



Communications  
Security Establishment

Centre de la sécurité  
des télécommunications

TOP SECRET//CEO

TOP SECRET//SI//CEO



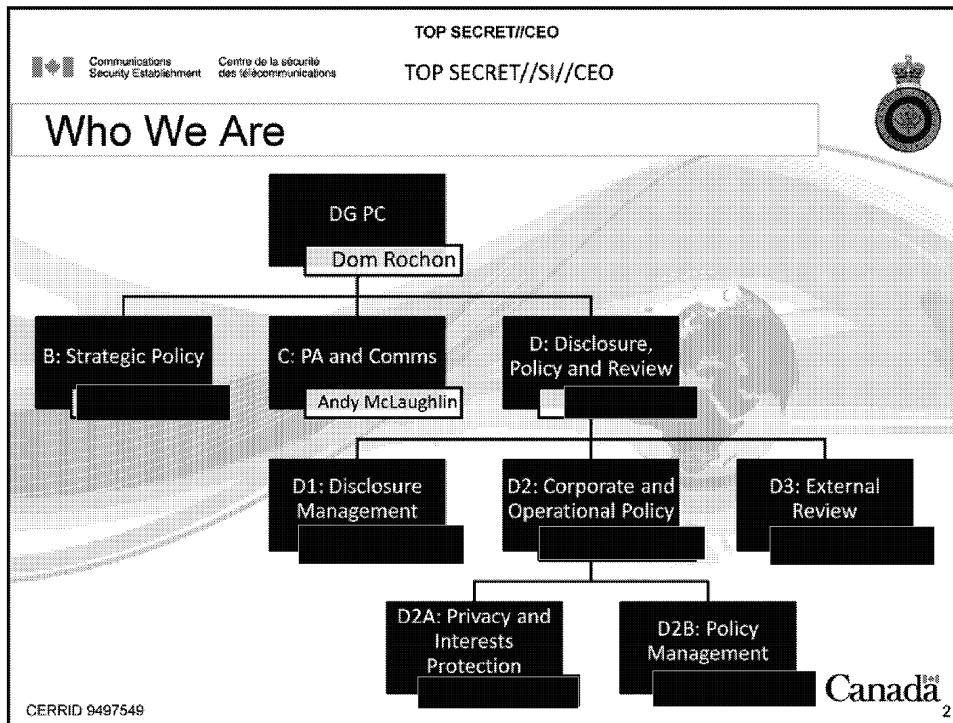
## D2: Corporate and Operational Policy

March 2014

Canada

CERRID 9497549

- Chief to make introductory remarks
- The objective of this briefing is to provide you with an overview of:
  - Who we are,
  - What we do and why,
  - How we do it, and
  - How we protect the privacy of Canadians in our activities.



The Privacy and Interest Protection Team (D2A) will assume the duties associated with "Privacy Protection", e.g.:

- Management of PIF and MPER
- Managing exceptions to standard guidelines (e.g. naming, targeting)
- Canadian status (citizenship and Permanent Residence) verifications


Policy Management team (D2B) will assume responsibilities of a policy interpretation, guidance, awareness and concurrence nature e.g.:

- Responding to questions requesting clarification on policy interpretations, etc.
- Develop training and awareness programs on CSEC ORG and OPS policies (including annual OPS-1 Quiz)

IRRELEVANT

TOP SECRET//CEO  
TOP SECRET//SI//CEO

Communications Security Establishment  
Centre de la sécurité des télécommunications



## What We Do

### D2A: Privacy and Interests Protection Team

... is responsible for ensuring that CSE protects the privacy of Canadians and Five Eyes entities in its activities, as well as CSE reporting and equities

**This means that D2A:**


- Liaises with Five Eyes policy and privacy protection centres
- Manages exceptions to standard practice for naming and targeting
- Verifies Canadian citizenship and PR status
- Manages the Privacy Incidents File
- Conducts Mistreatment Risk Assessments
- Manages the CII release process
- Coordinates action-on and sanitization requests

