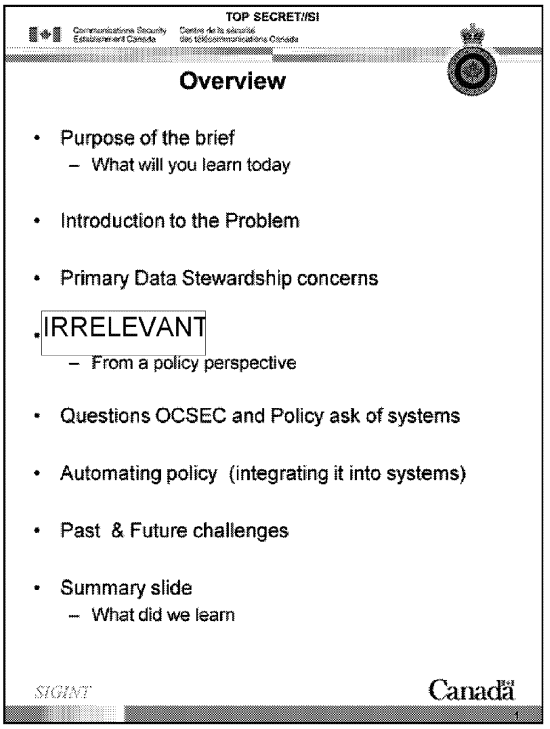


Welcome to the SIGINT System Development Policy Awareness Course (SSDPAC)

Here's an overview of what we will cover; the purpose of this session, I would like to know what you're hoping to get out of it and I can tell you what I have planned to cover.

If there are gaps between your expectations and I had planned then I will try to address them at the end or will follow up by email,

I will try to define what we consider to be the "problem" when it comes to systems development and compliance issues mainly around data storage, use.

We will talk about some of the main data stewardship issues we (SPOC) come up against in handling SIGINT data

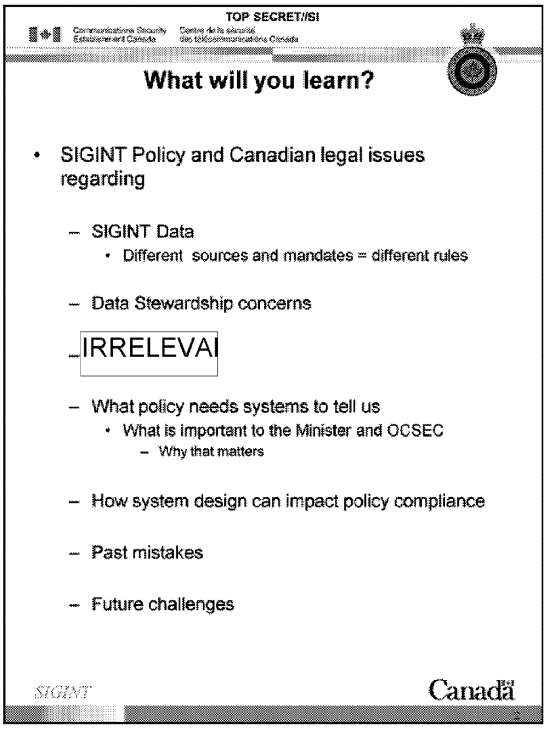
I will talk about IRRELEVANT from a policy perspective as we have a scheme in mind that we hope will fit nicely with CSE's current IRRELEVANT initiative.

From there we'll go over some of the questions the Minister and OCSEC ask us every year about our data- questions we hope systems will make it easy to answer as we move forward

Next we'll talk about ways we hope systems can help us automate some of our policy and compliance needs to make it easier for analysts and for ourselves to handle the data in a compliant manner

Finally I'll quickly go over some of the past issues we've come up against that we are hoping won't happen in future and I'll also discuss some of the current

challenges we have regarding handling and staying compliant



For this slide before putting the lines up ask the participants to shout out what they are hoping to learn, why they came, or why their boss sent them.

After everyone has had a chance to shout out their need, show them the bullet points you will cover.

