


Communications Security
Establishment

Centre de la sécurité
des télécommunications

TOP SECRET // COMINT // CEO

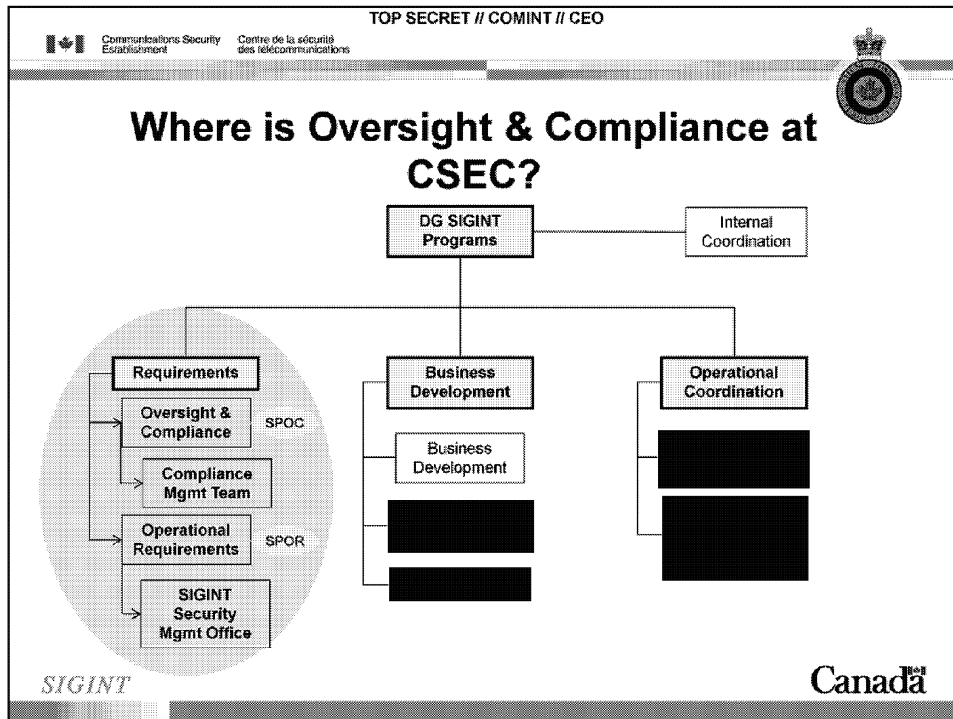


Overview

- **Why is there an office of Oversight & Compliance ?**
- **What does Oversight & Compliance do on a daily basis?**
- **What is the difference between SPOC and D2?**
- **When should I contact SPOC?**
- **Group exercises**

SIGINT

Canada



- SPOC fits under the Directorate General SIGINT Programs (DGP), within the directorate of SIGINT Requirements