### D2B: Policy Management

... is responsible for drafting and interpreting CSE-wide policies and ensuring policy compliance

**This means that D2B:**

- Reviews and updates operational and organization policies
- Responds to questions on how to apply CSE's policies
- **IRRELEVANT**
- Delivers training on OPS and ORG policies
- Conducts sensi-checks for Five Eyes partners

Canada 

CERRID 9497549 3

The Privacy and Interest Protection Team (D2A) will assume the duties associated with "Privacy Protection", e.g.:  
Management of PIF and MPER

Managing exceptions to standard guidelines (e.g. naming, targeting)

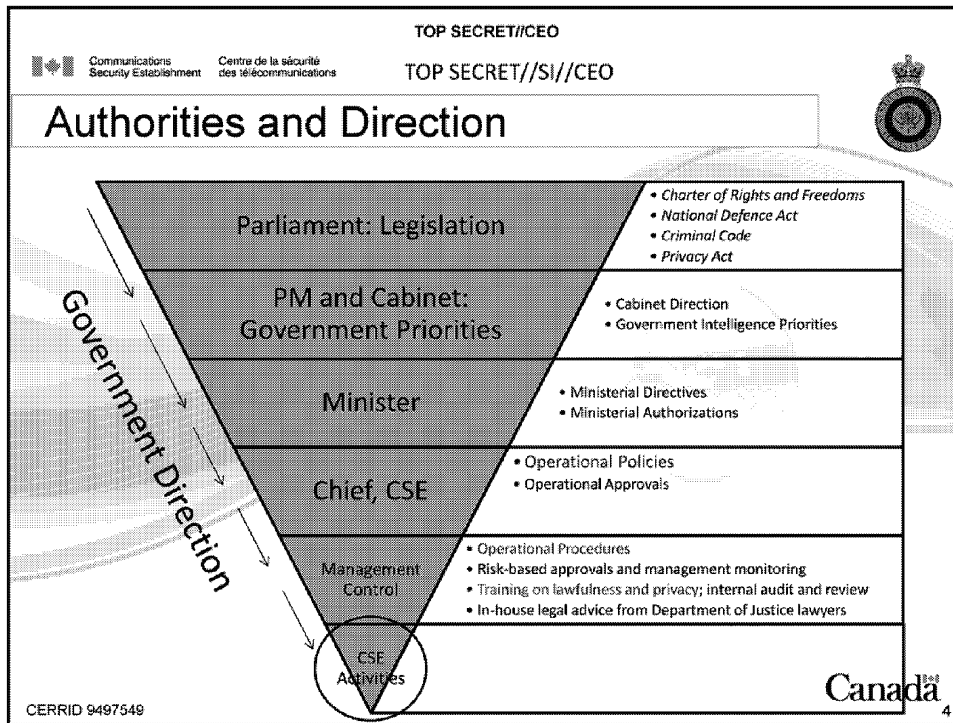
Canadian status (citizenship and Permanent Residence) verifications

Policy Management team (D2B) will assume responsibilities of a policy interpretation, guidance, awareness and concurrence nature e.g.:

Responding to questions requesting clarification on policy interpretations, etc.

Develop training and awareness programs on CSEC ORG and OPS policies (including annual OPS-1 Quiz)

IRRELEVANT



### Parliament: Legislation

- CSE operates within all Canadian laws, including the *Charter of Rights and Freedoms*, the *National Defence Act*, the *Criminal Code*, and the *Privacy Act*.
- The NDA defines foreign intelligence as information about the capabilities of a foreign individual, state, organization or terrorist group, related to international affairs, defence or security, and provides the broad parameters of what CSE is allowed to do, including important limits on CSE's activities.
  - Notably, CSE's activities cannot be directed at Canadians and CSE must have measures in place to protect the privacy of Canadians in its activities.
- The Privacy Act also applies to how we collect, use, retain and disclose personal information.
- In addition, executive-level oversight provides essential constraints and restraints on CSE's activities.
- Each level of the triangle is a further, and appropriate, constraint on the organization in order to ensure that our activities are appropriately focused and in compliance with the law.

