


TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada



## What's on the Agenda?

- Who's Who? SPOC vs D2
- Incidents: Defined and How to Handle Them
- Privacy: What that Really Means to You
- Highlights of some of SPOC's Instruments and How They Affect You
- Data Retention and Stewardship Agreements

SIGINT


Canada

2

So today, we're going to review some of the stakeholders when it comes to policy here at CSEC. At the best of times when I first started here at CSEC, I had a hard time figuring out who did what and who I should talk to about an issue I had.


At the end of this session, I hope that you all will have a better understanding of some of the different policy areas and their key policies, which team to contact when you have an issue and how to be accountable when incidents happen.

About me: who I am, how long I've been in SPOC and what I do there.

 Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

TOP SECRET//SI



## Course Objectives

At the end of this course, you will have a better understanding of:

- the different policy instruments in SIGINT that affect you and your job
- what privacy incidents are, how to identify them and how to handle them
- proper data retention and stewardship agreements


*SIGINT*

Canada

3

TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada



## Who's who in the Policy Zoo

- There are many policy offices at CSEC but here are the ones SIGINT have relationships with:
  - **Corporate and Operational Policy (D group):** Featuring D1, D2 and D3
  - **Strategic Policy (B group)**
  - **ITS Policy Oversight and Compliance (IPOC)**
  - **And an honorary mention: Audit, Evaluation and Ethics (DAEE) Directorate of Legal Services (DLS)**

SIGINT

Canada

4

There are a lot of policy offices here at CSEC and to be honest you won't really have to interact with them. There are some key office that we work closely with that do affect how you are able to work:

Let's start with D group. There are 3 areas to D group:

- **Disclosure Management (aka D1)** is responsible for coordinating activities related to managing public disclosure of CSEC information either as evidence in legal proceedings and Inquiries or as requests made under the Access to Information Act and Privacy Act. D1 consists of two offices, Legal Disclosures (D1A) and ATIP Unit (D1B).
- **Corporate and Operational Policy (aka D2)** is responsible for the sanitization and release of suppressed identities and for ensuring CSEC's lawfulness and the protection of the privacy of Canadians
- **External Review (aka D3)** is responsible for CSEC's relationship with external review bodies, in particular, the Office of the CSE Commissioner (aka OCSEC). Once a year, the

Commissioner submits a public report on his activities and findings to the Minister of National Defence.

Next, Strategic Policy (aka B group). They aren't an area that you would interact directly with but they definitely affect how you are able to do your work. The important thing to remember about them is that they help coordinate our applications for ministerial directives and ministerial authorizations and produce the annual reports for the minister. These are what allow you to do the work you do everyday.


IPOC provides ITS cyber defence policy advice and guidance, facilitates reviews for ITS cyber defence operations, conducts ITS cyber defence compliance monitoring activities, and is heavily involved with policy development. They work closely with SPOC with regards to many items, including moving our joint Cyber Mission.

Again, you likely won't have any interactions with DAEE but they are important because they independently provide assurances on the soundness of CSEC's risk management strategy and practices, identify problems and provide recommendations for appropriate and available remedial action. SPOC works with DAEE in the sense that we received the report and coordinate the application of the recommendations.




DLS get a special mention as well. They provide legal services and advice covering the full range of legal issues touching the mandate of CSE, its policies and operations. They only accept requests from director and above so if you have any questions or concerns, bring it to SPOC and we'll raise it with them.

TOP SECRET//SI


Communications Security Establishment Canada    Centre de la sécurité des télécommunications Canada



## We all publish... stuff

- What policy instruments do they publish?
- SPOC (Go SPOC on Web 2.0)
  - CSOIs (Canadian SIGINT Operational Instructions)
  - SPIs (SIGINT Programs Instructions)/Guidance
- D2 
  - OPS procedures
- IPOC 
  - ITSOIs (ITS Operational Instructions)
  - ISPIs (ITS Simplified Program Instructions)/Guidance
- Cyber Mission
  - JOI (Joint Operating Instructions) - Joint Cyber guidance (from SIGINT & ITS)