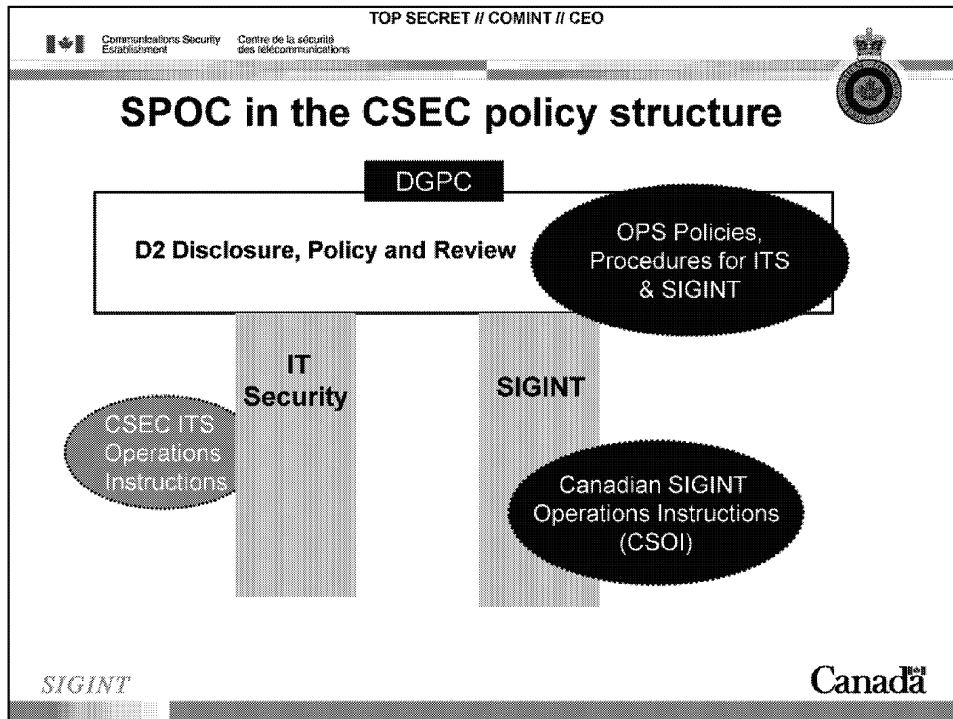
- This directorate is responsible for formally stating our operational, capability and compliance requirements for DC SIGINT

- SIGINT Programs Oversight & Compliance – SPOC – compliance requirements, such as compliance audits, upgrades and evolution

- SIGINT Programs Operational Requirements – SPOR – [REDACTED], National SIGINT Priorities List (NSPL), strategic pursuits

- Side note – directorate evolved from a single individual, [REDACTED] who was responsible for all these areas; we are moving away from single point (unmanageable) to a processes which will better capture & track these requirements

- Having all these functions under a single directorate enables better accountability because they are centralized



- As you will see in a few days, D2, is a part of Disclosure, policy and Review; they are responsible for corporate level policies, articulates in OPS documents (e.g., OPS-1)

- These documents apply to all of CSEC (ITS and SIGINT)

- Within IT Security and SIGINT, there are obviously a number of specific policy needs that need to be met

- ITS has the Cyber-Defense Support Office (CDSO) which is responsible for the ITS Operations Instructions

- SIGINT has SPOC – and we are responsible for the Canadian SIGINT Operations Instructions or CSOIs, among many other things

TOP SECRET // COMINT // CEO

Communications Security Establishment / Centre de la sécurité des télécommunications

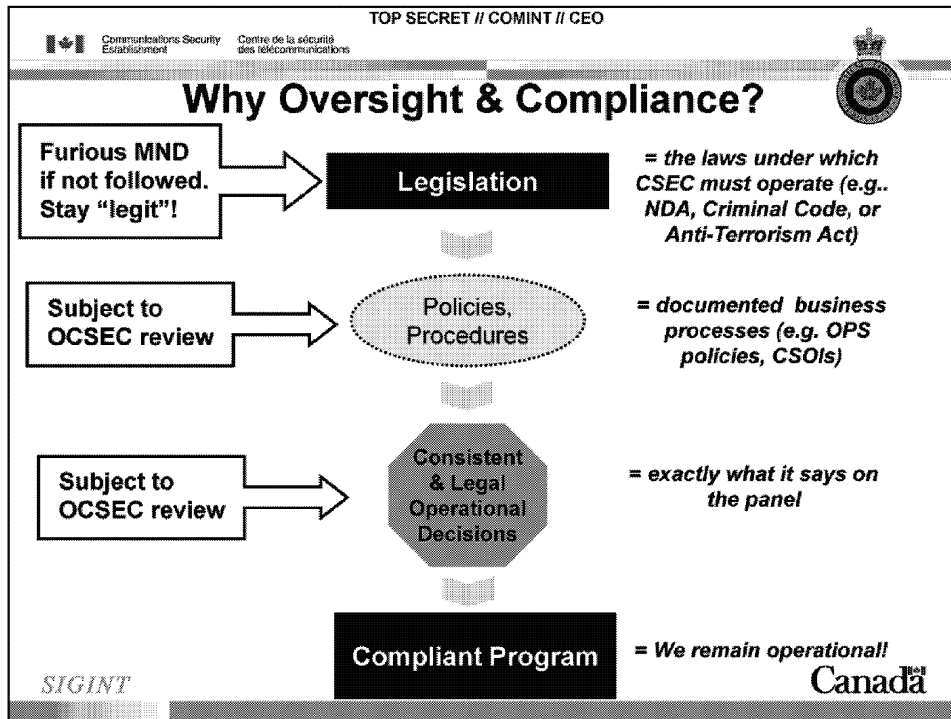
Comparison of D2 and SPOC Responsibilities