### PM & Cabinet: Government Priorities

- At the strategic level, the Prime Minister and the Cabinet identify the Government's intelligence priorities.
- Under the NDA, we are only authorized to collect foreign intelligence in accordance with what the identifies as its FI priorities.

### Minister

- These intelligence priorities are communicated to CSE by the Minister of National Defence through a Ministerial Directive.
- The Minister provides Chief, CSE with written instructions on how he is to carry out his duties and functions and those of CSE through Ministerial Directives. These can range from operational and legal issues to administrative matters and often include annual reporting requirements. The MD on the Privacy of Canadians provides general direction on how CSE must protect the privacy of Canadians when fulfilling its duties.
  - CSE is currently reviewing this MD to ensure it is sufficiently robust.

- In addition, Ministerial Authorizations are required to authorize activities where there is a risk of intercepting private communications – that is communications that either originate or terminate in Canada and where the originator has a reasonable expectation of privacy.

- Under its foreign intelligence mandate, CSE collects communications as they are transmitted on the global information infrastructure.
- While CSE's activities are targeted at foreign entities outside Canada, it is unavoidable that CSE will incidentally intercept private communications and the communications of Canadians outside Canada. To understand why this occurs, it is necessary to understand how communications are transmitted.

- While, CSE can minimize the likelihood of incidentally intercepting a private communication, the risk cannot be eliminated.

- For example, even if CSE only views the traffic of foreign targets, there is still a possibility that a foreign target may be in communication with a Canadian or person in Canada.

- Parliament recognized the risk of incidentally intercepting private communications and established the Ministerial Authorizations regime within the NDA to manage this risk.

- Ministerial Authorizations provide the authority framework necessary to allow CSE to fulfill its mission in an efficient, effective and lawful manner.

- MAs do not convey any new authorities beyond the law.

- When an incidental intercept occurs and is recognized, an analyst will determine whether a piece of traffic has foreign intelligence value. If it doesn't the traffic will be deleted from CSE's repositories.

- Prior to issuing a Ministerial Authorization the Minister must be satisfied that specific conditions have been met, including measures to protect the privacy of Canadians. For activities in support of CSE's foreign intelligence mandate, the Minister must be satisfied that:

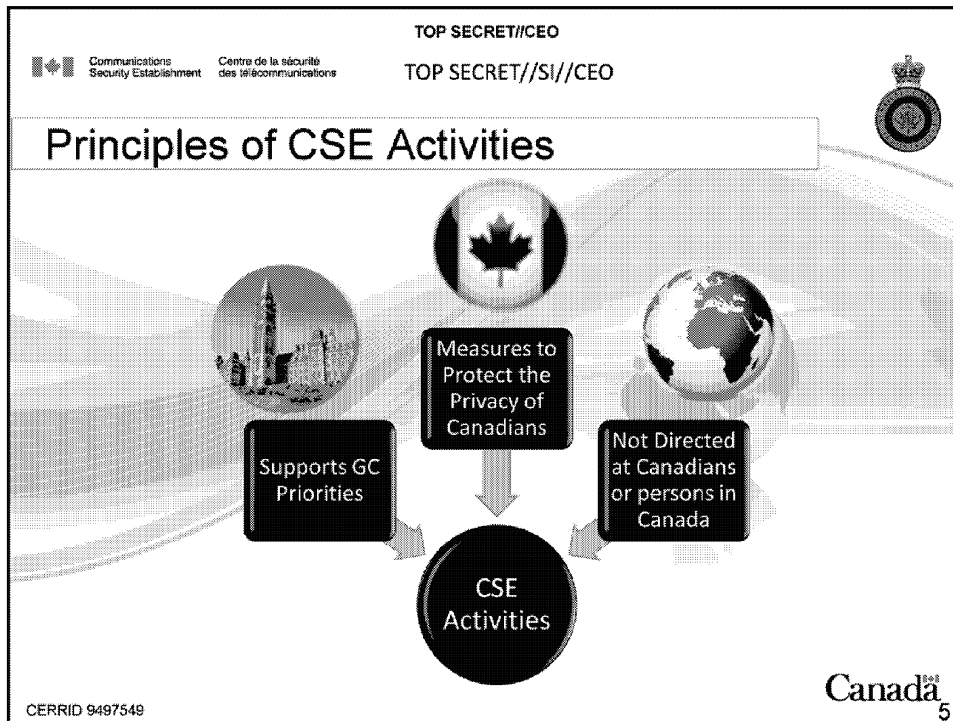
- The interception will be directed at foreign entities outside Canada;
- The information to be obtained could not reasonably be obtained by other means;
- The expected foreign intelligence value of the interception justifies it; and
- Satisfactory measures are in place to protect the privacy of Canadians and ensure that intercepted private communications will only be used or retained if they are essential to international affairs, defence, or security.