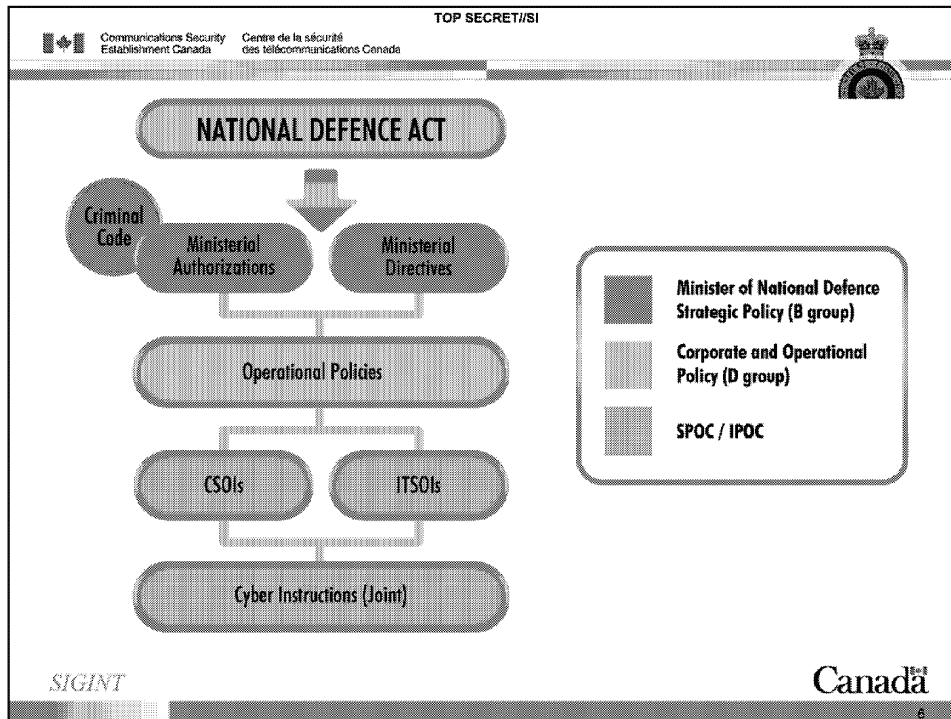
SIGINT

Canada 

5


All policy areas have policy instruments. The one you will likely be using most often are from the following areas. Can you guess which policy instruments each area publishes? There are treats involved...

All publications can be found on SPOC's website and a lot of times you can find the instrument by just entering the title in the search box from the main page. Or just to the group's page.



TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada



## Quick Policy Instrument Quiz!

1. Who produces SPIs?
2. Who produces ITSOIs?
3. Who produces OPS procedures?
4. Bonus question: Who is the lead singer of The Rolling Stones?

*SIGINT*

Canada


7

No really, it's quick!



TOP SECRET//SI

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



## Let's Dig In: SIGINT Programs Oversight & Compliance

- A refresher from SIGINT 101: What does SPOC do?
  - Verifies SIGINT's activities are conducted in compliance with CSEC's legal and policy framework
  - Performs internal oversight for SIGINT (compliance validation monitoring procedures)
  - Provides specific guidance to SIGINT personnel on how to conduct their work on a day-to-day basis.
  - Liaises external and internal audits and reviews
  - Provides guidance on projects proposals and tool development

SIGINT

Canada

8


1. As stated, SPOC works with SIGINT to ensure activities are compliant. This comes in the form of giving guidance, putting out documentations, working with other areas, helping them comply with policy

2. CMT Team

3. Under the authority of DC SIGINT.

4. From OCSEC and DAEE; oversees the implementation of recommendations resulting from these reviews

5. (e.g., Access to Information requests, government inquiries, criminal prosecutions and civil litigation suits).