<ul style="list-style-type: none">• D2 operates for ITS <u>and</u> SIGINT• D2 states the rules (e.g., OPS documents)• Ident requests, sanitization requests• Tracks privacy violations and responses	<ul style="list-style-type: none">• SPOC is for SIGINT only• SPOC advises on the specific procedures in place to ensure compliance with the rules (e.g., CSOs)• Mitigates privacy violations
---	--

SIGINT

Canada

- D2 is responsible for all operational policies, procedures and guidelines for legal compliance, protecting the privacy of Canadians, and for activities directly related to CSEC's mandate.
- SPOC, on the other hand, is the main Point of Contact for all SIGINT policy requests. SPOC also acts as the main interface to all SIGINT groups for policy-related questions and is responsible for liaising with D2 as required.



PAGE 18 in textbook

•**Legislation** states the mandate; is interpreted in policies and procedures, which document the business processes that ensure

operational decisions are consistent with our legislated mandate - this is the National Defence Act and our Ministerial Authorization & Directive Framework that D2 talked to you about earlier.


•**Policy, procedures, instructions** enable staff to make consistent decisions in their day-to-day operations to make the organization run more smoothly; to be accountable -- respond to audit and review - these are the OPS documents and our Operational Instructions.

•As a result of documenting our business processes and compliance requirements in these policies & procedures, we make more consistent operational decisions.

•Not only does SPOC ensure compliance – we also work hard to emphasize consistency.

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications



Our Legislation: The National Defence Act & CSEC's Mandate

- **Part A: Provide intelligence from the global information infrastructure (SIGINT)**
- **Part B: Protect the systems of most value to the Government of Canada (IT Security)**
- **Part C: Provide operational and technical assistance to security agencies (Support to Lawful Access)**

SIGINT Canada


Provide a brief review of the National Defence Act and our Mandates.

One mandate, three parts

Mandates A & C are most relevant to SIGINT. Mandate B applies to IT Security.

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications



CSEC Mandate Part "A" has key tests:

- Involves Global Information Infrastructure (GII) exploitation
- Solely to obtain Foreign Intelligence (FI)
 - Capabilities, intentions or activities;
 - Foreign individual, state, organization or terrorist group
 - Relate to international affairs, defence or security
- Addresses Government of Canada Requirements (GCRs)
 - Established by a Ministerial Directive and organized by GC intelligence priorities
- Not directed at Canadians anywhere, or any person in Canada
- Measures must be in place to protect the privacy of Canadians

SIGINT

Canada

Does what you are about to do meet the criteria here?

- Are you directing your activities against a foreign target located outside Canada?
- Do your activities relate to international affairs, defence or national security?
- Do your activities support a GCR?

-If yes to all, then you may proceed. If no to any, you cannot proceed.

-Measures to protect Canadians include the annotations process that you heard about from D2 (i.e., determining whether or not a private communication, information about Canadians or communication involving a Canadian meets the essentiality test).

-Handling procedures in place in each of your respective areas as to the storage and tracking of this information. We are also in process of drafting a CSOI to standardize these procedures.


-Reporting sign-off levels reflect the sensitivity with which we handle these types of communications, as well.