- Ministerial Authorizations for activities conducted under CSE's IT Security mandate have distinct conditions to be met, though they include similar measures to protect the privacy of Canadians.

#### Chief & Management Control

- The Chief then communicates the Minister's expectations and articulates how CSE is to put them into practice through operational policies and instructions, management oversight, and the approvals required for operations.

- Ongoing training on lawfulness and privacy ensures that CSE personnel are aware of how they are to respect privacy in their daily activities.
- At the pointy end of the triangle are the activities that CSE carries out on a daily basis. These are reviewed by the CSE Commissioner for compliance with the law, ministerial expectations and CSE policies and procedures.



- To summarize, this is the scope for CSE activities.
- All CSE activities must comply with relevant Canadian laws, including:
  - The *Charter of Rights and Freedoms*, which protects Canadians and persons in Canada from unreasonable search and seizure;
  - The *National Defence Act*, which outlines clear limitations on CSE activities;
  - The *Criminal Code*, which prohibits the interception of private communications; and
  - The *Privacy Act*, which outlines how CSE is to manage use privacy-sensitive information that it has lawfully acquired.
- Ministerial Authorizations and Direction outline robust requirements for how CSE may retain and use any private communications that it incidentally intercepts during its lawfully-mandated activities.
- CSE's foreign intelligence activities must support a GC intelligence priority, as determined by Cabinet.
  - CSE must have reason to suspect that its activities will lead to foreign intelligence, as defined in the NDA, before it can target the communications of a foreign entity.
  - CSE's foreign intelligence activities may not be direct at Canadians anywhere or any person in Canada.
    - As per the NDA, a "Canadian" means a Canadian citizen, a permanent resident or a corporation incorporated in Canada, though organizations are afforded the same protections. Dual citizens are treated as Canadians and may not be targeted.
  - CSE has measures in place to protect the privacy of Canadians in the use, retention, disclosure and storage of any privacy-sensitive information that it acquires. I will discuss these measures later in

the presentation.

- Only analysts that are trained and tested have access to the targeting database, which contains the privacy-sensitive information about foreign targets.
- Finally, even when a communication has “foreign intelligence” value, CSE only reports on it if it relates to a Government of Canada intelligence priority, as determined by Cabinet.
- CSE’s IT security activities are similarly restricted.
  - CSE is mandated protects electronic information and information infrastructures of importance to the Government.
  - CSE must have the consent of the system owner and may only conduct activities where there is a risk of intercepting a private communication on GC systems.
  - CSE has robust measures in place to protect the privacy of Canadians in its use and retention of privacy-sensitive information.
- IRRELEVANT
- CSE’s operational policies provide guidance on how analysts are to ensure lawfulness and protect the privacy of Canadians in the course of the duties.
- CSE’s policies cover all aspects of operations – including targeting, collection, analysis, report writing, and information sharing.