Communications Security

Establishment Canada

Centre de la sécurité

des télécommunications Canada


TOP SECRET//SI




## What's the difference?

<b>Contact SPOC</b> (SIGINT Done Inside)	<b>Contact D2A</b> (SIGINT leaving SIGINT Channels)
<ul style="list-style-type: none"> <li>All SIGINT policy requests &amp; Questions</li> <li>Clarification of operational policies</li> <li>Responsible for Liaising with D2 as required</li> <li>Privacy Incidents</li> <li>Questions related to Raw SIGINT</li> </ul>	<ul style="list-style-type: none"> <li>Sanitization of EPRs</li> <li>Ident requests</li> <li>Contextual Idents requests</li> <li><span style="background-color: black; color: black;">[REDACTED]</span> Report Release requests from partner agencies</li> <li>Report Cancellations</li> </ul>

*SIGINT*




- Both SPOC and D2 have 2 very distinct functions.
- SPOC is responsible for All SIGINT policy requests, Clarification of a SIGINT Policy, Responsible for Liaising with D2 as required.
- 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. On top of that, they are also responsible for (read the list)



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

TOP SECRET//SI



## Compliance Management Team

Compliance Validation	Other Activities...
<ul style="list-style-type: none"><li>Validating SIGINT's compliance activities</li><li>Providing annual and bi-annual reports on SIGINT's compliance to senior management</li><li>Advising on projects and elements of SIGINT with privacy of Canadians and compliance focus</li></ul>	<ul style="list-style-type: none"><li>Development &amp; Life-cycle Management of Policy Instruments</li><li>Inadvertent Targeting, Naming and Collection Incidents Management</li><li>Annual MA reports to Minister</li><li>Supporting OCSEC reviews &amp; ATIP requests</li></ul>


SIGINT

Canada

10

TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada



## The 4 Ws... and then some of the SIGINT Production Chain (CSOI-1-2)

1. **Who:** CSEC employees/contractors, Second Parties, CF and CFIOG who operate under DC SIGINT's authority
2. **What:** S to the P to the C...
  - This refers solely to the production and use of SIGINT
  - Includes:
    - » SIGINT enabled activities
    - » SIGINT production activities
    - » SIGINT Oversight

SIGINT

Canada

11

What does SIGINT production chain mean? Basically it refers to the production and use of SIGINT... so what you do for a living pretty much.

What does it include? Well, it includes:

SIGINT enabling activities such as technologies or techniques that either facilitate or enable [REDACTED] SIGINT target of FI

SIGINT production activities such as tradecraft (as well as activities) that use information from the GII to generate FI; so SD analysis, reporting, and evaluating intel value

SIGINT oversight activities such as processes we've designed to assess and ensure the proper handling of SIGINT data; so monitoring for compliance with legislation, MDs and policy instruments; creating policy instruments and audit and review processes.


CSEC activities associated with the protection of networks of importance to the GC; this is ITS' part as certain areas are part of the [REDACTED] specifically the cyber defence mission. [REDACTED]

[REDACTED] of foreign threat actors. This is the current situation but things may change in the future.

What part 2? Well as mentioned, it refers to SIGINT data. This includes **Raw**

**SIGINT data**; an example of that would be comms content or metadata that has not been assessed for FI or altered to protect the privacy of Canadians and **Evaluated and/or Altered SIGINT data**; an example of that would be data that has been evaluated for FI. An example of altered data would be data that has been minimized or suppressed (which would protect the privacy of Canadians) or sanitized which protects the source of information.


Important point here: RAW SIGINT must stay within the SIGINT Production Chain... what does that mean? What Snowden did was literally taking RAW SIGINT OUT OF THE SIGINT PRODUCTION CHAIN!! In case you didn't realize it, that's a big no-no.



Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

TOP SECRET//SI



## The SIGINT Production Chain (con't)

**3. What part 2: SIGINT Data... what does that include?**

- » Raw data
- » Evaluated data
- » Altered data


**4. Where: Gotta be secure!**

If you're **NOT** part of the SPC; NO access to SIGINT data for you!

Other requirements? Legal Briefing! OPS-1 Quiz!

Questions about SPC? CSOI-1-2!

