internet – unless you work in an area that deals with the public and have been properly trained on public relations

[redacted]

- Use prudence when surfing websites. The sites note and record who has visited.

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

The "INTs"

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

The better-known “INTs”

- SIGINT (Signals)
- HUMINT (Human sources)
- IMINT (Imagery)
- MASINT (Measurements and Signatures)
- OSINT (Open Source)

Unofficial OPSEC-related "INTs"

- Ego-INT
- Mall-INT / Bus-INT
- Faith-INT
- Restroom-INT
- Drunk-INT
- Trash-INT

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

EgoINT…a real life example…

The following is a rough layout of a conversation that was overheard in the waiting room of a local car dealership's service centre. Speaker "A" is a member of the Canadian Armed Forces in full-length flight overalls. "B" is a young woman behind the reception counter. The following is an approximation of one portion of that conversation that immediately piqued the interest of a CSEC employee who happened to be sitting in the waiting room. ***All details (aircraft make/model, callsigns, etc) have been changed for obvious reasons***:

EgoINT…a real life example…

- **CF person (A):** Yeah, the [redacted] has a [redacted]
- **Attractive young woman (B):** U-huh.
- A: And we gotta have the thing ready for Monday mornings in case he has to fly out. So that's Sunday night it has to be ready.
- B: Really?
- A: You know what the callsign is? It's [redacted]
- B: Hmmm.

EgoINT…a real life example…

- A: But he's got [redacted] other aircraft as well. [redacted] If it's not the [redacted] then it could be a [redacted] using them.
- B: Wow.
- A: So they always have to be ready. And you should see the insides of them. Really nice, lot's of leather. The food is incredible.
- B: Yeah?

- A: Yeah. Those are based in [redacted] You know, there's that area just west of the airport here in Ottawa, there used to be three hangars…now there's only two.
- B: Not really.

EgoINT…a real life example…

- A: Well, they're bringing on a new aircraft for the [redacted] and that's where they're outfitting it. It's a [redacted] It's a bit on the smaller side, but it's being converted into an [redacted]
- B: Oh yeah?
- A: Yeah. But you know what? – [redacted]

EgoINT…a real life example…

QUESTION

Why would any airman for the [redacted] aircraft talk about something like this to a stranger with no need-to-know? To be more exact: why would a young **male** speak so freely to an attractive young **female** about everything that he knows about [redacted] aircraft?

- If this weren't called "Ego-INT", what would you call it?

(…)-INT!

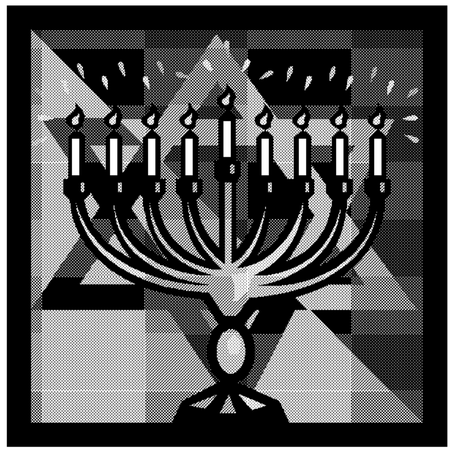
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

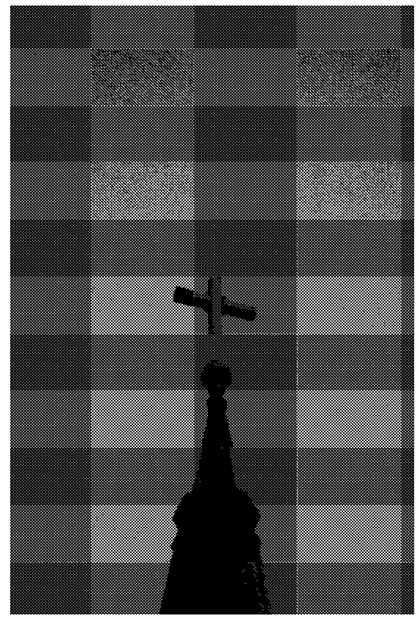
Mall-INT / Bus-INT

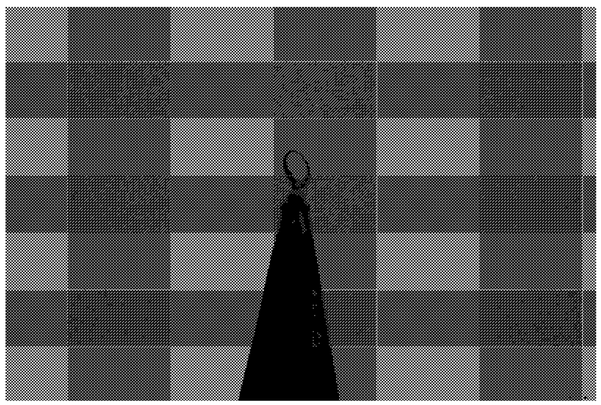
- It's a "CSEC Building Pass". Not a "*Billings Bridge Mall* Pass" or an "*OC Transpo* Pass"
- A knowledgeable adversary will identify you rather quickly
- Remove your building pass once you've left the premises

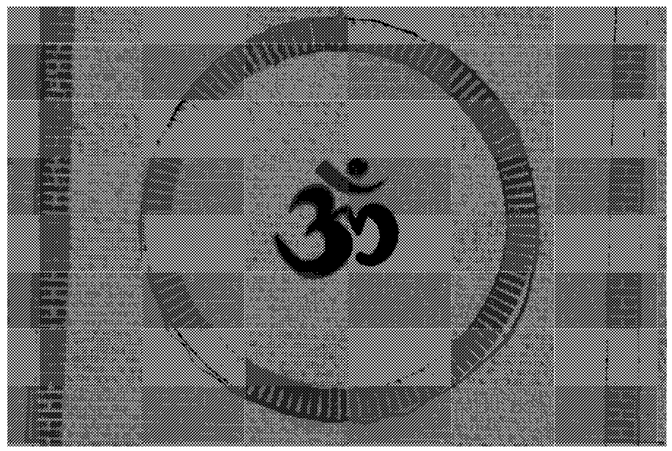
Faith-INT

- Social groups, functions at church, mosque, temple
- Wearing a CSEC t-shirt or ball cap to church / mosque / temple. Good idea?









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

Restroom-INT

- Restrooms are not offices or meeting areas!
- Who else is in the restroom?
- Use discretion…that is, unless your office or conference room looks like this…

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

Drunk-INT

- What stopped him from talking?

Conference-INT

- All those little groups of people who gather together in the lobbies and talk “cryptically”

- Some of the worst offenders: [redacted]

- You’re not in a secure environment. Exchange business cards and talk about the sensitive stuff later and through secure channels!

Trash-INT

- Your personal trash can be somebody else's treasure
  - Identity theft: credit card bills, old documents, receipts, health info
  - Attribution to intelligence: AMEX travel docs, e-tickets, receipts, etc
- Your workplace trash can lead to compromise:
  - Tossing classified waste in the recycling can
    - Documents
    - Equipment
    - Parts
    - Envelopes and other indicators that may reveal our partners outside CSEC

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

Trash-INT

Don’t invite a “Break & Enter”

Reduce the indicator!

Page 581

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c), 19(1), 15(1)

of the Access to Information

de la Loi sur l'accès à l'information

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

Contact The IOSS

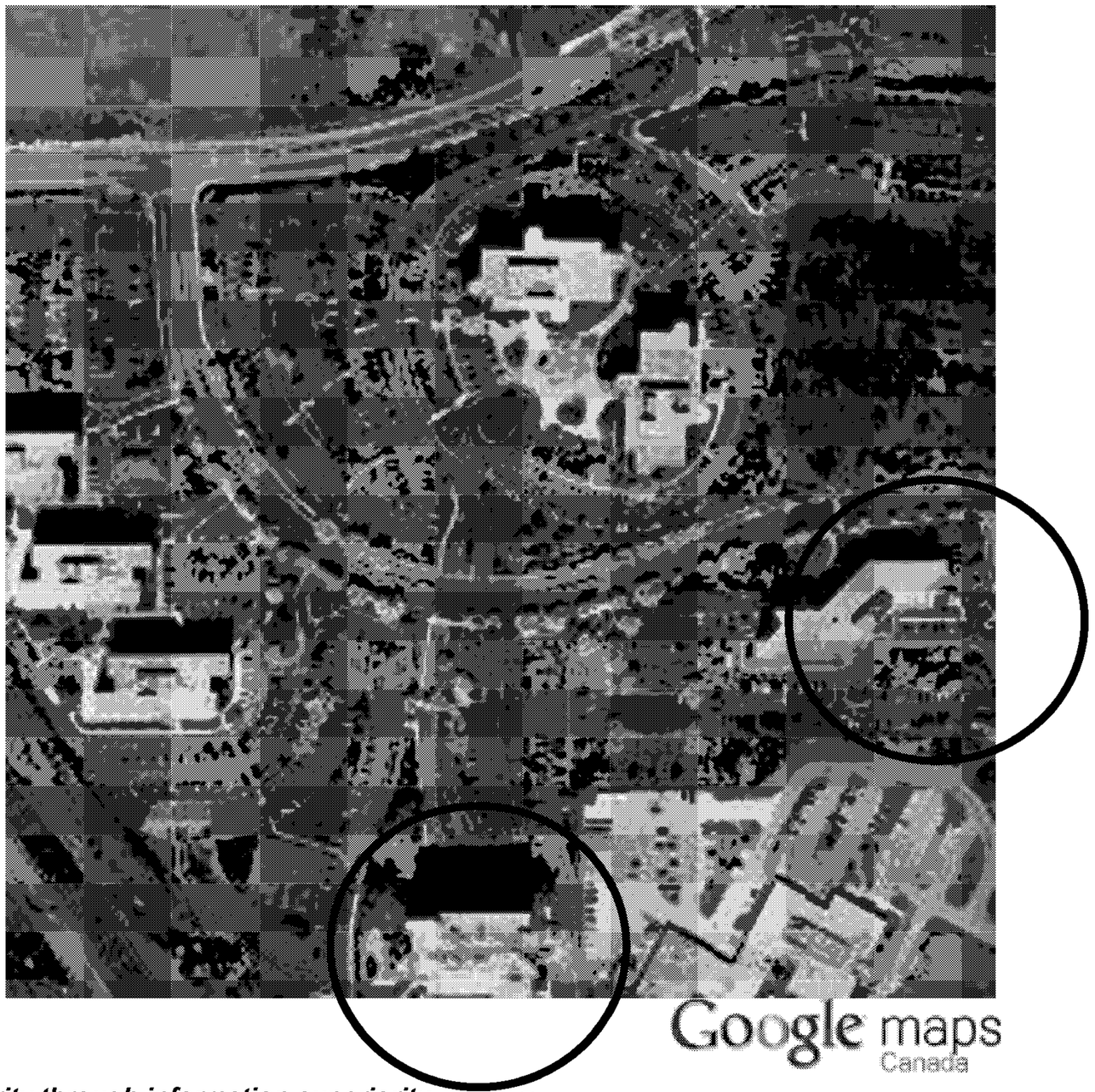
~~Address:~~
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770
(directions)

Phone Numbers:
(443) 479-IOSS (4677)
(443) 479-4701
DSN 689-4677

Fax Numbers:
(443) 479-4650 (secure)
(443) 479-4700 (unclassified)
Email:
ioss@radium.ncsc.mil

(…and what is the "IOSS?"…)

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



Source:

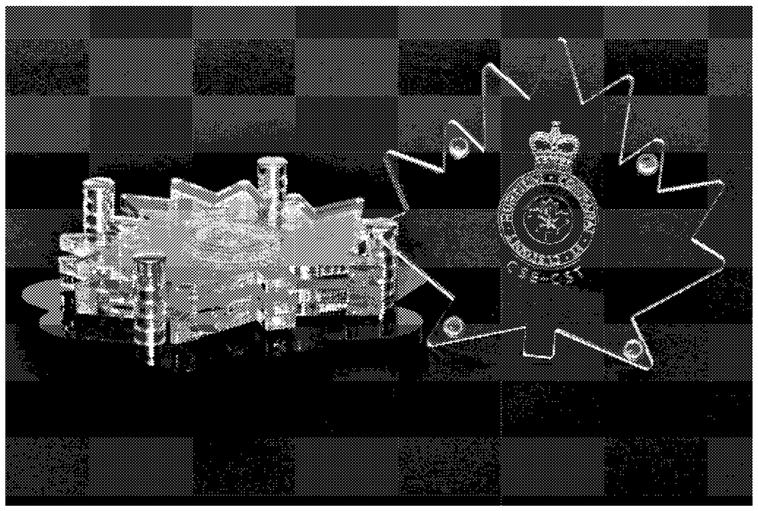
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Intelligence community memorabilia

- Indicators around the house: display with discretion.
- Assess where you are going to display it or wear it