TOP SECRET//CEO  
TOP SECRET//SI//CEO

Communications Security Establishment  
Centre de la sécurité des télécommunications

**CSE's Operational Policy Suite**

- OPS-1 Series: Privacy and Lawfulness
- OPS-2 Series: Information Sharing
- OPS-3 Series: Sensitive or ECI Programs
- OPS-4 Series: IRRELEVANT
- OPS-6 Series: IRRELEVANT (Draft)

<http://www2.cse-cst.gc.ca/resource/csec-operational-policies>

Canada 6

OPS Policy Suite is currently under review

## OPS 1

OPS-1, Protecting the Privacy of Canadians & Ensuring Legal Compliance in the Conduct of CSEC Activities

OPS-1-1, Procedures for the Release of Suppressed Information from SIGINT Reports

OPS-1-6, Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports

OPS-1-7, Operational procedures for Naming in SIGINT Reports

OPS-1-8, Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians

OPS-1-10, Operational Procedures for Metadata Analysis [REDACTED]

OPS-1-11, Retention Schedules for SIGINT Data

OPS-1-13, Operational Procedures Related to Canadian [REDACTED] Collection Activities

OPS-1-14, Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization

OPS-1-15, Operational Procedures for Cyber Defence Activities Using System Owner Data

## **OPS 2**

### OPS-2-3, Sensicheck Procedures

## **OPS 3**

### OPS-3-1, Procedures for [REDACTED] Activities

#### OPS-3-4 - Procedures for [an ECI Program]

#### OPS-3-6 - Procedures for [a CEO activity]

## **OPS 4**

IRRELEVANT

## **OPS 5**

### OPS-5-3, Write-to-Release (WTR) Procedures

### OPS-5-9, End-Product Sanitization/Action-on Procedures


- Operational policies provide guidance on how to put the Minister's expectations into practice
- They provide procedural principles and practices that CSEC must apply to mandated activities to ensure that our activities comply with legal requirements, ministerial requirements and management direction
- They are organized thematically into series.
- For example, all the Ops 1 series provides specific guidance on how CSEC needs to protect privacy and ensure lawfulness. Key policies in this series are:
  - OPS 1: establishes baseline measures to protect the privacy of Canadians in the use and retention of information intercepted by CSEC

OPS-1-1: describes measures that

OPS-1-8: describes CSEC's policy compliance monitoring program, which demonstrates the legal compliance of CSEC's mission operations that might impact lawfulness/privacy. The policy describes what must be monitored and assigns responsibility for management and oversight.

TOP SECRET//CEO  
TOP SECRET//SI//CEO

Communications Security Establishment  
Centre de la sécurité des télécommunications



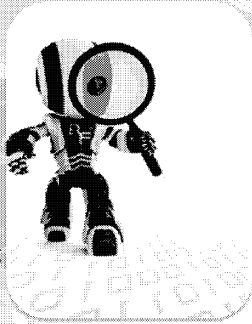
## Protecting Privacy

A **privacy incident** occurs when the privacy of a Canadian is put at risk in a manner that runs counter to CSE's operational policies

For example, a privacy incident occurs when ...

- An analyst unknowingly targets a Canadian or person in Canada
- Inadvertently includes CII in a report
- An analyst releases CII to a GC partner
- Improper access controls are applied to databases containing private communications or CII

All privacy incidents must be reported to SPOC  
SPOC will notify D2A to include the incident in the Privacy Incidents File (PIF)



Canada <sup>88</sup> 7

CERRID 9497549

### The NDA:

- prohibits CSE from directing its activities at Canadians or persons in Canada; and
- requires that CSE's activities are subject to measures to protect the privacy of Canadians
- All CSE activities contain robust measures to protect the privacy of Canadians. These measures are built into each stage.
- **Stage 1:** In terms of the "Oakes Test," CSE can demonstrate the necessity, proportionality, effectiveness and minimal intrusiveness of its activities.
  - Necessity: The Government of Canada requires foreign intelligence about the capabilities, activities, and intentions of foreign entities, including states and terrorist groups, as they relate to international affairs, defence or security. The NDA mandates CSE to provide the Government with this intelligence.
  - CSE's only source of foreign intelligence is the global information infrastructure.
    - CSE acquires only the information it needs to produce foreign intelligence or to protect GC systems or information infrastructures of importance to the Government.
    - To ensure that CSE is acquiring information in the least intrusive way possible, CSE collects metadata. Metadata is information used to identify, describe, manage, or route a telecommunication. It is not a private communication but it can have a privacy interest.
    - CSE uses the metadata it collects to better understand how communications are transmitted on the global information infrastructure and to identify new foreign intelligence targets.
  - Proportionality: CSE must direct its activities at foreign entities outside Canada. Any intercept of a private communication or a communication of a Canadian outside Canada is incidental to CSE's