SIGINT




12

Who's part of SPC and therefore has access to SIGINT data? Well, that's a 2 part affair. Just because you work at CSEC or are part of the CF does not mean you automatically have access to raw SIGINT. You must also be working under the authority of DC SIGINT. This means if you are working in [redacted] group and you successfully compete for a job in Finance, when you move to your new job, you will no longer be part of the SPC and therefore will not have access to raw SIGINT. As with everything, you must also hold a SIGINT Information ACCESS (SIA) Indoctrination.

Where? I guess it's stating the obvious but SIGINT data can only be used in a secure accredited area that has been cleared for TOP SECRET.


If you are not part of the SPC, you should not have access to SIGINT data. ***This means if you go on assignment to another area, you and your supervisor must take the necessary steps which include, suspending/closing accounts to [redacted] [redacted] notify SSD so that your SIGINT accounts turned off/suspended for the duration of your absence or shut down completely if you've left SIGINT permanently.***

Are there exceptions? Sure! OK, not exactly. There are exceptions for [redacted] [redacted] but those exceptions are granted through SPOC management.

**Communications Security  
Establishment Canada**

**Centre de la sécurité  
des télécommunications Canada**

**TOP SECRET//SI**



**Break time!**

**back in 15**


*SIGINT*

**Canada**<sup>15 of 20</sup>

13

TOP SECRET//SI

Communications Security Establishment Canada    Centre de la sécurité des télécommunications Canada



## Privacy: Your Role

- What does CSEC mean by privacy and how do we protect it?
  - There's an OPS for that... OPS-1!
- Oh geez, that's a Canadian! What now?
  - What is a privacy incident?
  - The Privacy Incident File, aka The PIF: Why it's important

SIGINT

Canada

14

- Explain the gist of OPS-1: the protection of the privacy of Canadians.
- So what is considered a privacy incident? Well, according OPS-1:
  - If you have inadvertently targeted a Canadian or person in Canada: that's a privacy incident.
  - If you inadvertently use a Canadian selector [REDACTED]: that's a privacy incident.
  - [REDACTED]
- So what happens when there's an incident? Well, first and foremost, let me assure you that we know that mistakes can and do happen. SPOC and OCSEC realize that in this line of work, sometimes a target is not always clear cut. Sometimes a target is incredibly evasive with who they really are. What is important to OCSEC, our oversight body, D2 and SPOC is that swift and corrective actions and measures are taken. SPOC has tried to make reporting privacy incidents easier for you by providing web forms for you to fill out. We ask that you fill out the web form as completely and as detailed as possible. [one liners and such are not helpful and pretty much guarantee a phone call from us] The Compliance Management Team within SPOC will confirm all the information and then send




the incident and details to D2. D2 in turn will add the incident to the Privacy Incident File, fondly referred to as the PIF.

- What is the PIF? Well, it's a annual report that is created by D2 for the OCSEC commissioner to review. The OCSEC Commissioner reviews this file in order to confirm that when a privacy incident occurred, CSEC promptly reported and dealt the situation, therefore insuring that we have done everything we can to protect the privacy of Canada. For this reason alone, we ask you all to report privacy incidents as soon as you recognize them.

TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

## Inadvertent Targeting Web Form



*SIGINT* Canada

15

This is an example of what the web form looks like. Let's go over some of the fields so that you give us all the info... and we don't have to pester you about information you haven't included.



## Quick “How’m a doin’?” Quiz

- Question: What does SPC stand for?
- **SIGINT Production Chain**
- True or False: The SPC includes specific collection equipment.
- **False**
- True or False: I’m (as part of SPOC) part of the SPC.
- **True**
- Question: Can you give me an example of a privacy incident?
- **Inadvertently target a Canadian selector and or and/or name a Canadian in a End product report.**
- **Inadvertently use a Canadian selector** [REDACTED]
- **Inadvertently collect unselected content via CSEC equipment**


SIGINT

Canada

16

TOP SECRET//SI


Communications Security Establishment Canada    Centre de la sécurité des télécommunications Canada



## A Little Privacy, Please: CPRI and How to Protect It

- What's CPRI? Canadian Privacy-related Information
  - Refers to private communications, communications of a Canadian abroad or information about Canadians or Canadian Identity Information (CII)
- GII = Really complex...
  - it is inevitable that CSE analysts will come across CPRI while conducting SIGINT activities
- CPRI can be retained for three reasons
  - For FI, background info and to prevent inadvertent targeting
- STRICT measures in place to protect privacy and are outlined in several operational policy documents!