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

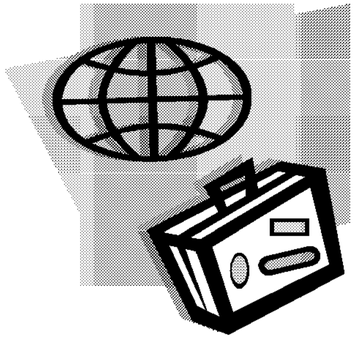
Memorabilia: around the house

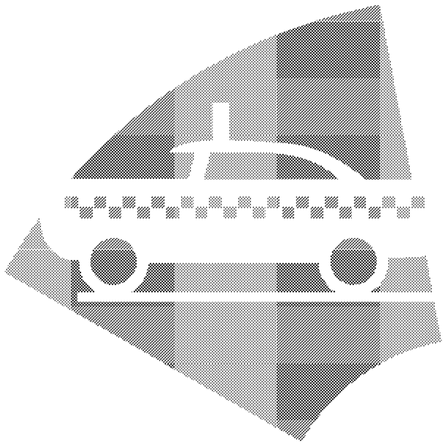


Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

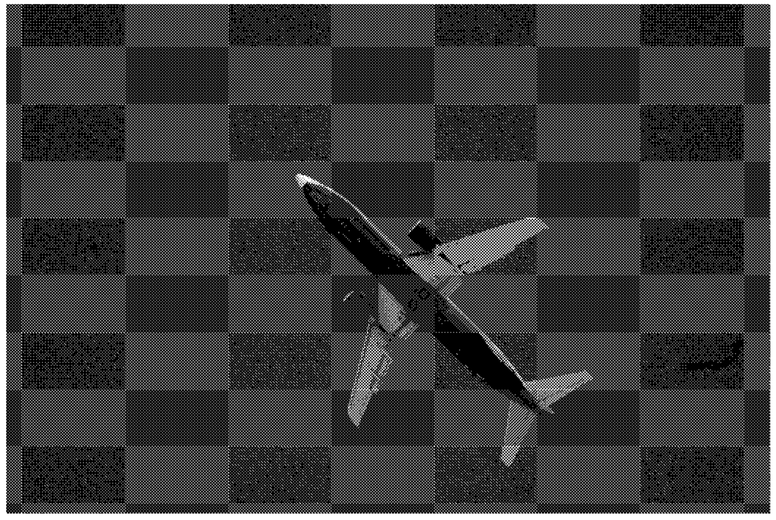
Canada

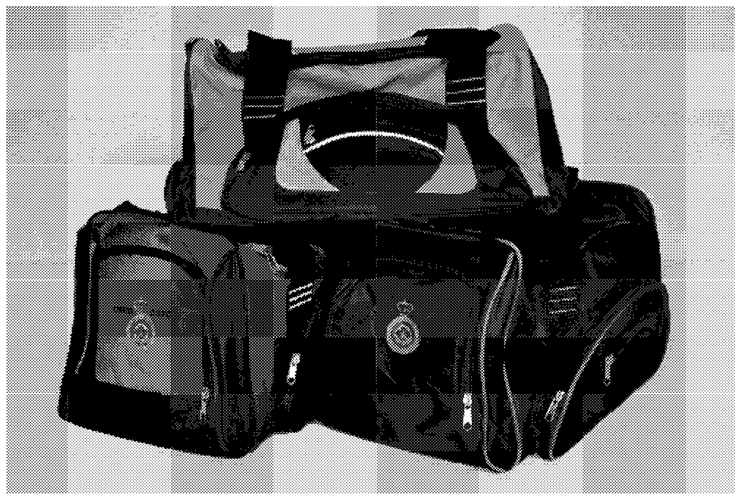
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

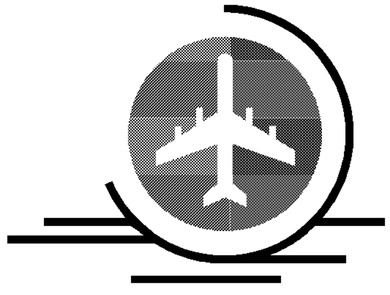




Travel





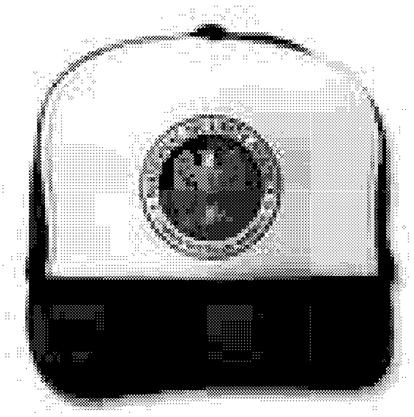


Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

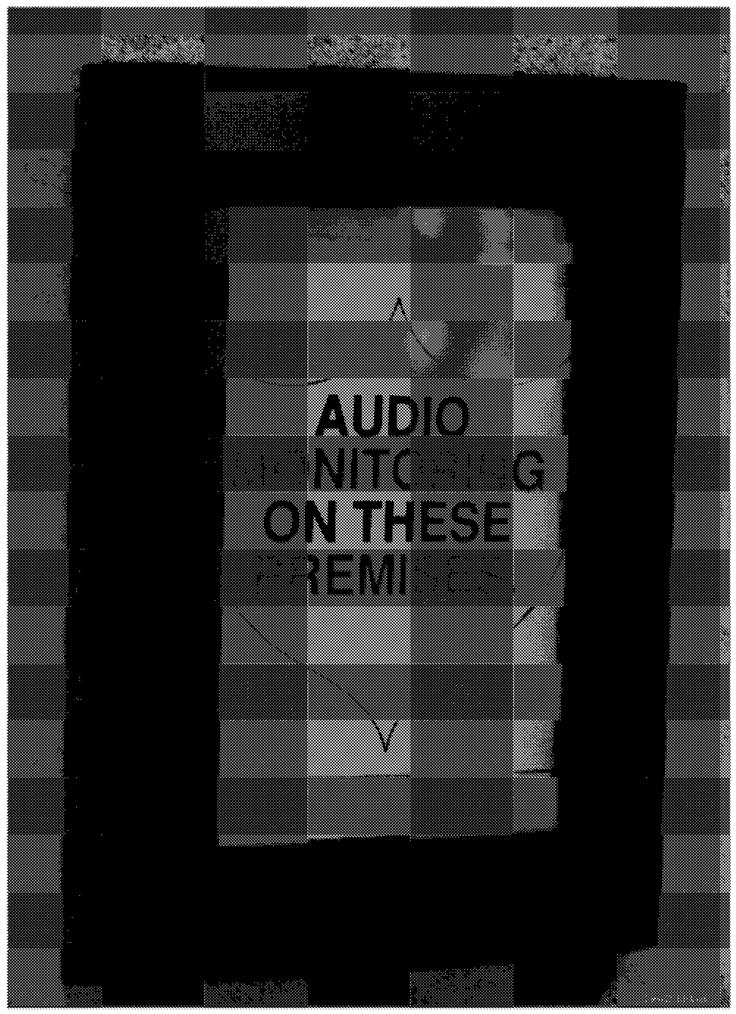
Attribution to CSEC / intel community

- Leave your CSEC, CSIS, NSA, DND, etc, memorabilia back home in Canada: you don't need to advertize your affiliation with an intelligence agency when you're beyond Canada's borders
- Bad mix: [redacted]



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

"Audio Monitoring on These Premises"



- Lobbies
- Elevators
- Hallways
- Washrooms
- Airports
- Shopping malls

Leaving your hotel room for an evening

- Indicators you can use to ward off others!
  - Leave on your television with the sound on: instils a sense of uncertainty within those in hallway who may be looking to break in.
  - Leave some lights on so they can be seen under the door.
- Try to avoid rooms on first floor of your hotel.
- Use room safe for valuables and other indicators.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

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

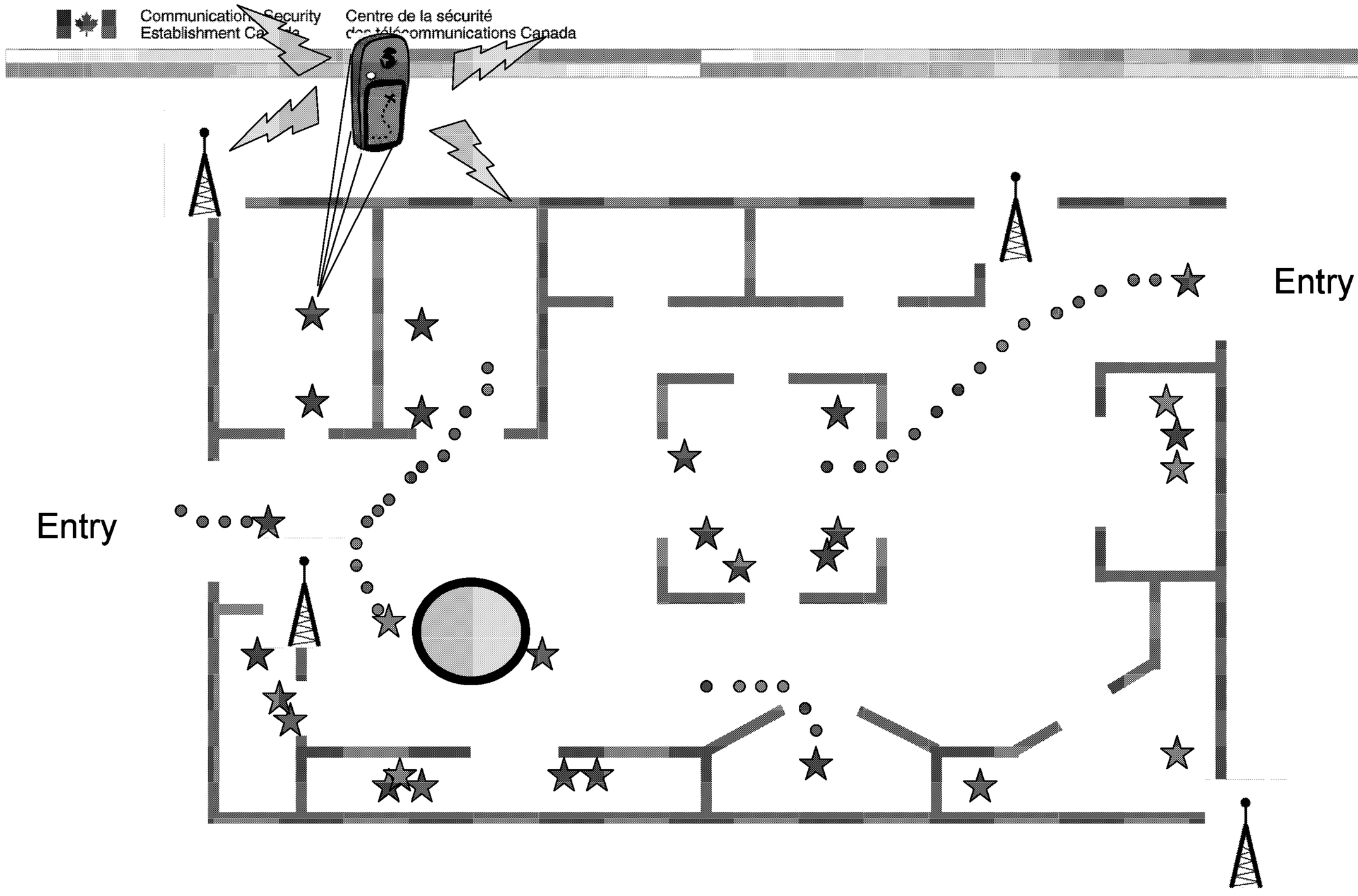
Cellular phone tracking

Your whereabouts tracked via cellular signals
vs
You sharing your whereabouts via social network sites

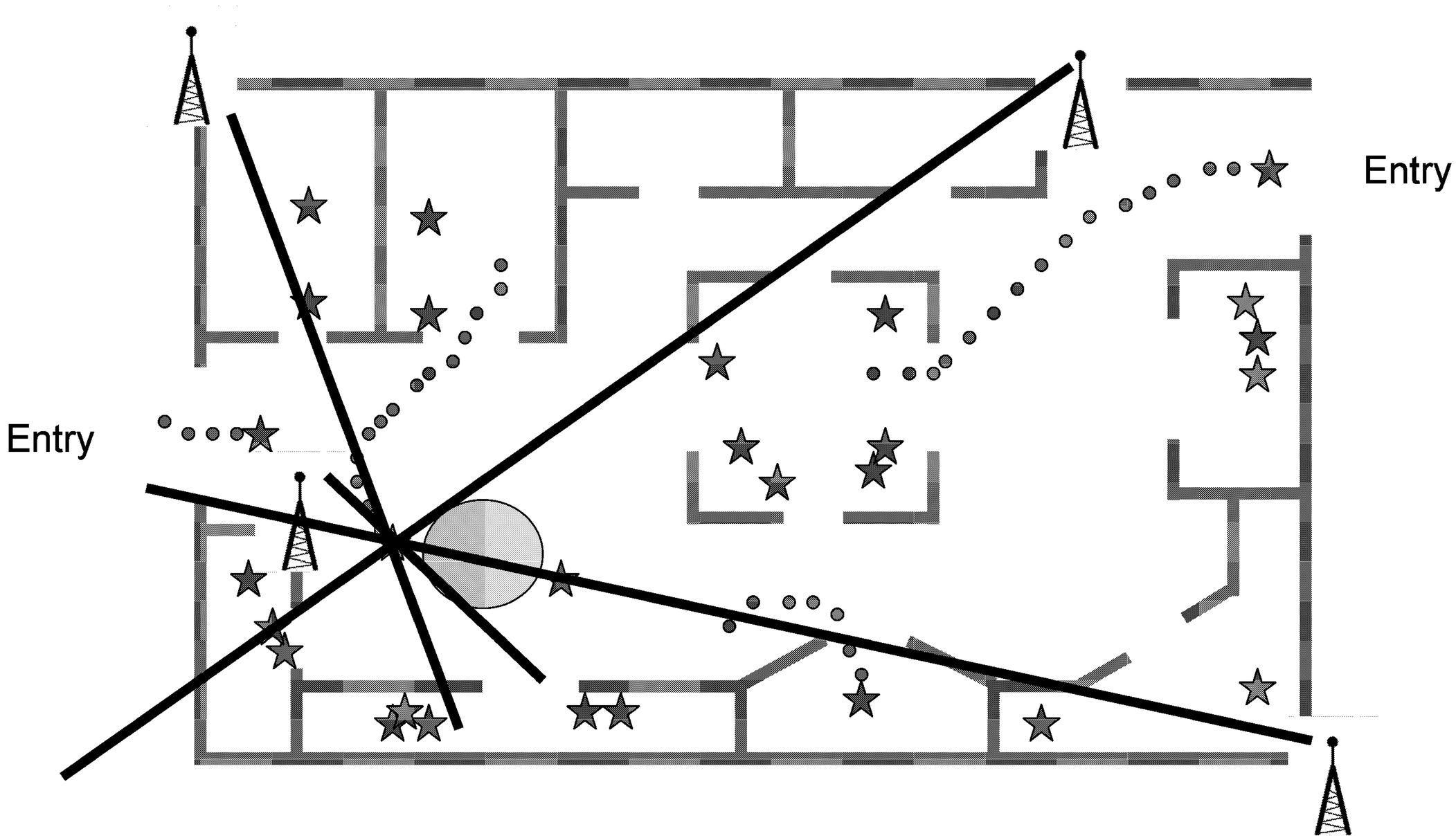
Geolocation-based companies

- Your PDA or cellular phone signal is an indicator
- Now emerging more and more as a profitable venture
- Sell human movement pattern info to real estate property holders
- The info helps determine which areas of a property are popular; which are not:
  - Shopping malls
  - Airports
  - Neighbourhoods