- activities.
- Metadata enables CSE to select those communications it is authorized to acquire – i.e. communications of foreign intelligence value that relate to Government intelligence priority or those that will better enable CSE to protect GC networks and systems.
  - Metadata helps CSE reduce the likelihood of acquiring communications it is prohibited from acquiring. (i.e. two-end Canadian)
  - **Effectiveness:** CSE's produces actionable and strategic intelligence for the Government of Canada. CSE's intelligence advances the Government's foreign policy interests and protects Canadians – both at home and abroad.
  - **Minimal Intrusiveness:** Finally, there must satisfactory measures in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence, or security.
  - CSE's MA regime requires that it "make the case" to the Minister that these conditions are met before it is authorized to undertake any activities that risk the incidental intercept of a private communication.
    - Specifically, for SIGINT MAs, CSE must demonstrate that:
      - Its activities will be directed at foreign entities located outside Canada (Proportionality);
      - The information to be obtained could not reasonably be obtained by other means (Necessity);
      - The expected foreign intelligence value of the information that would be derived from the interception justifies it (Effectiveness); and
      - Satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security (Minimal Intrusiveness).
  - Similar conditions are in place for IT Security activities.
  - **Stage 2:** CSE has measures in place to properly protect any privacy-sensitive information it acquires.
    - **Accountability:** CSE must conduct its activities in accordance with the expectations set out by the Minister in the MD on Privacy.
      - CSE has a Chief Privacy Officer to provide oversight and accountability for how CSE protects the privacy of Canadians.
      - CSE's operational policy suite defines roles and responsibilities, including those related to privacy.
      - All privacy incidents must be reported to the Privacy and Interests Protection team, who maintains a central repository of all incidents.
    - **Limiting Collection:** CSE limits its collection of privacy-sensitive information by directing its activities at foreign entities outside Canada in accordance with the Government of Canada's intelligence priorities. For IT Security activities, CSE limits collection to GC systems and networks in order to acquire information that

would be harmful to networks of importance to the Government.

- **Limiting Use, Disclosure and Retention:** Communications with a recognized Canadian angle – including incidentally intercepted private communications, communications of Canadians outside Canada, and communications containing information about Canadians – are deleted from CSE’s traffic repositories unless analysts determine that their retention is necessary for CSE to successfully implement its mandate.
  - For SIGINT activities a communication may only be retained if it contains foreign intelligence, is essential to protect lives, or contains information about serious criminal activity related to the security of Canada.
  - For IT Security activities, information may only be retained if it is necessary to protect GC systems or networks.
- The inclusion of personal information in CSE’s foreign intelligence and cyber defence reports is carefully managed. CSE only discloses information that is necessary.
- Information about Canadians may only be included in CSE’s intelligence reports if it is required to understand or exploit the foreign intelligence.
- By default, any information in a CSE report that could identify a Canadian is suppressed and replaced by a generic reference, such as “a named Canadian.” Limited exceptions to this rule include situations where there is an identified threat to life.
  - These cases still require approval from the Chief Privacy Officer.
- Reports with a Canadian angle must be approved by a Senior Manager at the Director General level or above.
- SIGINT and IT Security reporting standards require that suppressed identity information is stored in an accredited suppressed information repositories.
  - Access to this repository is limited to designated personnel. Suppressed privacy-sensitive information obtained from allied reporting is also retained in these repositories.
- **Stage 3: *Running the Programme***
  - **Accessible Policies and Practices:** CSE’s process for sharing foreign intelligence and cyber defence information is carefully managed by Operational policies, operational instructions and organizational policies.
  - These documents provide guidance to CSE personnel on how they are to protect privacy in their daily activities. These are available to staff on our internal website. The Corporate and Operational policy team review and update these policies as required.
  - **Ongoing Privacy Training:** CSE offers robust privacy training to all personnel and staff are required to re-validate their awareness of CSE’s legal and policy requirements to protect privacy annually.
  - **Senior-level Accountability:** All CSE activities are subject to internal and external audits and reviews, including active monitoring, audit and evaluation, CSE