I'm hoping by the end of this session you will know more about how SIGINT policy and Canadian law impact what we can do with SIGINT data

You will understand that data collected under different authorities or coming from different sources has different handling rules

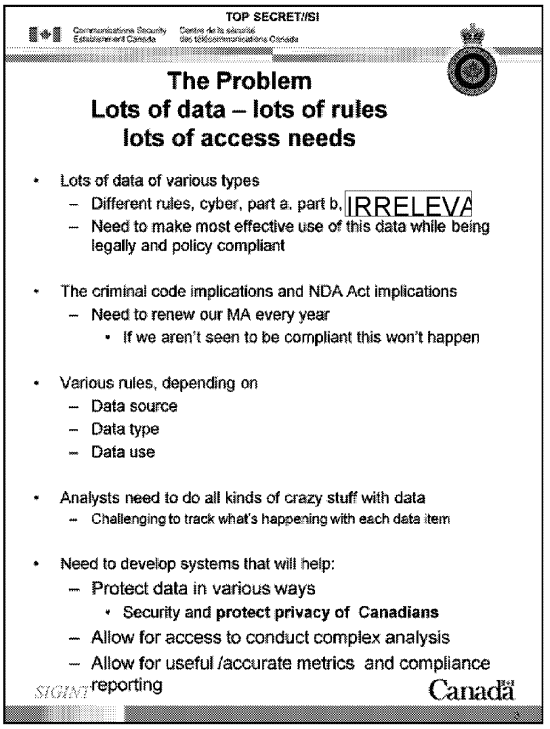
You'll find out the key policy concerns that come up regularly in handling data

You'll learn about SPOC's piece/place in IRRELEVANT

I'll tell you many of the questions SPOC needs to ask of systems on a regular basis in order to satisfy Ministerial and OCSEC requirements

I talk about some of the things systems have been able to do to help us with compliance and give you some ideas of how we think systems might be able to help us implement policy more effectively in future

Then I'll talk about some past issues we've had and current and future challenges we see in SIGINT data handling



Lots of Data and various rules

One problem is that we have tons and tons of data and tons of rules and it's sometimes difficult to figure out what rules go with what data.

For instance CSE can only collect SIGINT data under the authority of the National Defence Act section 273.64 part a, b IRRELEV

Part a – is data acquired for the purpose of providing foreign intelligence to the GC (SIGINT collected by CSE)

Part b – is to provide advice and guidance to the GC on protection of electronic infrastructure (ITS stuff)

IRRELEVANT

So the rules around data acquisition, use, storage, and sharing, are different depending on whether your data is collected under the a, b IRREauthority – For the purpose of this brief I'll only be speaking to part a IRRELEVAdata, that is data collected by SIGINT for the purpose of providing foreign intelligence IRRELEVA

IRRELEVANT

Part a data covered under Ministerial Authorization

Another important issue for us to continue collecting SIGINT data under Part A is

that we have to have a Ministerial Authorization signed by the MND every year by 1 Dec, (MA s run from 1 Dec of a given year to 30 Nov of the next year) in order to keep collecting SIGINT. If we don't get those Mas signed then CSE would be in violation of the criminal code. The only reason we are allowed to continue doing what we are doing without breaking the law is for us to get a signed ministerial authorization each year.

There are certain conditions we need to satisfy to get that authorization and one of the main ones is to REPORT on an annual basis what we are collecting, what we are doing with it, and how we are protecting privacy of Canadians while doing it. If we can't easily produce accurate metrics and be able to show that are systems are handling data in a proper manner and have measures in place to protect the privacy of Canadians then the Minister may decide not to sign our MA for that year. In addition, OCSEC the Office of the CSE Commissioner, completely separate from CSE, our oversight body, has the right to come in and look at anything they want to assure the minister that we are doing a good job at managing our SIGINT data and protecting the privacy of Canadians. If they come and see that our systems are not managing things well they will recommend changes to the Minister.