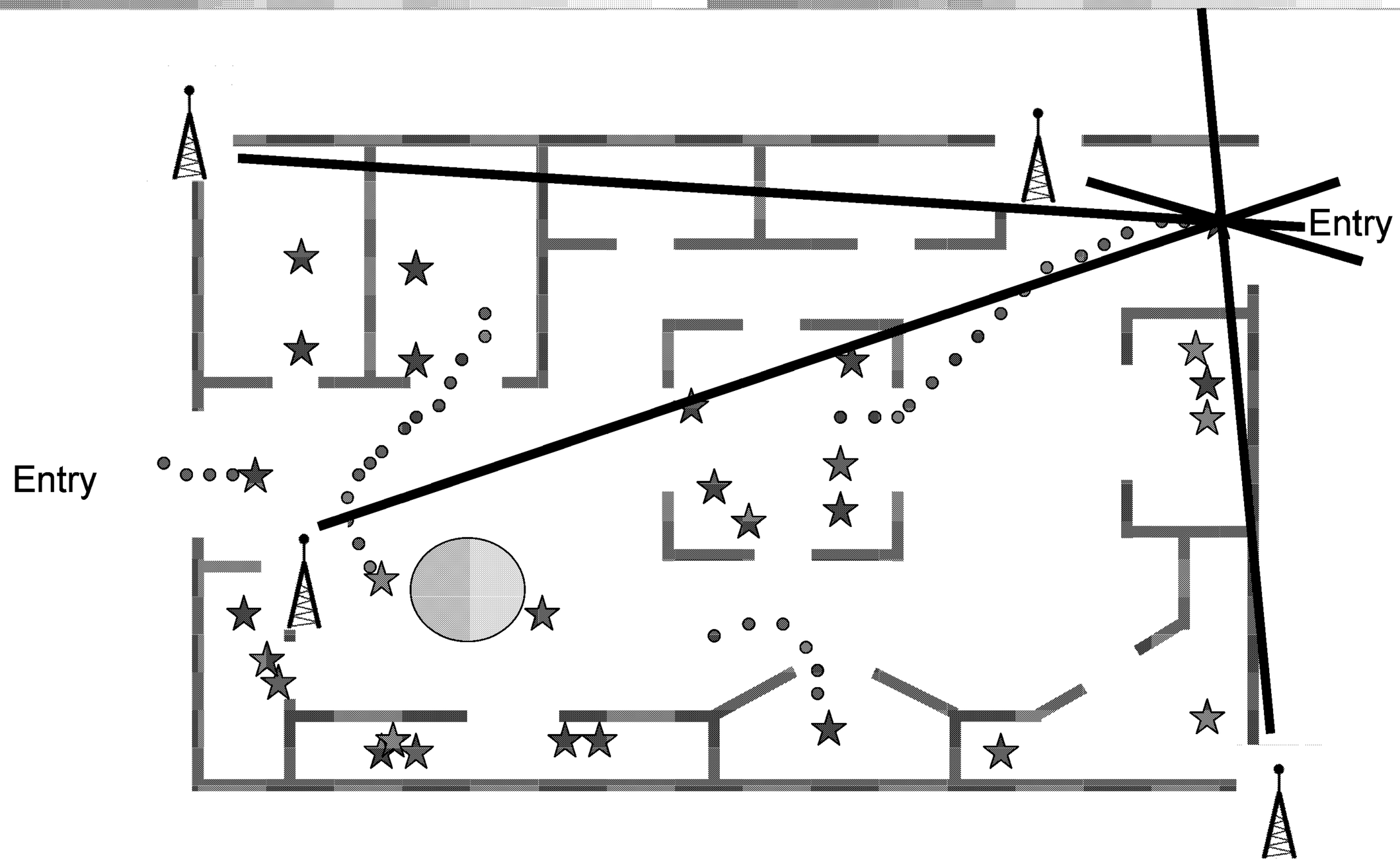
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada



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



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

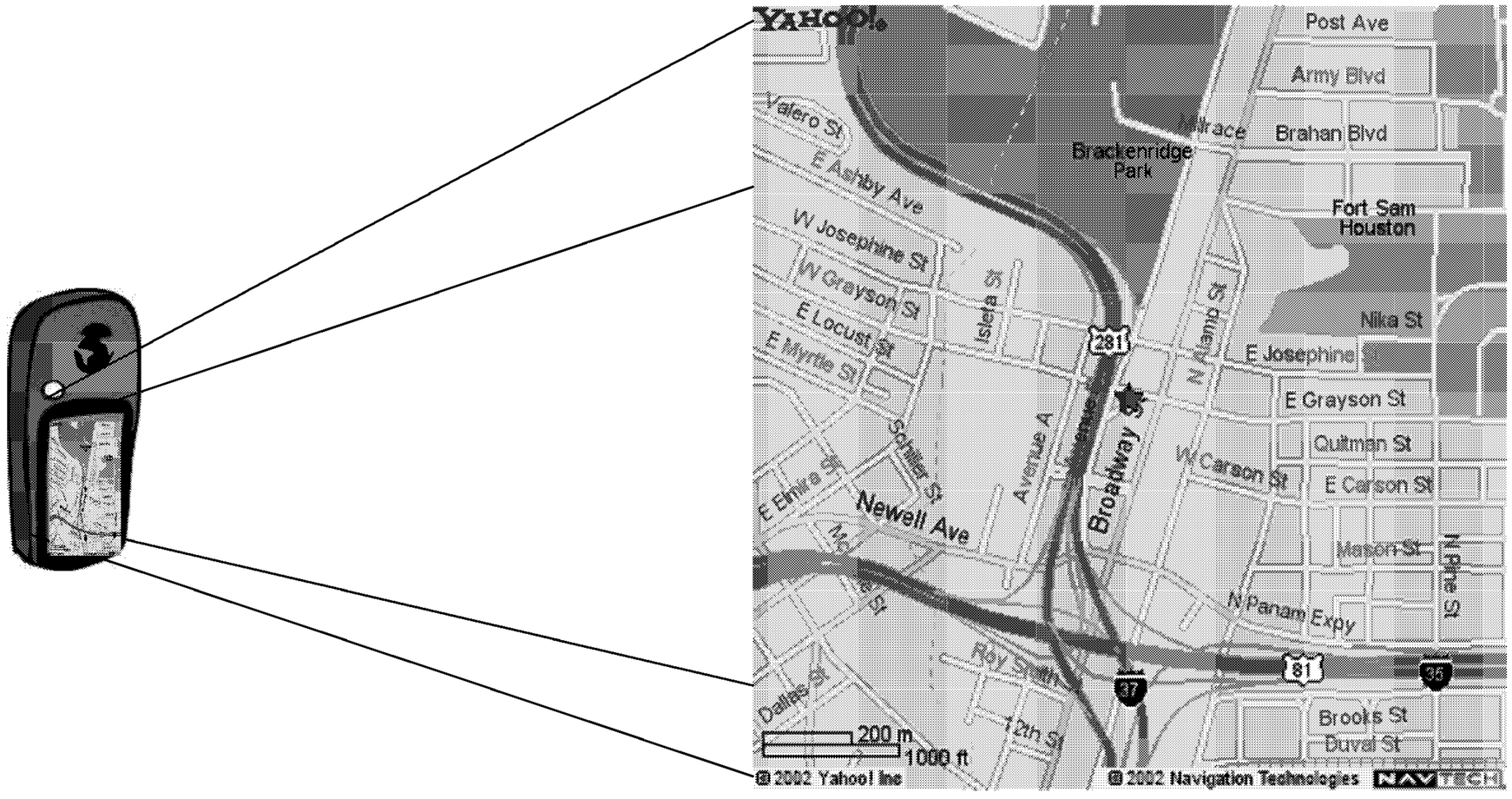


Who else can track cell phones?

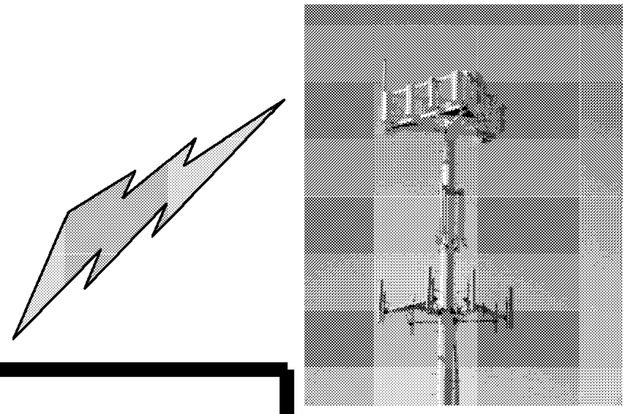
- Foreign governments
- The private companies who set these systems up
- Communications hobbyists
- Terrorists
- Organized crime

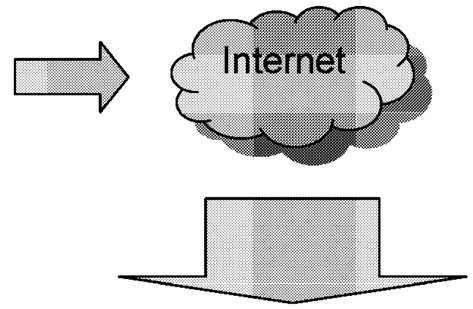
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

What your PDA shows you

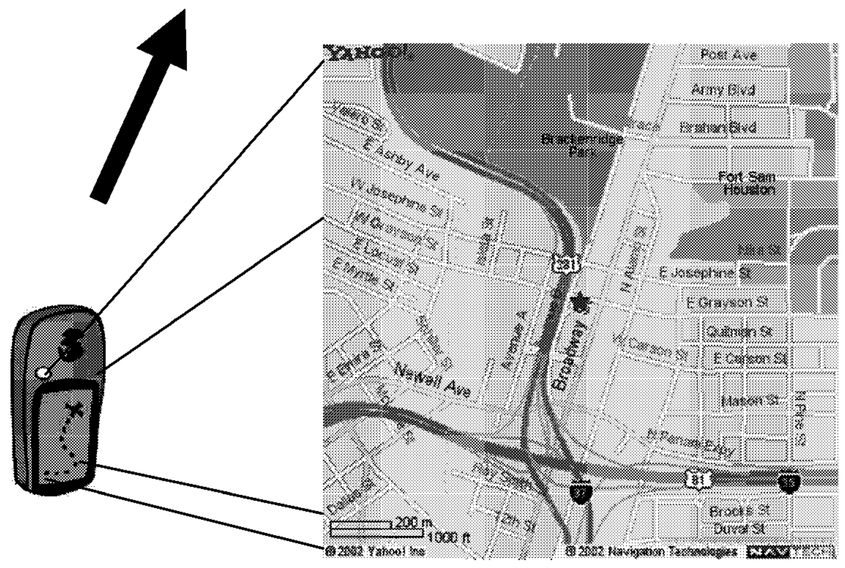


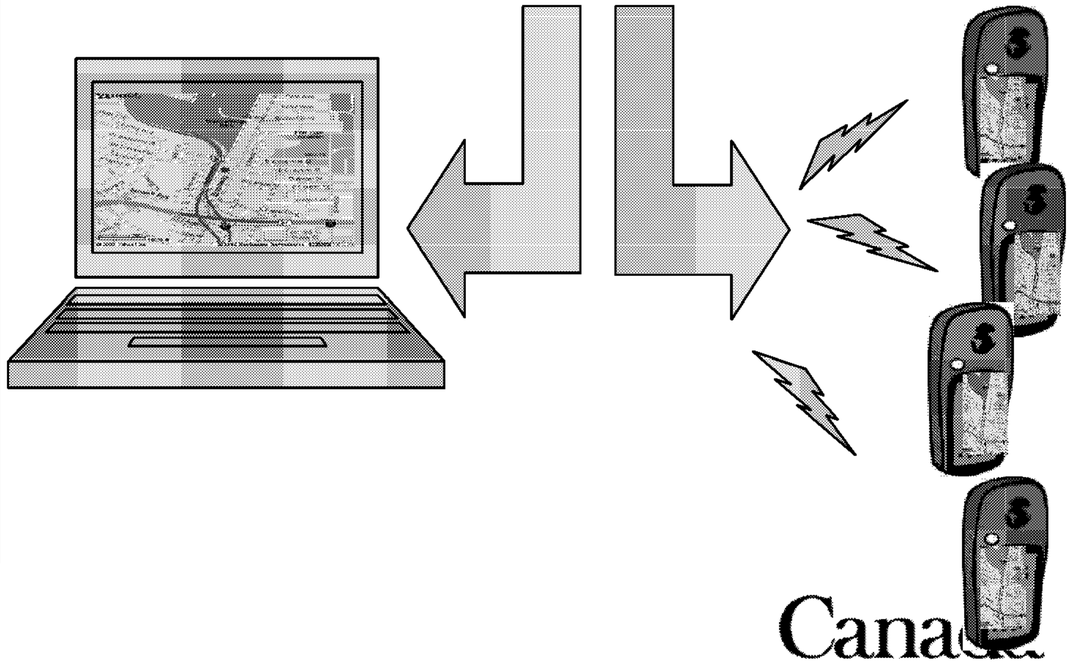
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada





Service's proprietary software installed on phone





Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Review

- **OPSEC: failures vs successes**
- **The OPSEC Analytical Process**
- **No such thing as an *OPSEC violation***
- [redacted]
- **Online work-related activities**
- **The "INTs" and "Triggers"**
  - **Ego-INT, Mall-INT, Bus-INT, Faith-INT, Restroom-INT, Drunk-INT, Conference-INT, Trash-INT**
- **Intelligence community memorabilia**
  - **During travel; around the house**
- **Travel (hotels, lobbies, room security)**
- **Cellular phone tracking**

Contact info

Questions about today's presentation:

[redacted]

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

CSEC Relationship with CSIS

[redacted]

Canada

Overview

- Background
  - Who is CSIS?
  - What does CSIS do?
  - Oversight
  - Structure
- Areas of CSEC / CSIS collaboration
  - Operational support
  - Investigations
    - Section 12 – Threats
    - Section 16 – Foreign Intelligence

Who is CSIS?

Canada's national security intelligence agency

- Established by CSIS Act in 1984
  - A civilian organization
- Work is preventive
- No power to arrest or detain

What does CSIS do?

Mandate

- We investigate threats
- We collect and analyze information
- We produce intelligence reports
- We advise the Government of Canada
- We provide security assessments

Threats to the Security of Canada

Threats – Defined in Section 2, CSIS Act

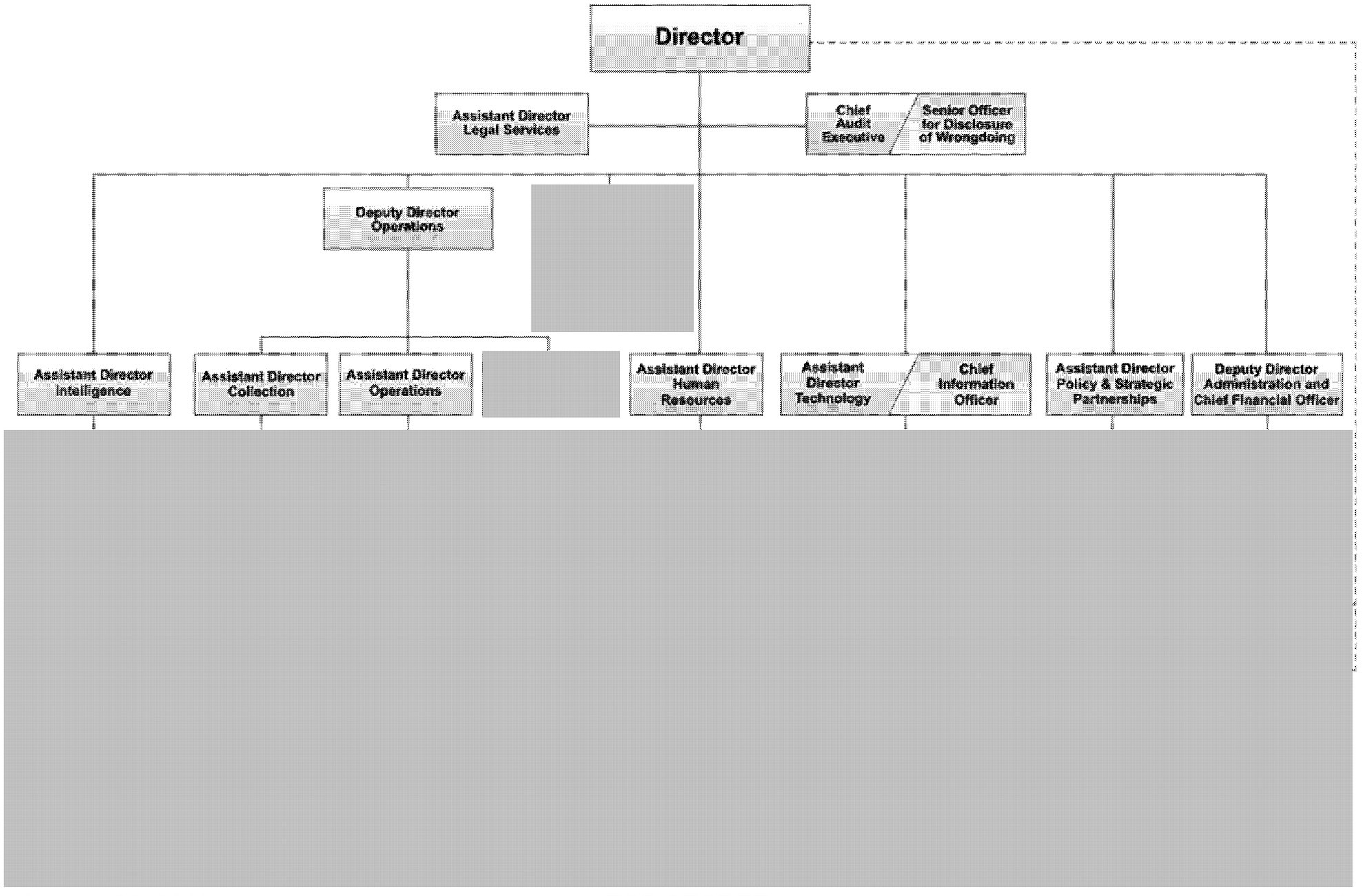
- Espionage or sabotage
- Foreign influenced activities
- Terrorism / ideologically motivated violence
- Subversion

Investigation of these threats is mandated by Section 12

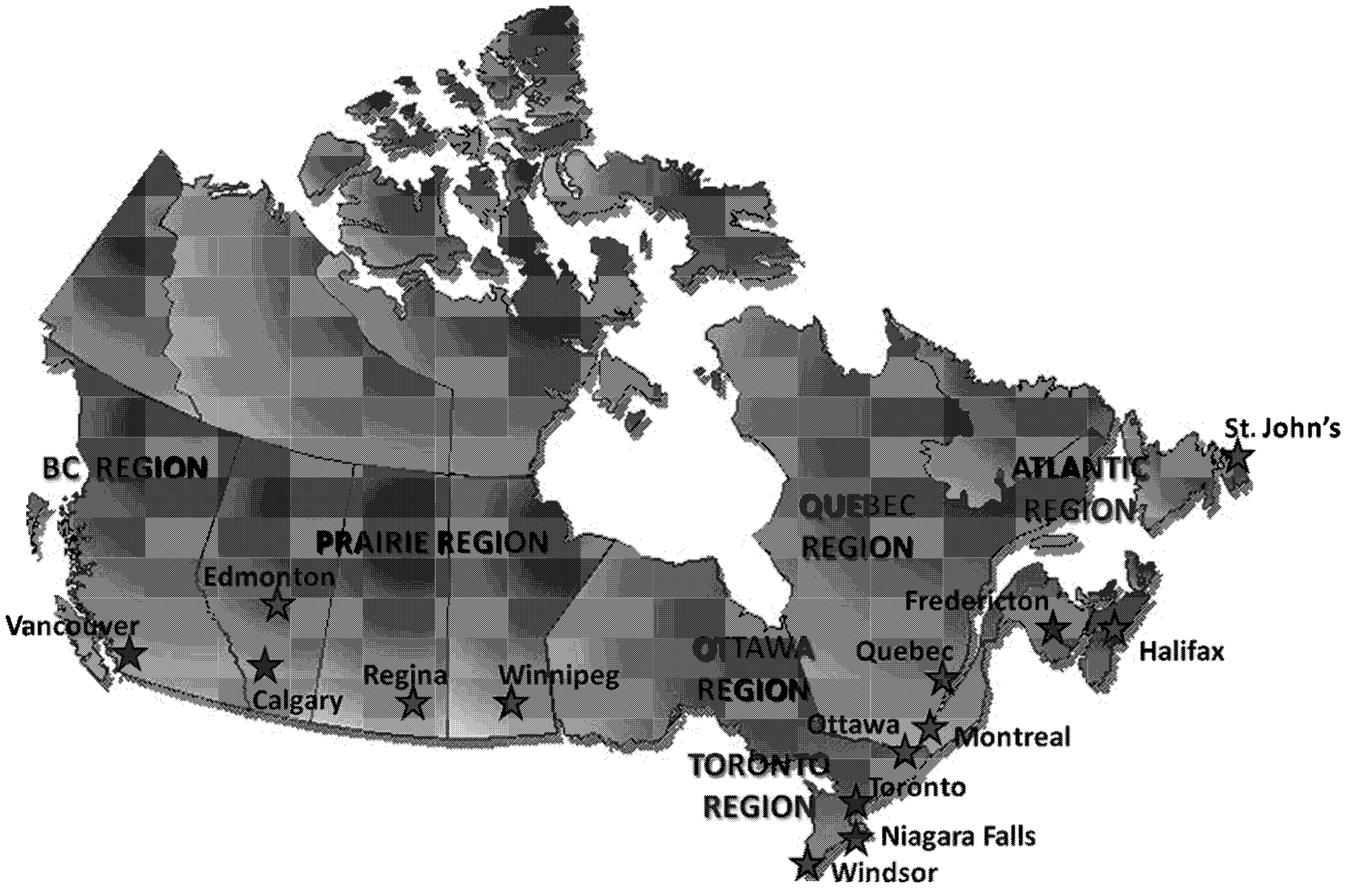
Security Intelligence Review Committee (SIRC)

- Reviews performance of duties and functions
- Conducts reviews in response to complaints
- Monitors compliance with operational policies
- Reviews operational activities

CSIS Structure



CSIS Across Canada



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

How CSEC Helps – Operational Support

CSIS Operational Support Branches:

[redacted]

- Security Screening

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

How CSEC Helps – Investigations

HUMINT: Focus on human sources, [redacted]

[redacted]

SIGINT assists HUMINT investigations through:

[redacted]

Investigations – Section 12

CSEC / CSIS Collaboration

- Ad hoc support for [redacted] collection
- Formal mechanisms
  - Mandate C / Support to Lawful Access (SLA)
  - Domestic Interception of Foreign Telecommunications and Search (DIFTS)

Investigations – Section 12

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

Case Study:

[redacted]

Mandate C / Support to Lawful Access (SLA)

CSIS

- CSIS *can* target Canadian citizens as well as foreign nationals visiting Canada

[redacted]

CSEC

- CSEC *can* target foreign nationals abroad, but *not* within Canada
- CSEC *cannot* target Canadians, anywhere

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

Examples of SLA Activities

[redacted]

- DIFTS

Domestic Interception of Foreign Telecommunications and Search (DIFTS)

- CSIS warrant power

[redacted]

Page 616

is withheld pursuant to sections

est retenue en vertu des articles

15(1), 16(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Investigations – Section 16

CSEC / CSIS Collaboration

- Section 16 relates to the collection of foreign intelligence *within Canada*

[redacted]

- Includes:
  - Support to Lawful Access (SLA)

[redacted]

Pages 618 to / à 621

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 16(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Emerging Opportunity

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

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Questions?