Commissioner.

- The Minister is accountable to Parliament and Cabinet for CSE's activities.
  - The Chief CSE is accountable to the Minister of National Defence and must report on an annual basis how many private communications CSE intercepted, as well as how many of these were retained and how many were destroyed.
  - CSE also maintains an internal audit office to review CSE activities.
- **Stage 4: *Calibrating the System***
    - We're working to find the right balance between increasing transparency, protecting national security, and managing the personal information CSE acquires.

IRRELEVANT

- All CSE activities are subject to internal and external audits and reviews, including active monitoring, audit and evaluation, CSE Commissioner.


Communications  
Security Establishment

Centre de la sécurité  
des télécommunications


TOP SECRET//CEO

TOP SECRET//SI//CEO


TOP SECRET//SI




D2A




Targeting: Canadian citizenship and PR Status verification




Reporting: Contextual identifications; CII disclosure; PIF



Protecting CSE Equities: Sanitizations and Actions-on



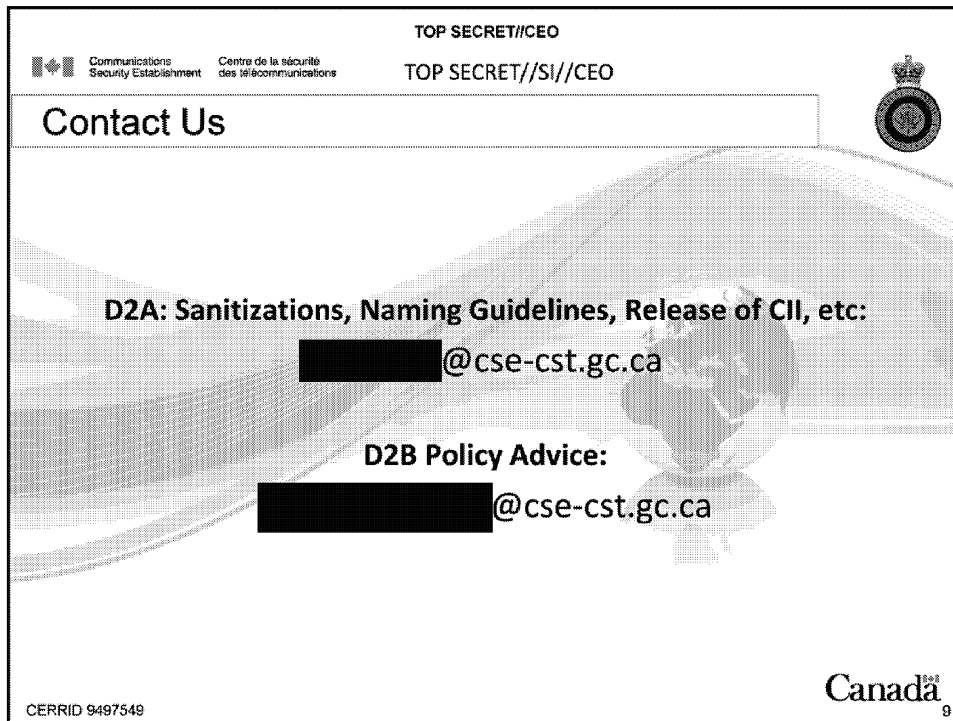
Sharing: Mistreatment Risk Assessments



Relationships: Liaison with Five Eyes

Canada

8



- The CSE Commissioner is independent from CSE. He operates at arms-length from the government and receives his own appropriation from Parliament.
- The Commissioner must be a retired senior judge. To date, Commissioners have been former senior judges from the Appeals Court (Quebec and Federal Court) or the Supreme Court. The present Commissioner, the Honourable Jean-Pierre Plouffe, is a supernumerary Judge in the Superior Court of Quebec as well as a Judge in the Court Martial Appeals Court of Canada.
- The Commissioner's role is to:
  - Review CSE's activities for compliance with the law, Ministerial Authorizations and Directives, and its internal policies, including how CSE meets its obligations to protect the privacy of Canadians; and
  - Receive, investigate and respond to complaints about CSE.
- In executing his duties, the Commissioner has all the powers of a Commissioner under the Inquiries Act, including the power to subpoena. This allows him to:
  - Examine CSE's hard copy and electronic information records, policies and procedures, and any legal advice received from the Department of Justice;
  - Request briefings and demonstrations of specific activities;
  - Interview CSE managers and employees;
  - Observe CSE operators and analysts first hand; and
  - Test information obtained against the contents of CSE's systems and databases.
- The Commissioner reports directly to the Minister of National Defence.
- He is required by law to inform the Minister of National Defence and the Attorney General of any CSE



- behaviour that may not be in compliance with the law.
- Produces classified reports for the Minister (typically 3-7 classified reports each year).