IRRELEVANT

IRRELEVANT

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications



Other Legislation

- **Canadian Charter of Rights & Freedoms** – States the right for Canadians to be secure against unreasonable search or seizure
- **Criminal Code** – Defines activities (such as intercepting private communications) that CSEC requires MAs to address
- **Privacy Act** – Outlines Canadians' right to privacy and the government's responsibility to protect private information
- **Anti-Terrorism Act (2001)** – provided a new mechanism under which we could conduct our activities - the Ministerial Authorizations and Ministerial Directives


SIGINT

Canada

These will be covered in more detail in a few days during the D2 presentation.

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications



What are Ministerial Authorizations (MA) and Ministerial Directives (MD)?

- **MA**s protect us legally from the incidental collection of private communications while conducting our foreign intelligence collection activities, subject to explicit conditions
- **MD**s provide us with specific guidance from the **MND** as to how we should do our business

SIGINT Canada


Review

We are permitted to disclose but not release some MAs and MDs

Other, more generalized MDs are available on the D2 website

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications



Ministerial Authorizations

- **MA**s are currently in place for each of our collection programs: [REDACTED] Activities in support of the GoC in Afghanistan, and [REDACTED]
- SPOC evaluates changes to these programs to ensure that we continue to meet the conditions of the MA and OPS-1 (Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities)
- Changes may include upgrades to collection equipment, or requests to expand our collection capability to include new technologies

SIGINT


Canada

SPOC needs:

- to understand what is included in the MAs, the corresponding OPS documents and be up-to-date on:
- technical changes or upgrades to these collection programs – to ensure we meet the MA conditions; document these changes
- Determine if any CSOIs are required, associated with the MA activities
- Ensure management monitoring practices are in place to identify any compliance weaknesses (in progress)

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications



Ministerial Directives

- ***Ministerial Directive on the Collection and Use of Metadata*** relates directly to SIGINT activities and stipulates a number of conditions
- **SPOC** provides guidance to SIGINT on what constitutes metadata, how metadata can be used, and evaluates the measures in place to protect the privacy of Canadians


SIGINT

Canada


In the case of this MD, SPOC works closely with analytic and technical areas to:

- Ensure the correct definition of metadata is applied
- Ensure that people had the flexibility to do the queries they need to, while remaining compliant under the MD
- Developed an approach to “minimize” or protect Canadian identifiers in metadata before sharing it with Second Parties

TOP SECRET // COMINT // CEO



Communications Security Establishment
 Centre de la sécurité des télécommunications



SPOC exists to ensure we...

- ***Demonstrate* lawfulness**
- ***Meet the conditions* of CSE's Ministerial Authorizations and Ministerial Directives**
- ***Establish internal controls* and awareness**
- ***Identify and address procedural weaknesses and risks***
- ***REMAIN OPERATIONAL!***

SIGINT

Canada

Demonstrate lawfulness (don't take it personally; we can't take your word for it, we have to show it).

•Current climate: read the newspapers **IRRELEVANT** (Iacobucci inquiry -- Canadians have a right to know we are operating scrupulously within the laws of Canada) – inquiries, reviews: SCRUTINY

•Pre legislation: fewer employees; lower profile; different context; oversight procedures are new for much of the CSE workforce.

•While employees are largely aware of their responsibilities, the “oversight” mechanics are new. This is different from how we operated in the past.

Internal controls: “it’s a basic “best practice”

•Given the growth of the organization, it is a management responsibility to ensure that we document what our practices and procedures are, and then to ensure that these documents and their meaning are clear for employees. Without clear direction on this front, employees are not adequately prepared to be fully functional public servants.

•Management needs to develop op'l instructions, keep them updated, continuously strive to ensure that employees are aware of the limits and parameters within which they can do their jobs.