Canada

The Canadian Forces and the Integrated Signals Intelligence Operational Model

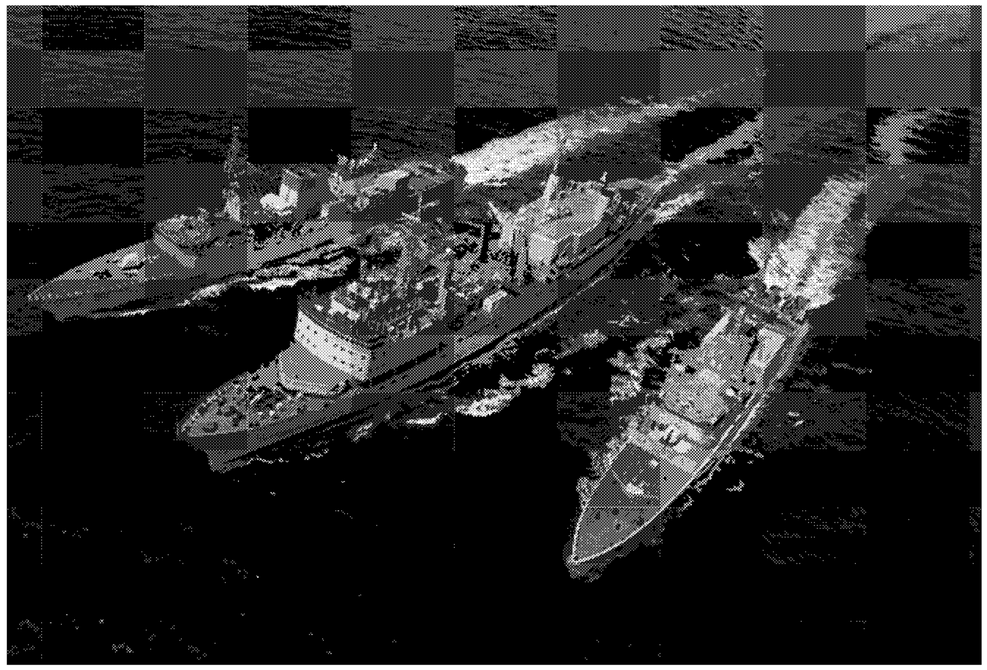
Captain Kevin Klein, Farid Yaghini and [redacted]
Office of Director General Military SIGINT
23 November 2012

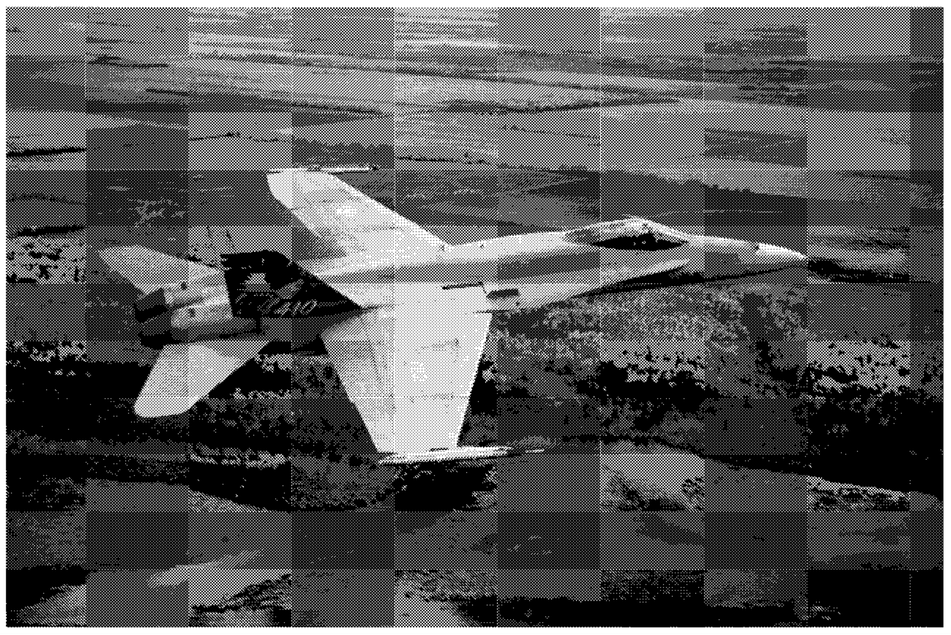
The overall classification of this presentation is TOP SECRET SPECIAL INTELLIGENCE

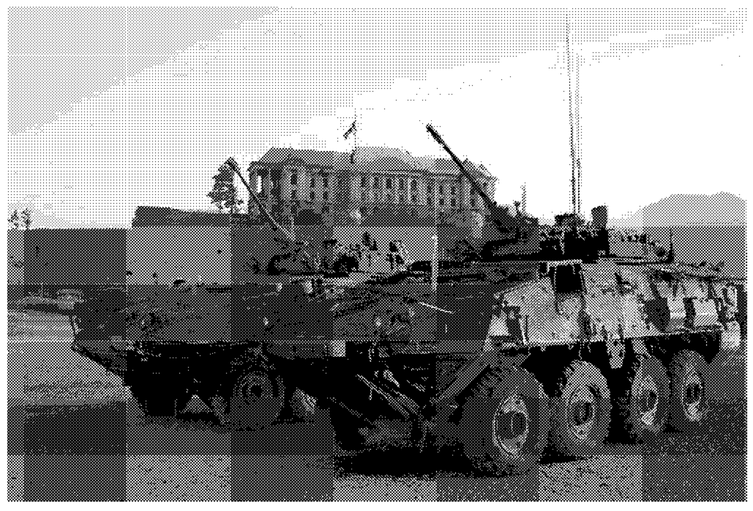
The Canadian Forces (CF)

Aim:

To provide you with a quick overview of the Canadian Forces and its relationship with CSEC.







The Canadian Forces (CF)

65,000 – Regular Force Members

25,000 – Reserve Force Members (4, 000 - Rangers)

28,000 - Civilians

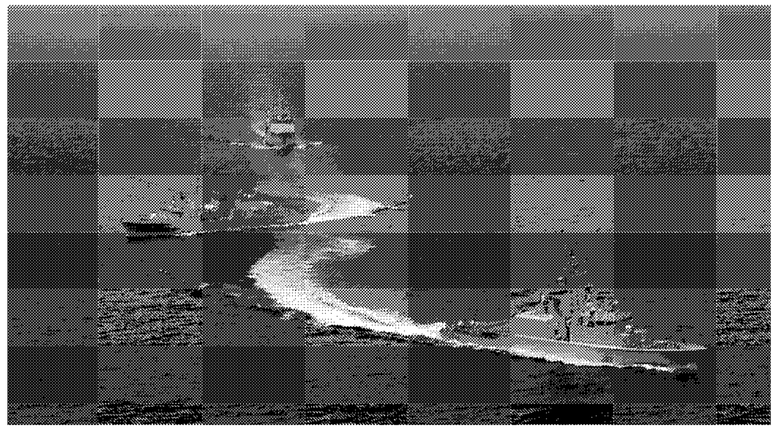
Mandate

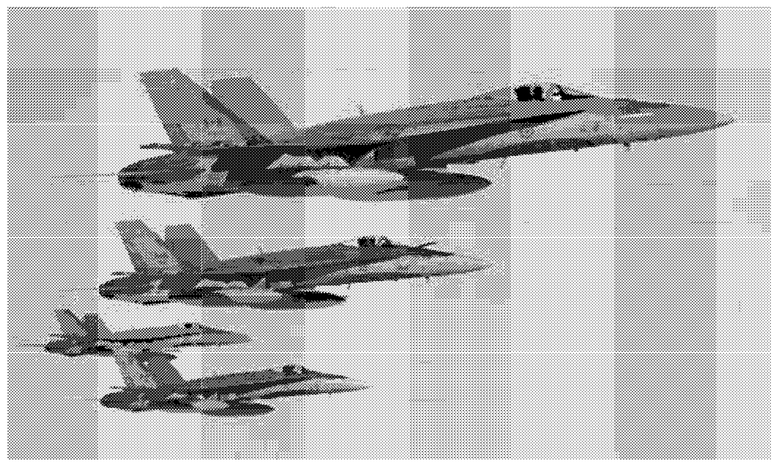
- Protecting Canada and defending our sovereignty.
- Working with closest ally, the U.S., to defend North America.
- Contribute to international peace and security through operations around the world.

The Canadian Forces (CF)

Three Elements:

- Navy
- Army
- Air Force





The Canadian Forces (CF)

Operational Commands:

- Canada Command (Canada COM)
- Canadian Expeditionary Force Command (CEFCOM)
- Canadian Special Operations Forces Command (CANSOFCOM)
- Canadian Operational Support Command (CANOSCOM)

The Canadian Forces (CF)

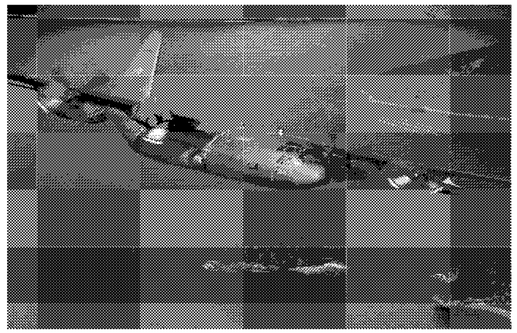
Transition:

- Canada COM
- CEFCOM
- CANOSCOM

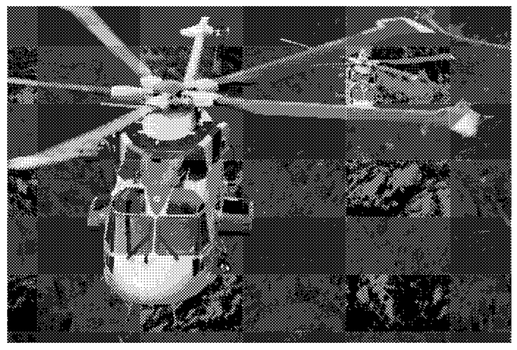
Canadian Joint Operations Command (CJOC)

Domestic Roles

- Provide surveillance of Canadian territory and air and maritime approaches.



- Maintain search and rescue response capabilities – anywhere in Canada on a 24/7 basis.



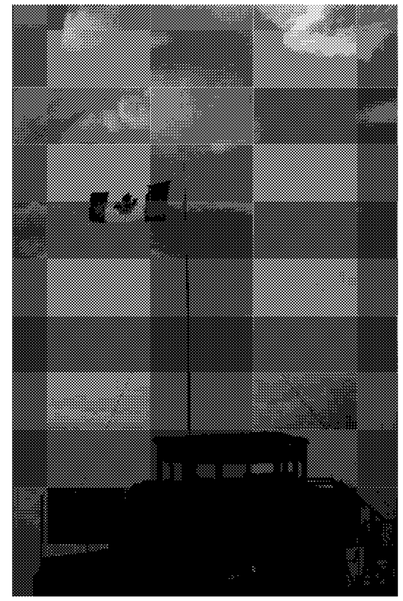
- Assist in civil authorities in responding to a wide range of threats – from natural disasters to terrorist attacks.

International Roles

- Maintain combat-capable units at high rate of readiness.

- Provide deployed forces with right mix of equipment to take part in full spectrum operations (from countering asymmetric threats to reconstruction efforts).

- Work closely and develop a coherent strategy with departmental partners



National Operations and Exercises

- Op ASSISTANCE

- Op PODIUM

- Op CADENCE

- Op NANOOK

CF DEPLOYMENTS
Military Pers Deployed Effective – 13 Aug 2012

CFICC • CCIFC

Legend
Region 1 – 5 Ops
Region 2 – 2 Ops
Region 3 – 8 Ops

TF BALKANS (OP KOBOLD)
NATO HQ - Kosovo: 5

TF JERUSALEM (OP PROTEUS)
MEPP – Jerusalem : 19

TF GOLAN HEIGHTS (OP GLADIUS)
UNDOF – Golan : 3

TF MIDDLE EAST (OP JADE)
UNTSO – Middle East: 8

TF ARTEMIS (OP ARTEMIS)
HMCS CHARLOTTETOWN
CMF-CTF 150: **267**

TF CYPRUS (OP SNOWGOOSE)
UNFICYP – Cyprus: 1

TF EL GORAH (OP CALUMET)
MFO - Sinai, Egypt : **41**

TF HAITI (OP HAMLET)
MINUSTAH: 5

JTF AFGHANISTAN (OP ATTENTION)
ISAF/ NTM-A: **864/852/694**

TF FREETOWN (OP SCULPTURE)
IMATT – Sierra Leone: 10

TF TAMPA (OP FOUNDATION)

Liaison Team – Tampa :	4
NAVCENT: Bahrain – UAE:	3
AFCENT: Al-Udeid	5
Sub-Total:	12

TF DRC (OP CROCODILE)
MONUSCO – DRC : 9

TF TRIPOLI (OP LOBE)
18

TF SOUTH SUDAN (OP SOPRANO)
UNMISS – Sudan : 14

TF NORTHWOOD (OP ARTEMIS)
Various Locations: 3

FORCE COMMITMENT

Number of Operations: 15
Total Pers Deployed: 1279

SECRET – NATO

000635

SIGINT & The Canadian Forces

- CF SIGINT Requirements
  - Timely
  - Contingency planning based
- Clients (CDI/ECS/CEFCOM/SOFCOM/Deployed Commanders/NORAD/5-Eyes/SIGDASYS/ LEA)
- Deployments – Force protection (Life or death)
- CF SIGINT component - Canadian Forces Information Operations Group (CFIOG)

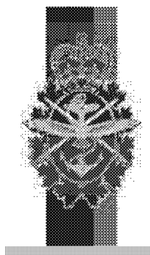
Canadian Forces Information Operations Group (CFIOG)

Mission:

To coordinate, develop and employ assigned Information Operations enabling capabilities for the Canadian Forces and the Department of National Defence.