SIGINT

Canada 

17

Well it stands for Canadian privacy-related information and that includes raw SIGINT, reporting and other information. In your line of work, most of you are bound to run into CPRI so SPOC developed a CSOI to help you protect that information: CSOI-4-3 Protecting the Privacy of Canadians in the Use and Retention of Material for SIGINT.

CPRI which includes raw traffic (CTR) can only be retained for three reasons: Foreign intelligence value in the production of an End Product Report; background information to enable analysts to further develop foreign intelligence targets; and to prevent inadvertent targeting.

Additionally, there are a number of OPS documents to guide you: OPS-1 (of course!): Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities; OPS-1-1: Procedures of the Release of Suppressed Information from SIGINT Reports; OPS-1-7: SIGINT Naming Procedures; OPS-1-10: Operational procedures for Metadata Analysis [REDACTED] and OPS-1-11: Retention Schedules for SIGINT Data.

TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

**A Little More Privacy, Please: CPRI and How to Protect It**

- Severing of Data
- Need-to-Know, Ya Know?
- “Clean Desk” Approach
- Avoid Making Copies
- Restrict Access
- EPR Sign-off
- Retention and Storage of EPRs
- But wait, there’s more... CSOI-4-3!

SIGINT

Canada

18

This sounds pretty obvious, but it must be stated: Information that does not meet one of the three criteria for retention mentioned earlier needs to be removed from reporting and/or associated material.

Report drafts and associated material must only be reviewed and edited by individuals with a need-to-know.

A “clean desk” approach has to be adopted when dealing with a report in progress and its associated material. This means that when you are away from your desk you need to store your report and any associated material in a holding folder out of sight – either in a drawer or in the overhead storage of your workstation (which we won’t have at the LTA, so just remember drawers).

As a general rule, traffic items should not be copied. The exception is when there is a requirement to attach traffic and collateral material to the EPR. But... hardcopy material that’s no longer needed after the release of the report and which was not actually used in an EPR must be shredded in an approved shredder.


Traffic items may only be shared via email within immediate teams and when absolutely necessary, and in these instances CPRI should not be included unless it is

deemed absolutely essential. When this is the case, emails must be set up in such a way that they are easily identifiable as containing CPRI (i.e. in the subject line). You'll do this to ensure that they are deleted when no longer required or when the retention period expires. By the way, these emails may only be sent to those within the report release chain, D2 and SPOC.

The sign-off sheet, EPR and associated material must be hand delivered to the various signing authorities within SIGINT in a special "Privacy Information" holding folder. Also, these have to be in blue pouches when carried from one building to another (which is one more thing we won't have to worry about when we move to the LTA).


EPRs and their associated material must be stored in an approved security container in your operational area and the container must have restricted access. EPRs and associated material – including the completed sign-off sheet - must be retained [REDACTED] since they constitute what we refer to as the official record. When the approved security container has been filled to its capacity and your team requires additional space, older EPRs have to be sent to Information Holding Services (or IHS) for storage. And in cases where, for whatever reason, a team is disbanded, all files subject to [REDACTED] retention must be shipped to IHS (there are standard archiving procedures in place...). Also, when preparing to send material to IHS, boxes containing CPRI material must be visibly labeled "Contains Canadian Privacy-related Information" and "Canadian Eyes Only".

Don't get too excited, but there's still more to know: how to handle CPRI not used in the production of EPRs and how Level IV Managers complete mandatory reviews of all holdings. For these, you can consult CSOI-4-3.



Communications Security  
Establishment Canada

TOP SECRET//SI



**Break Time!**

**Back in 10**


*SIGINT*

**Canada**<sup>150</sup>

19

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

TOP SECRET//SI



## You Just Keep Me Hangin' On: Data Retention & Stewardship Agreements

- Bonus points: who made that song famous?
- Data retention! Again, there's an OPS for that! OPS-1-11
- The Traffic Fairy and Never-Ending Repository don't exist!