•our ongoing activity relies on you and your awareness of what is and is not appropriate behaviour or activity in our business

Identify weaknesses – these can be identified by knowing which areas/activities do not have enough guidance provided to them, or in the case of errors, we can determine where we need more monitoring or advice

•SPOC cannot be everywhere at once, so in part, we rely on employees to identify areas of weakness to us and we work with them to respond

•SPOC needs to hear from you with your questions & concerns in order to make us better at our job


Remain operational:

•MYTH – Policy says no to everything and is risk-averse. FACT: SPOC works very hard to ensure that SIGINT employees can do as much as possible within the existing policy framework and we work to change policy as well.

- MYTH: Policy is “overhead”. FACT – Policy is necessary to ensure we meet our legislative mandate appropriately. Canadian tax payers have a right to know that we are operating appropriately; it is our duty to demonstrate that we are. If we don't, we could have our Mandates and other authorities curtailed or revoked.
- Policy, instructions: these are enablers [cf your credit history]. We prepare for future activity TODAY –and beyond – by establishing and following policy / instructions – operational best practices

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications




CSOIs

- Issued under DCSIGINT's authority
- Provide direction on how activities are to be conducted within existing legal and policy framework
- Capture "lessons learned", so less time is spent thinking about how we could/should do something and more time actually doing it!
- CSOI-4-1 *SIGINT Reporting*, CSOI-4-4 *Targeting and Selector Management Using [REDACTED] National SIGINT Systems For Intelligence Reporting Purposes*

SIGINT

Canada


PAGE 19 – shows the different areas which CSOI's cover



Communications Security
Establishment

Centre de la sécurité
des télécommunications

TOP SECRET // COMINT // CEO



SIGINT

Canada

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications

What else does SPOC do?

- **5-Eyes** [REDACTED] issues including: metadata sharing, [REDACTED]
- **Priority SIGINT** policy files including: Cyber, ELINT and [REDACTED]
- **IRREL** and MA administrative and reporting duties
- **Liaise with Second Party SIGINT** policy
- **Circulation of OPS docs** within SIGINT for comment
- **Sharing of SIGINT data** (CSOI 5-3)
- **Operational questions**
- **Point of entry to SIGINT** for inquiries, ATIP and civil litigation

SIGINT Canada

5 Eyes [REDACTED]: 3 small words...

5 Eyes SIGINT relationship – let them think about that – what could it be?

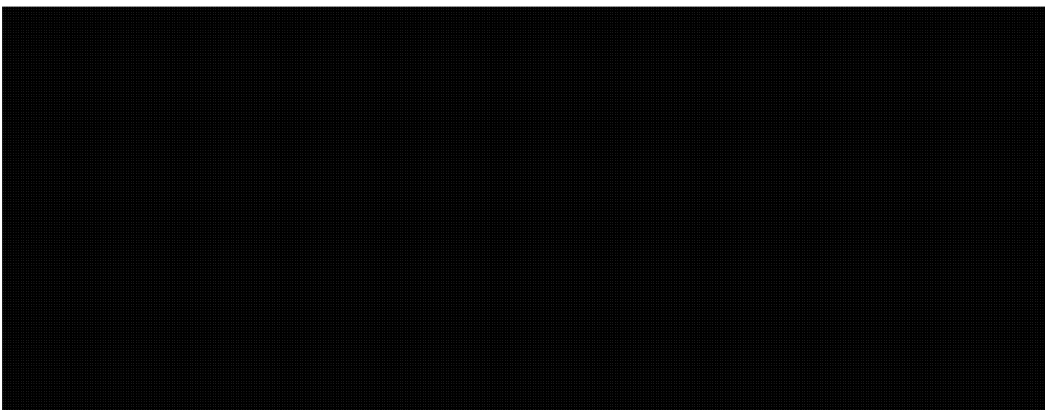
Documentation // explanation

How do we share data? [formats; policy; processes]

[REDACTED] legal and policy
compliance requirements need to be met

[Joke re 5 agencies separated by a common language ☺] – e.g., definition of metadata

SIGINT Policy and Legal Compliance Processes and technologies





New capabilities: what compliance requirements need to be factored in? [SPCR collab]