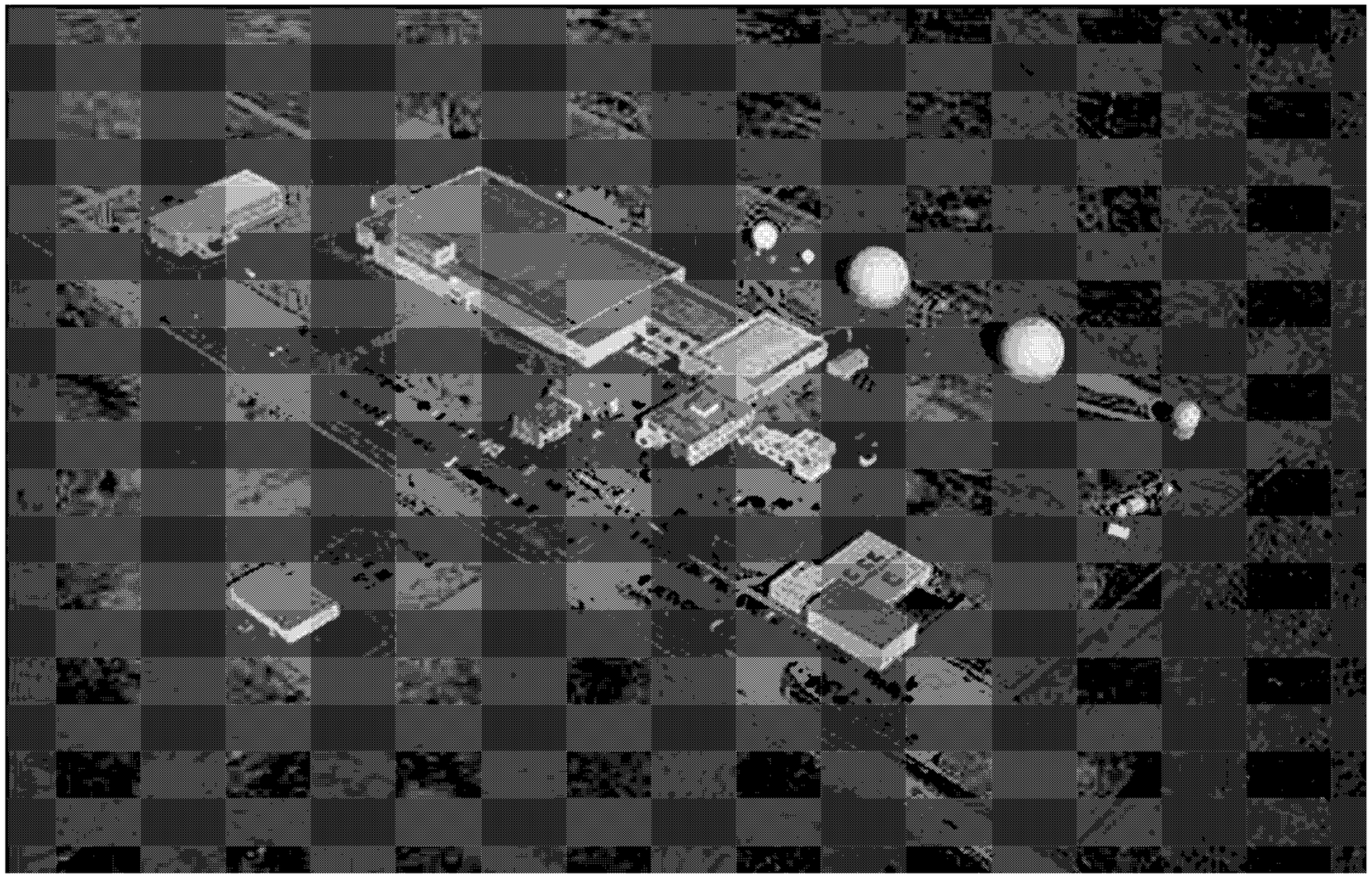
CFIOG Units

- Canadian Forces Electronic Warfare Centre (CFEWC)
- Canadian Forces Networks Operations Centre (CFNOC)
- Canadian Forces SIGINT Operations Centre (CFSOC)



CFIOG – Working With our Allies

Canadian Forces Station (CFS) Leitrim



Page 642

is withheld pursuant to section

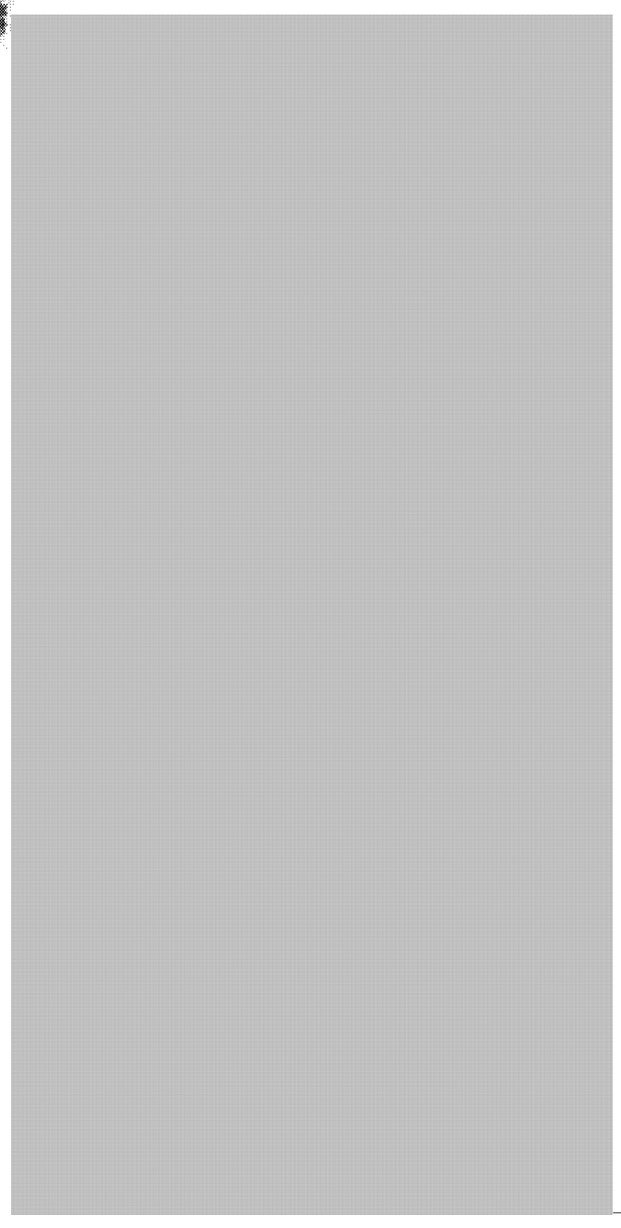
est retenue en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

CF Deployed SIGINT and Electronic Warfare Capability



RC(S) SIGINT & EW Architecture

Integrated SIGINT Operational Model (ISOM)

Aim

- The purpose of this presentation is to inform you about ISOM:
  - What is ISOM?
  - History
  - Future

What is ISOM?

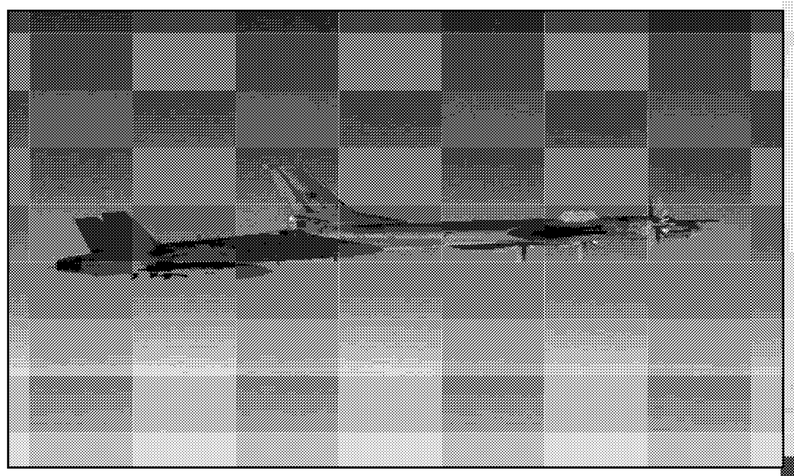
Integrated SIGINT Operational Model = One Canadian SIGINT Mission

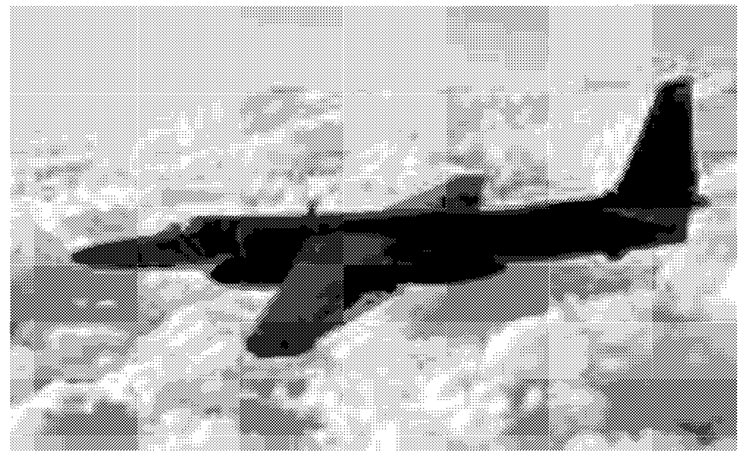
- [redacted]
- [redacted]

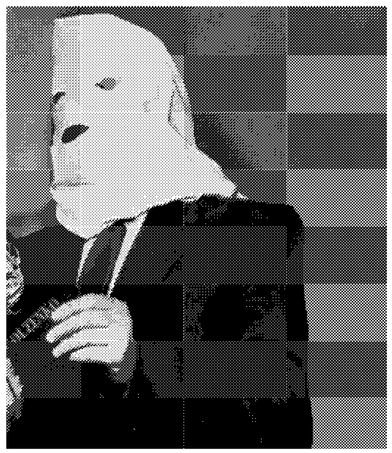
World War II

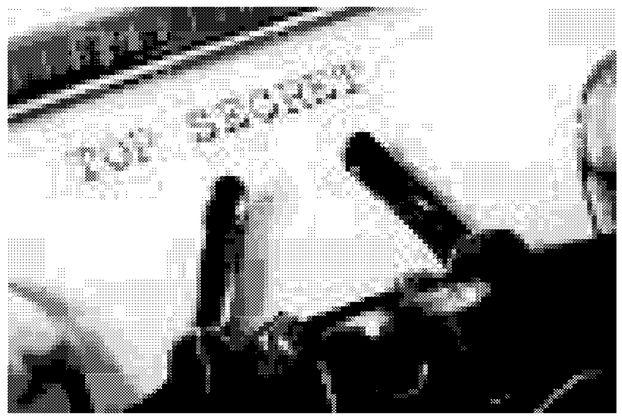
CFS Leitrim Circa 1940s

Cold War





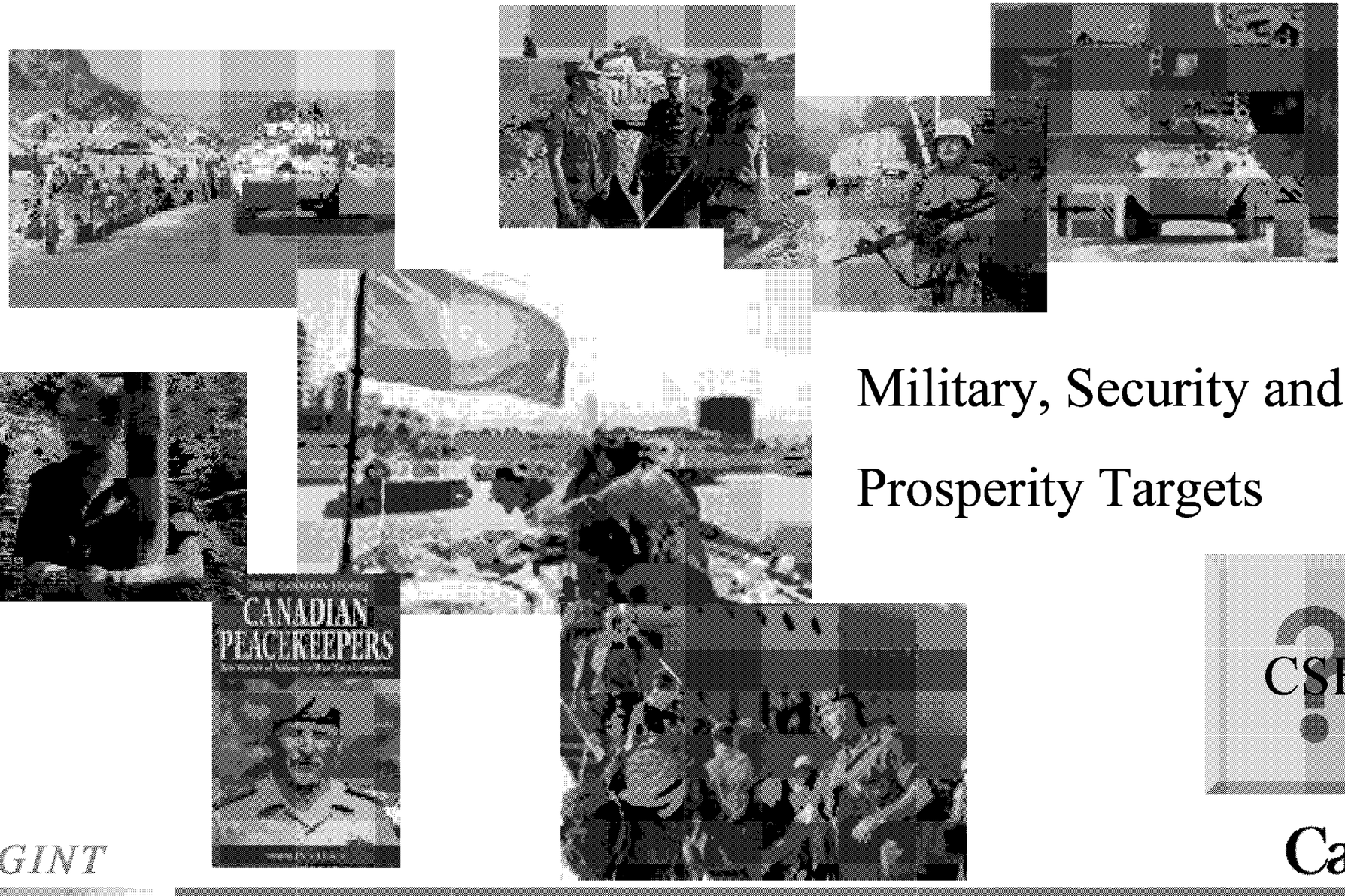




1989 – Fall of the Wall

1990s

International Peacekeeping



Military, Security and Prosperity Targets

CSE

Canada

SIGINT

1998

- CSEC responding to broad Government priorities (not security, only 3% of reporting security related)

- CFIOG established to focus on direct CF military support

For the survival of both organizations

9/11

War in Afghanistan

- Op Apollo (2001 - 2003) – Canada's contribution to the War on Terrorism – Southwest Asia, Khandahar Afghanistan & areas.
- Op Athena (2003 - 2005) – Kabul, Afghanistan
  (2006 - 2011) – Khandahar, Afghanistan
  | International Security Assistance Force (ISAF)

- Op Archer (2005 - 2011) – Canada's participation in Op Enduring Freedom (OEF), the US led multinational effort to assist the Afghan Ministries of Defence and Interior.