- Tables an unclassified report in Parliament.
- Since the creation of the Office of the Commissioner in 1996, there have been 74 completed reports containing 138 recommendations.
- The Commissioner makes a recommendation when he feels business practices should be improved or when a change will improve CSE's ability to demonstrate lawfulness or the protection of the privacy of a Canadian.
- CSE gives these recommendations serious consideration.
- Since 1997, 92% of the Commissioner's recommendations have been accepted.
- All of the recommendations related to privacy and lawfulness have been implemented, with the exception of recommendations from the most recent report which is underway.
- IF PRESSED ON REJECTED RECOMMENDATIONS:
- In an instance where CSE initially rejects a recommendation, the Commissioner reviews the reasons provided by CSE, then assesses whether to accept these reasons or to pursue the issue further. This process can lead to CSE eventually accepting the recommendation.
- For the 8% of recommendations that CSE rejected, there is no set reason or reasons why CSE would not accept a recommendation as each recommendation is assessed individually.
- As the Commissioner's reviews are historical in nature, some of the recommendations will be related to issues already addressed by CSE and the recommendation is rejected as appropriate safeguards are already in place and the recommendation is no longer valid.
- In other cases it could be assessed that the workload required to adopt a recommendation would be counterproductive and place an unacceptable strain on an operational area.
- Some of the recommendations made by the Commissioner's office would have an impact on, or are more appropriate for, CSE's domestic or international partners and it is not feasible for CSE to address them as the equity involved belongs to somebody else.
- Additional Information:
- Examples of OCSE reviews: These are only a selection of OCSE reviews on these topics. There have been many others (and all classified reviews have dealt with Canadian identity information one way or another).
- The key point here is that there have been multiple and repeated independent reviews over the years with consistently positive results:
- Metadata Reviews: 2010 on Contact Chaining, 2009 on Follow-up to Metadata Review, 2008 on Support to CSIS Review, 2008 Metadata Review, 2006 Support to RCMP Review (Phase II);
- Protection of Canadian Identity Information Reviews: 2013 on Second Party Sharing, 2008-2012 on Disclosure of Identities, 2011 & 2012 on Privacy Incidents File, 2009 on Privacy and Technology, 2007 on Client Relations Officers and Operational Policy; and
- Information Sharing Practices Reviews: 2013 on Second Party Sharing, 2008-2012 on

Disclosure of Identities, 2008 Support to CSIS, 2007 Client Relations Officers and Operational Policy, 2006 Support to RCMP Review (Phase II).