*SIGINT*

Canada

20

I bet one of my office mates that no one will know the answer to this. Full size chocolate bar to you if you can guess who made that song famous.

Data retention. It's an important topic and there's an OPS for it too. Like the misconception of the traffic fairy, the never ending repository does not exist either. Our system of record which in this case is the CTR has retention schedules that they must abide by.



TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

**Data Retention & Stewardship Agreements (con't)**

Myth-busting time!

1. It's no big deal to save a traffic item... or a few hundred to my desktop!  
False

2. Huh. I just found my first ever working-aid for a target CSEC doesn't even cover any more from 2007!! Meh, I'm keeping it for posterity!  
False

SIGINT

Canada

21

So anything you keep can be:


ATIP

EDRM (evidentiary disclosure risk management)

Need-to-Know – won't apply

Operational requirements – make sure it really is so that


CERRID (or [REDACTED] wiki) – if it's important, save it in a corporate repository.



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada


TOP SECRET//SI



## Data Stewardship - General

- Traffic (content) and Metadata
  - Criminal code implications
  - Ministerial Authorizations updated annually or we'd be out of business!
  - OCSEC are not CSEC
    - Review of CSEC's Activities
    - Thorough in their reviews
    - Can look at everything
  - Several policies in place to ensure proper handling & retention
    - The "corporate" SIGINT repositories have these rules built into them
    - Saving traffic or metadata off to your own folder = you are responsible for ensuring data continues to meet current policy requirements.

SIGINT



Privilege to have access to this information

Careful oversight by OCSEC

Not CSEC

Are very meticulous can see anything

MND yearly authorization allows us to collect and hold the SIGINT data we have, need to renew every year and account for what we did the previous year, stats, all PC used and not used counted, all traffic counted all reports counted, etc


Must have strict controls on who sees it and how it is handled

Particularly concerned with communications where one end is in Canada or is a Canadian

– contrary to Criminal code if not for the MA signed by the MND

The SIGINT corporate repositories have the controls in place that deliver metrics, delete files when they are up for deletion according to policy, can answer purge requests. They have all the checks and balances in place so that when OCSEC comes asking questions we can answer them. We can apply policy changes – ie AM marking, deleting incidental collect etc.


However, if analysts save traffic off onto their own we can't see it from a corporate perspective. The analyst will be responsible to be aware of the many policy rules that apply to the data they are holding onto and ensure they treat it the way it needs to be handled. If OCSEC conducts a review and finds these records it will be the analyst who will need to answer the questions.



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

TOP SECRET//SI



## Data Stewardship – Your role

- Leave the raw data (traffic and metadata) in the database
  - Use [REDACTED] for analytics when possible
- If you absolutely need to temporarily save a copy
  - Organize it so that it's easy to retrieve/find
  - Never keep it longer than the original is held in CTR
  - Ensure it is protected/retained in accordance with OPS 1, OPS 1-11, and CSOI 4-3
  - Be prepared to have OCSEC review your holdings
- Retention of raw traffic and metadata ≠ evaluated data
  - Data summaries and working aids may be retained as long as operationally required

SIGINT

Canada

23

What steps should you take to ensure you are policy compliant with your data.


Leave data and traffic in the databases whenever possible.

If you need to keep, only keep it temporarily until your finished with it, keep a folder where you keep traffic and regularly clean it out.

We are talking about raw traffic and metadata. If you've created a spreadsheet or working aid or have assessed the data and created working charts documents you may retain those as long as operationally required. It's just the raw SIGINT we are most concerned with. Also raw metadata **must** be deleted after [REDACTED]

TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada



## Wrapping Up

What are your take-aways from today?

*SIGINT*


Canada

24


What did you learn today? No, seriously, what did you learn today that you didn't know or maybe didn't totally get about 3 hours ago? I'll go first. I learned that you guys are really know so much, even though I bet you didn't think so. ☺

TOP SECRET//SI

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada



# Questions?

Contact us: @cse-cst.gc.ca

*SIGINT*

Canada

25