SIGINT

Canada

[redacted]

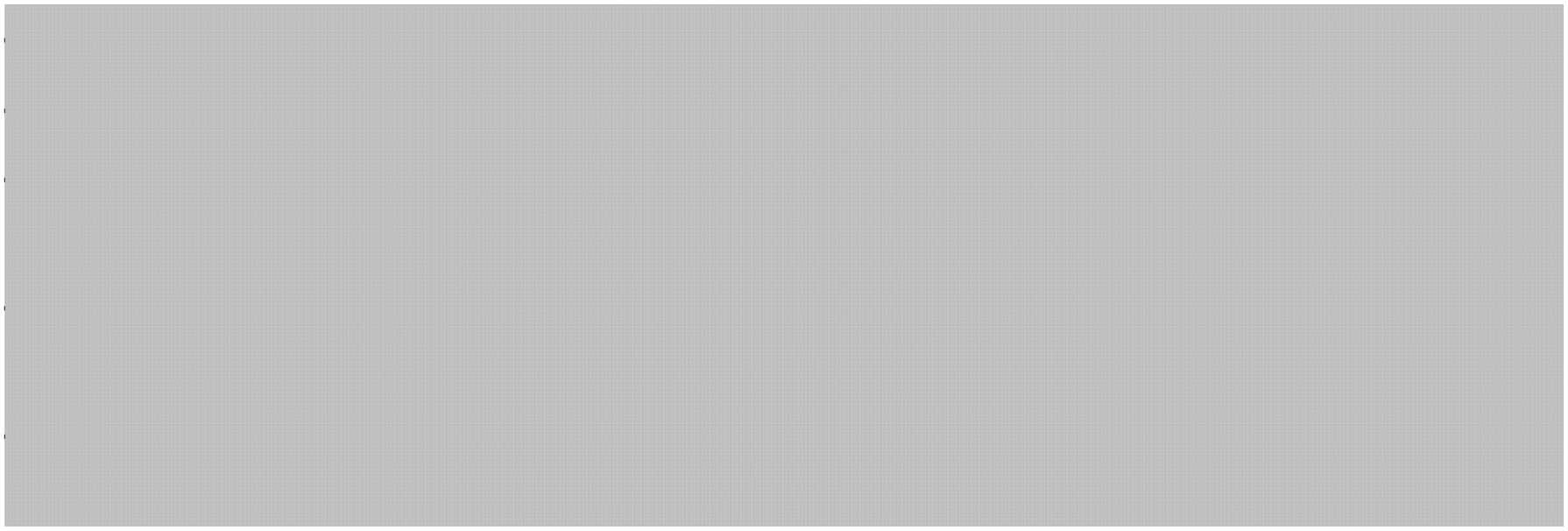
[redacted]

ISOM FIVE-YEAR REVIEW (2010)

- [redacted]
- Not a mandatory requirement, but a necessary one
- [redacted]
- [redacted]
- [redacted]

Integration Action Plan

- Functions and capabilities
- Integration of military and CSEC staff in each others' organizations
- The beginnings:



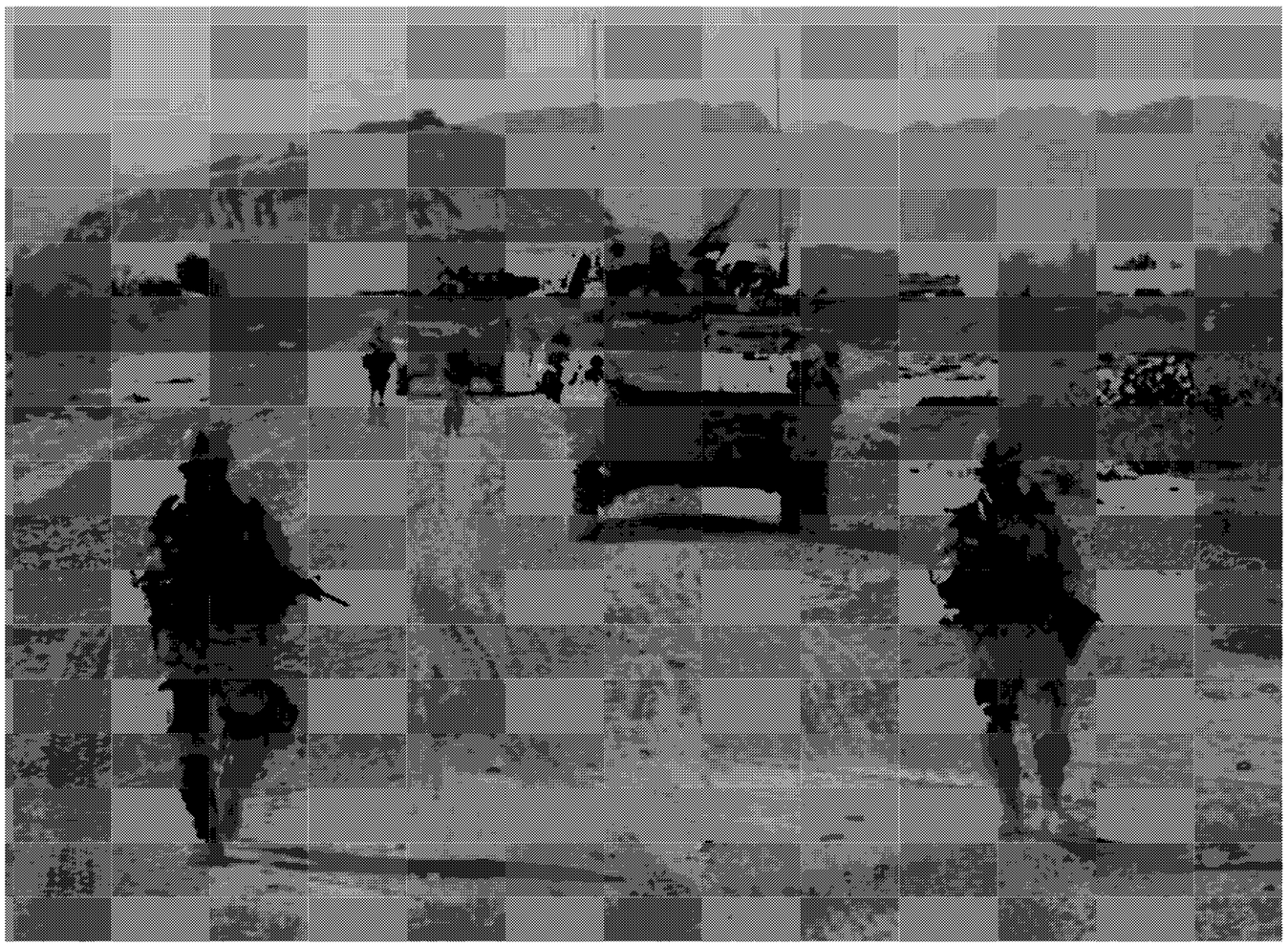
- Next:
  - Mission Management and planning functions
  - ELINTcapability…

Key takeaways

- Operational culture of CSEC is closely related to a heritage and recent experience of working with CF.

- One of the fifteen SIGINT 2015 thrusts is the “we will” statement:
  - “We will ensure that SIGINT and the CFIOG can operate as a single, seamless cryptologic enterprise, while ensuring that both CF and broader Government of Canada requirements are met.”

Questions?



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

Indoctrination Briefing for COHORTS/COOPS

Classification of this briefing: SECRET//SI

Corporate Security Directorate

Direction de la sécurité interne

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Today's Objectives

- Provide an overview of the Security of Information Act;
- Indoctrinate you to Top Secret, SIGINT Information Access (TS//SIA) and [redacted]
- Review <u>your</u> next steps.

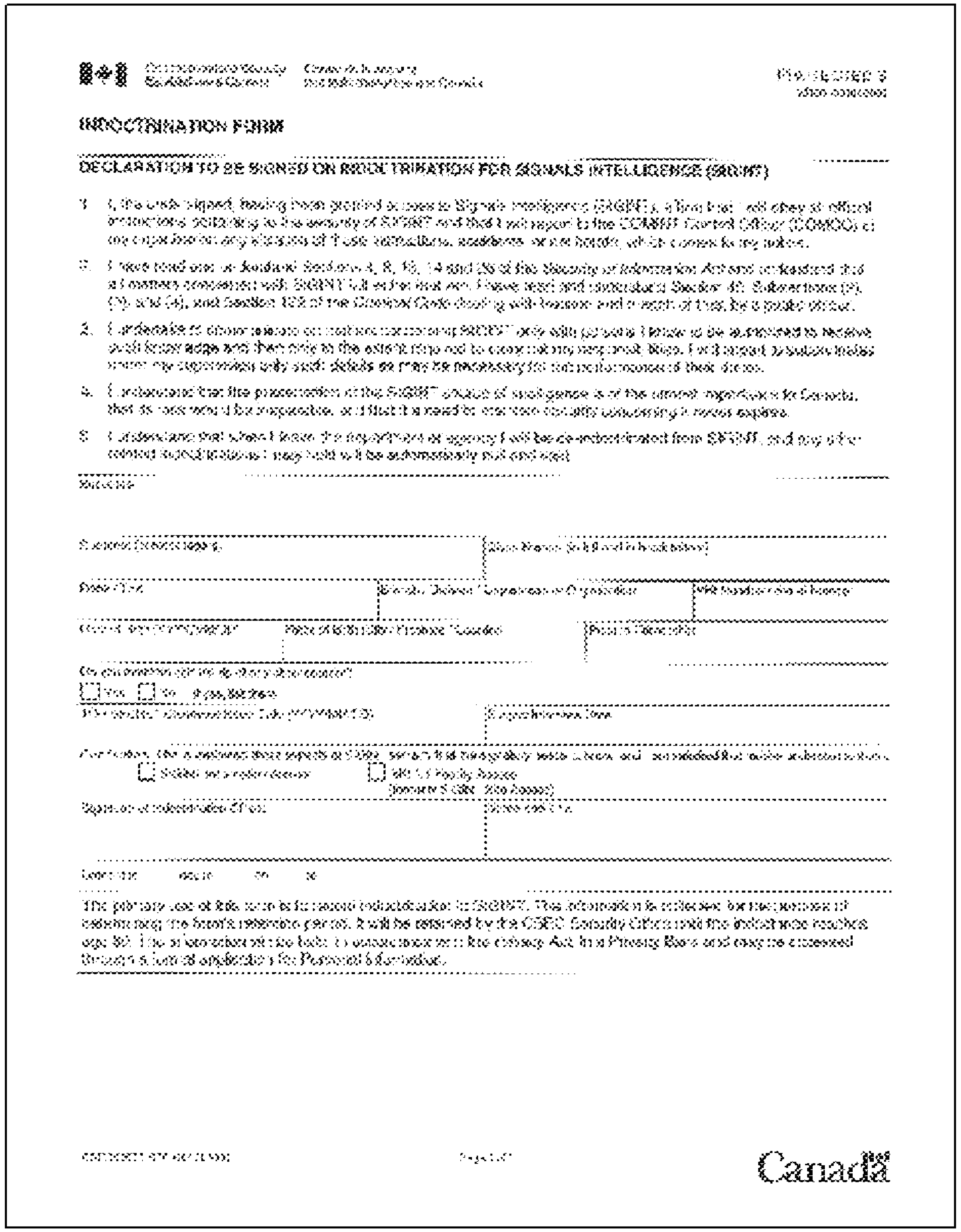
CSEC and our mandate

- CSEC is Canada's National Cryptologic Agency and a member of the Five Eyes.
- Our mandate is to:
  - Acquire and provide foreign intelligence to the Government of Canada;
  - Protect electronic information and information infrastructure of importance to the Government of Canada; and
  - Provide assistance to Federal Law Enforcement and Security Agencies in the performance of their lawful duties.