TOP SECRET // COMINT // CEO

Communications Security
Establishment

Centre de la sécurité
des télécommunications

The Office of the CSE Commissioner (OCSEC)

- **Office of the CSEC Commissioner (OCSEC) Reviews**
 - Has existed since 1996
 - Is separate and independent from CSEC
 - *Anti-Terrorism Act* of Dec 2001 formally established the OCSEC in legislation, through amendments to the *National Defence Act* (Part V.1)

SIGINT
Canada

Government of Canada inquiries

Examples: Air India; IRRELEVANT [redacted] Iacobucci (other 3)

SIGINT material required? SPOC is the contact.

Redaction of materials. What can be left in / what should be removed, and why.

What is already in the public domain?

If this is released, will there be a negative impact on CSEC / SIGINT sources?

Rationales [you need to give a reason for excluding material]

Complexity example: Air India: different systems; different customer delivery [sketch it out] – what information would have been available? Was Mr Bartleman right?

(reference litigation as well)

Access to Information and Privacy (ATIP)

DGPC – communications is the CSEC interface for ATIP; SIGINT material involved? SPOC is the contact.

Individuals want to know about selves or about cases from the past; some journalist queries: redaction – what to leave in and what to remove

It's not as straightforward as it might seem [press on ATIP but no one is equipped to deal with requests – systems not built to support; not costed]

INTERNAL REVIEW:

Internal audit – Dir AEE

Directorate of Audit, Evaluation & Ethics – independent advice on adequacy of management controls and risk management strategies

Evaluate the reliability of info used for decision making and performance reporting

Makes objective assessments of need for and cost-effectiveness of CSEC programs, policies, initiatives [see them on CCSE's web site]

This is to prevent the “monkeys guarding the bananas” scenario – it's a neutral party that examines mgt action

Internal audit: Active Monitoring – OPS 1-8:

oversee other areas' implementation of their monitoring practices (privacy angle) –

"Compliance Validation Monitoring"
OPS 1-8 relates back to lawfulness – "prove it"
Identify issues and address prior to a "privacy incident"

TOP SECRET // COMINT // CEO

Communications Security
Establishment


Centre de la sécurité
des télécommunications

OCSEC's Mandate


- **To review the activities of CSEC to ensure they are in compliance with the law and to advise the Minister and Attorney General of Canada of any activities that may not be in compliance with the law**
- **To receive complaints about the lawfulness of CSEC's activities**
- **To carry out specific duties under the "public interest defence" provisions of the Security of Information Act**

SIGINT
Canada

- Not the commissioner. The Commissioner.
- He and staff have access to CSE facilities, docs, personnel in conducting review of CSE activities to ensure they are in compliance with the law.
- Also concerned with safeguarding the privacy of Canadians
- Results go to Min National Defence
- OCSEC produces annual report; one version is classified, goes to Minister (and Cabinet); other is public, unclassified, and is tabled in parliament.
- SPOC spends a significant amount of time on reviews – in 2008-2009, approximately 10 reviews of SIGINT were ongoing, completed, or initiated and SPOC fielded 237 requests from the OCSEC
 - For example: Review of [REDACTED]
[REDACTED] Review of Information Sharing with Second Parties; review of targeting & selector management
 - SPOC is responsible, with the relevant areas of SIGINT, for implementing recommendations as the result of these reviews

 Communications Security Establishment
Centre de la sécurité des télécommunications

TOP SECRET // COMINT // CEO




Wrap Up


- **CSEC activities limited by legislation, Ministerial Authorization & Ministerial Directives**
- **CSEC's adherence to these limitations is subject to audit and review**
- **CSEC must also report on its compliance efforts.**
- **All of CSEC's activities are subject to review by the Office of the CSEC Commissioner**

SIGINT

Canada

 Communications Security Establishment
Centre de la sécurité des télécommunications

TOP SECRET // COMINT // CEO




Wrap Up

- **Failure to meet conditions set out by legislation or the MND can result in loss of credibility, diminished resources and, in the worst case, program suspension**
- **SPOC provides guidance to help ensure compliance, facilitates CSEC Commissioner reviews, and reports on compliance**
- **SIGINT REMAINS OPERATIONAL!**

SIGINT


Canada



Communications Security
Establishment

Centre de la sécurité
des télécommunications

TOP SECRET // COMINT // CEO



Final Thoughts on Compliance

- How we do things is as important as what we do.