Security of Information Act (SOIA)

- Replaced the Official Secrets Act in 2001;
- As a signatory to the SOIA, you have authorized access to "special operational Information (SOI)" and in the interest of national security, you are a "person permanently bound to secrecy (PPBS)";
- Persons permanently bound to secrecy (PPBS) are:
  - any current or former employees of a designated agency or department listed in the Act – list includes CSEC;
- Special operational information is information that the GOC is taking measures to safeguard that reveals, or from which can infer, specified sensitive information (SI). Unauthorized disclosure would cause obvious damage to Canada.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada


INDOCTRINATION FORM

DECLARATION TO BE SIGNED ON INDOCTRINATION FOR SIGNALS INTELLIGENCE (SIGINT)

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

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

Government of Canada / Gouvernement du Canada

SECURITY SCREENING CERTIFICATE AND BRIEFING FORM

CERTIFICAT D'ENQUÊTE DE SÉCURITÉ ET PROFIL DE SÉCURITÉ

- *See reverse for privacy statement and completion instructions* / *Voir au verso pour énoncé concernant la loi sur la protection des renseignements personnels et directives*
- *Please type or print clearly in black letters* / *Prière de taper ou d'écrire en caractères noirs*

Reference No. - N° de référence	Departmental Organization No. - N° de ministère de l'organisation	OFFICE USE ONLY / RÉSERVÉ À L'ADMINISTRATION File number - N° de dossier

PART A - TO BE COMPLETED BY SECURITY OFFICE
PARTIE A - À REMPLIR PAR LE BUREAU DE SÉCURITÉ

Surname - Nom de famille	Full given names (in initials) - Prénoms au complet (pas d'initiales)
Department/Organization/Agency - Ministère/Organisation/Agence	Unit/Branch - Section/Direction

☐ Initial briefing or reactivation / Première attribution ou réactivation
☐ Change in security requirement / Changement des exigences en matière de sécurité
☐ Termination / Cessation

AUTHORIZED LEVEL OF INDIVIDUAL - NIVEAU AUTORISÉ DE LA PERSONNE

Reliability status / security clearance authorized is: - Cote de fiabilité / de sécurité autorisé est:

☐ Reliability Status / Cote de fiabilité
☐ Site access / Accès aux emplacements
☐ Level - I (CONFIDENTIAL) / Niveau - I (CONFIDENTIEL)
☐ Level - II (SECRET) / Niveau - II (SECRET)
☐ Level - III (TOP SECRET) / Niveau - III (TRÈS SECRET)
☐ Other (specify) / Autre (préciser)

I, the undersigned, as an authorized security official, do hereby certify that the above information has been verified and the requested level is granted.
Je, soussigné, à titre d'agent de sécurité autorisé, certifie que les renseignements ci-dessus ont été vérifiés et l'autorisation est accordée.

Signature — Y-A M-M D-J

Name and title of authorized security official - Nom et titre de l'agent de sécurité autorisé	Office address - Adresse au bureau	Telephone - Téléphone	Facsimile - Télécopieur

PART B - BRIEFING SUMMARY
PARTIE B - SOMMAIRE DE LA SÉANCE D'INFORMATION

The individual named herein is authorized access to the level of information/assets indicated above when there is a work related need.

If an individual fails to safeguard, releases without appropriate authority or uses information/assets for unauthorized purposes, such action may constitute a contravention of the Security of Information Act, the Access to Information Act, the Privacy Act or other Acts of Parliament, a breach of the Government Security Policy or the Oath of Secrecy. These provisions apply both during and after service to the Government of Canada. Specific safeguards are identified in the Government Security Policy and Standards and in corresponding departmental or organizational policies which apply to classified and protected information/assets. These safeguards must be applied.

Classified or protected information/assets must be returned immediately to the appropriate institutional authority when notification is given that the person named herein no longer requires access to such information/assets.

La personne nommée dans le présent a le droit d'accès aux renseignements et aux biens au niveau indiqué ci-dessus lorsque cela est nécessaire à l'exercice de ses fonctions.

Si la personne ne protège pas, divulgue sans autorisation pertinente ou utilise les renseignements et les biens à des fins autres que celles officiellement autorisées, cette action peut constituer une infraction à la Loi sur la protection de l'information, à la Loi sur l'accès à l'information, à la Loi sur la protection des renseignements personnels ou à d'autres lois du Parlement, une violation de la Politique du gouvernement sur la sécurité ou du serment de discrétion. Ces dispositions s'appliquent durant et après la période de travail pour le gouvernement du Canada. La politique et les normes du gouvernement sur la sécurité et les politiques des ministères ou des organisations qui s'appliquent aux renseignements et aux biens classifiés ou protégés font état des mesures de sécurité qui doivent être prises.
Les renseignements et les biens classifiés ou protégé doivent être retournés immédiatement au représentant institutionnel approprié lorsqu'un avis est émis selon lequel la personne nommée dans la présente n'a plus besoin d'y accéder.

PART C - ACKNOWLEDGEMENT
PARTIE C - ACCEPTATION

I understand and agree to comply with the above statutory and administrative requirements.
Je comprends et j'accepte de respecter les exigences législatives et administratives précitées.

Signature of individual - Signature de la personne — Y-A M-M D-J

PART D - BRIEFING OFFICIAL
PARTIE D - REPRÉSENTANT QUI A DONNÉ LA SÉANCE

Name and initials - Nom et initiales

Title - Titre

Signature — Date

TSS/SCT 330-47 (Rev. 2002/05) — TBS/SCT 330-47 (Rév. 2002/05)

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

Special Operational Information

HUMINT = HUMan INTelligence

- HUMINT is information gathered by agents, who often use other human sources.
- Sources of HUMINT:
  - Comes from a variety of backgrounds/status;
  - Talent spotted early in a career and cultivated for future purposes;
  - Foreign person may offer their services for a number of reasons; and
  - Military intelligence also cultivates local sources during operations.
- Why is a brief needed?
  - CSEC is required to brief you on HUMINT to facilitate [redacted]/access to USA's counterpart agencies (CIA).

HUMINT (Cont'd)

- Who is responsible?
  - In the USA, CIA is the lead for HUMINT; and
  - In Canada, CSIS is the lead for HUMINT although RCMP, FAC, DND and CBSA are also major contributors.
- How do we handle HUMINT?
  - Usually classified (Top Secret, Secret or Protected C);
    - Can also bear other markings and caveats.

HUMINT (Cont'd)

- Compartmentalization is required because:
  - There is a high level of sensitivity of the target country, organization or entity;
  - There is potential loss by compromise of extremely valuable intelligence;
  - Compromise may cause physical harm to the source and/or the agent; and
  - Security constraints established by the provider of the material.

HUMINT (Cont'd)

- What is our responsibility in safeguarding the information?
  - Confine all exchanges on the topic to those with a clearly established "NEED TO KNOW"; and
  - Do not try to discern or guess who the HUMINT source is.

- Legal Obligations
  - It is an offence under the CSIS Act to publicly identify or publish the identity of covert CSIS Officers and human sources.

Threats to the Security of CSEC

- **Active** threat
  - Disgruntled employees (may divulge information in revenge); and
  - Foreign intelligence espionage, terrorism.

- **Passive** threat
  - Employees that are nonchalant about security (do not follow security policy, guidelines); and
  - Employees that are complacent (security it is not my responsibility).

Corporate Responsibilities

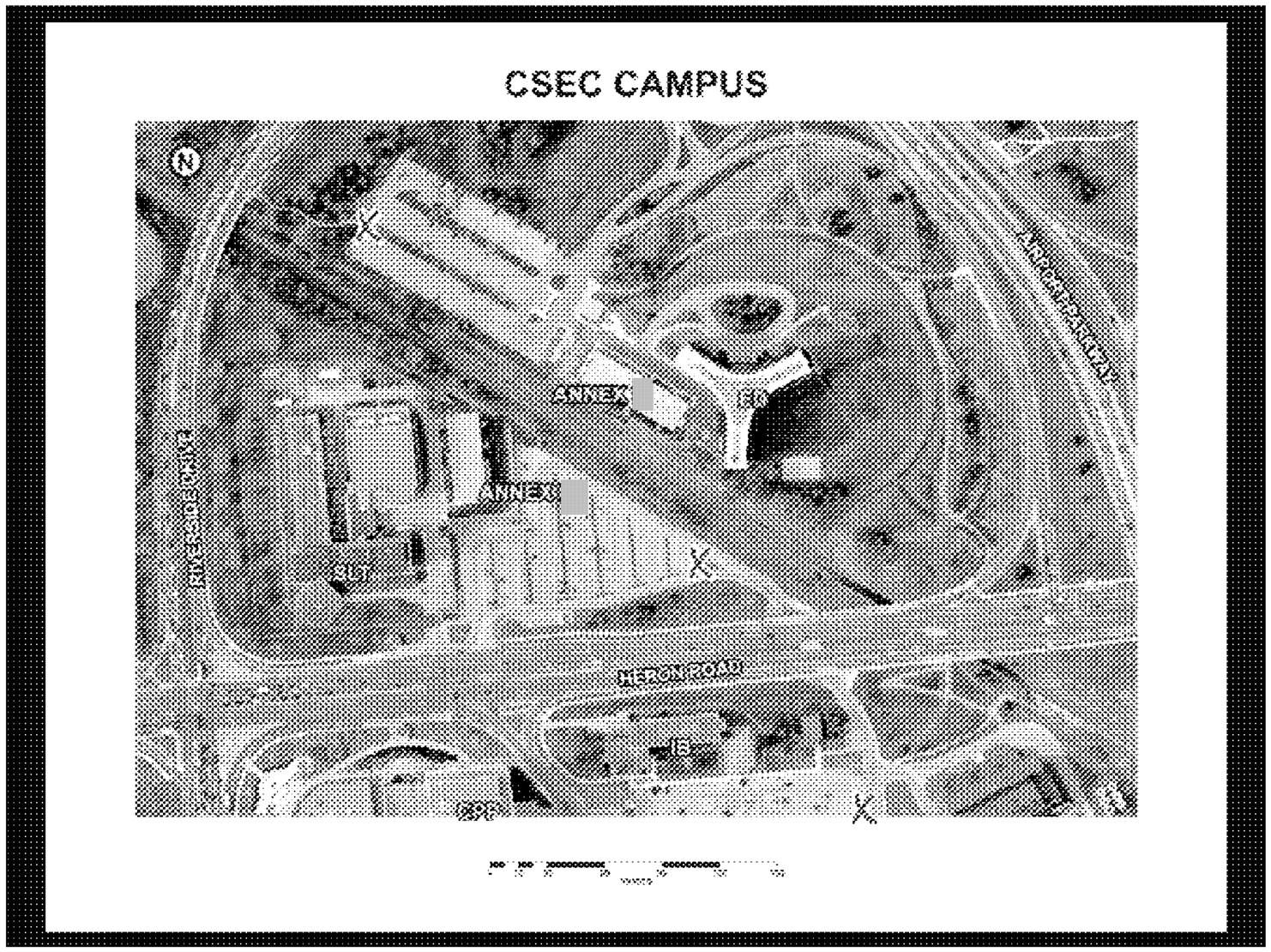
- CSEC provides you with tools, services, advice and an environment to minimize the threats by:
  - Security policies, procedures and guidelines;
  - Security education/awareness program;
  - Physical security;
  - Personnel security;
  - Information technology security; and
  - Information security.

Personal Responsibilities

- What you can do to minimize the threats:
  - Avoid complacency;
  - Adhere to policies, procedures and guidelines;
  - When in doubt, seek advise from security subject matter experts;
  - Talk to your Group Security Officer (GSO) and/or manager about what your group's specific security requirements ; and
  - Send your questions or concerns to Security via the [redacted]

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

The CSEC Campus

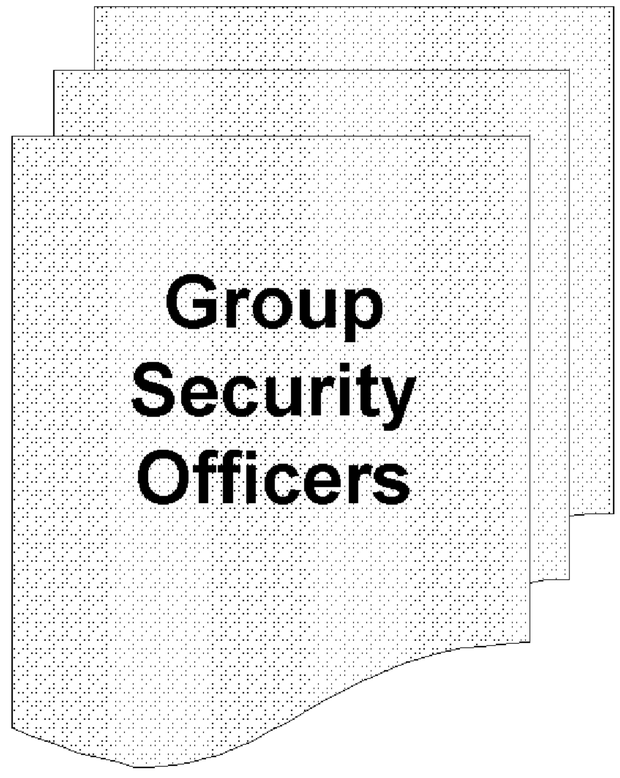


Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Group Security Officers (GSO) Program

- Every area has a Group Security Officer.
- Promote, collaborate and coordinate good security practices in support of established CSEC policies and procedures.
- Keep their group up-to-date on CSEC security policies, procedures and best practices.
- Initiate new employees to the security practices of the organization as well as group specific practices.



Your Next Steps

- Within 2 weeks:
  - Contact, meet and review security procedures and guidelines specific to your area with your Group Security Officer (GSO).

Final thoughts

- At CSEC, security is about much more than guards, alarms and locks. It's as much about *behaviors* as it is about *barriers*.

- Corporate Security is really a partnership between CSEC's employees and our security practitioners — we rely heavily on individual and team responsibility, vigilance, and a day-to-day commitment to security.

- If you're ever in doubt about a security issue, speak to your GSO, your manager, or come by and see a Personnel or Physical Security officer, or the Director, Corporate Security.

- Our goal is to enable CSEC's workforce to do its job securely and to ensure the secure delivery of CSEC's programs and services — and our success depends on you.

Questions?