Oversight and Compliance Ensures:


- **SIGINT activities are conducted legally**
- **CSEC powers are not abused**
- **CSEC can maintain the trust of the government & the people**
- **Public complaints can be avoided as a matter of principle and practicality**
- **Privacy of Canadians is maintained**

SIGINT

Canada

TOP SECRET // COMINT // CEO

Communications Security Establishment Centre de la sécurité des télécommunications

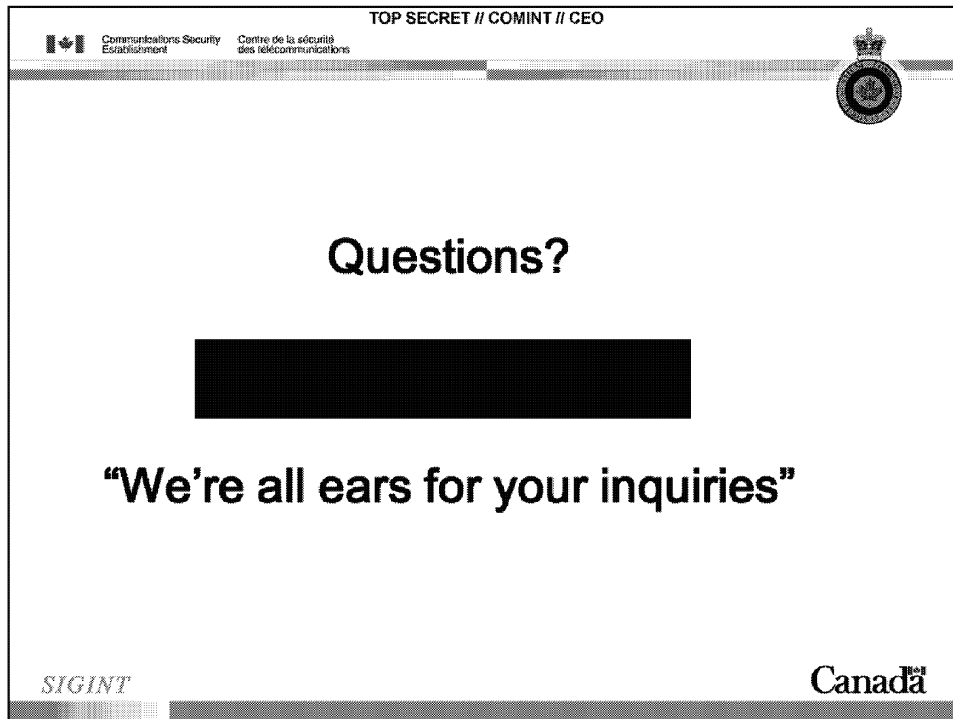


When can I contact SPOC?

- **Anytime!**
- **Contact our alias “[REDACTED]”**
- **If your response is better addressed elsewhere, we will put you in touch with that area**

SIGINT Canada

- Don't view SPOC as a toll-booth on your information highway! Instead, start out by coming to SPOC early and often to discuss your questions and concerns during the development stages of your project or activity.
- Don't be in the position of asking for forgiveness – ask SPOC for permission instead!
- SPOC works very hard to ensure that SIGINT employees can do as much as possible within the existing policy framework and we work to change policy as well. If you feel that a certain policy is lacking in any way, tell SPOC about it and we'll see what we can do to address that.



- Don't see SPOC and run! See SPOC run to your assistance!