More about Rules

As stated earlier the rules are different depending on the authority under which the data was collected, part a,b, IRREL well the rules are also different depending on the source of the data, (CSE, [redacted] humint, etc). They also change depending on the type of data, raw SIGINT, assessed SIGINT, Content, metadata, collateral, etc. There are also rules that impact the way you are going to handle, use or share the data. Maybe it needs to be minimized before sharing with 2 parties but can be unminimized within CSE. Maybe it can't be shared will all 2Ps. Lots and lots of rules that need to be applied to the right types of data and not to other types of data.

Crazy Stuff Analysts want to do with data

So as if things weren't already hard enough we have those crazy analysts that want to do all sorts of weird things with data to find their bad guys. [redacted] for instance. Now why would an analyst want to have [redacted] analyse [redacted] traffic items all at once to see if they have any [redacted] Crazy I tell you! How can I possible ensure all those traffic items are properly annotated to protect Canadian privacy when they aren't even looking at them. As technology evolves we need to become more and more creative in handling data in order to get the best intelligence possible out of it, but we also need to remain compliant so that's a challenge (more on that later)

Need SIGINT systems that will help us

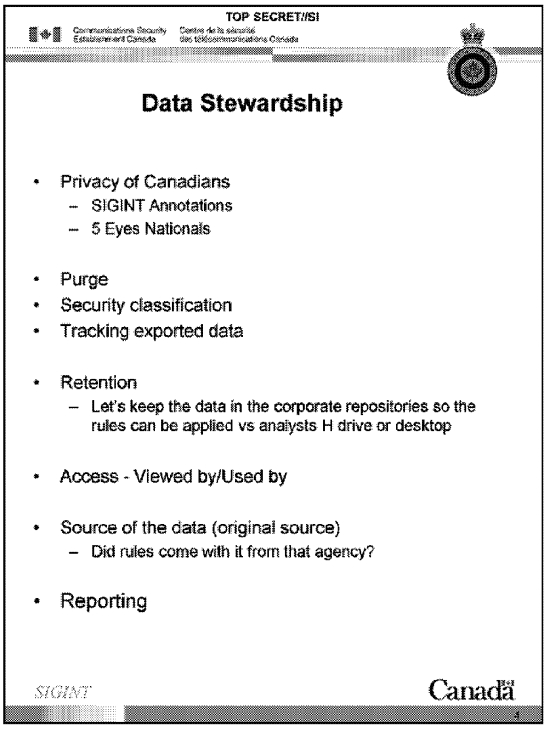
Need systems to not only protect each type of data according to it's bucket (I'll get into that in detail later), but also need to report stats as to what happened to the data from the time we collected it to it's final disposition on a yearly basis. One of the critical factors is how each system addresses the privacy of Canadians.

Please include us from the beginning when you are developing a new system or will be using data in a different way.

Where do the rules come from, the Law National Defence Act, Canadian Criminal Code – can't do what we do without the ND Act and our protection under MA s from the Criminal Code

-then Ministerial Directives that tell us how we will do what we do, down to OPS policies, CSOI Instructions, SPI Guidance

- Also get recommendations from OCSEC that require us to adjust our activities – case in point "marking" one end email [redacted]



Here is a list of the main data stewardship issues that come up regarding data storage.

Privacy of Canadians is always #1 for us, this is the key thing OCSEC is interested in. They want to know how are we collecting, using, storing, sharing/reporting, and retaining information about Canadians. So it will probably help to let you know what kinds of data fall into this Category. The key one here is raw SIGINT content. If you have intercepted an email or phone call on its way to a Canadian or anyone else in Canada - that it considered a private communication and this is where the Criminal code issues kick in. Under law you are not allowed to intercept private communications. You can not collect on anyone geographically located in Canada, this includes within 12 nautical miles of Canada. CSE does not target Canadians or anyone in Canada but we sometimes intercept communications coming from one of our foreign targets to someone in Canada. So that's why we need the MA coverage, to cover us from being prosecuted if we collect on of these private comms (PCs). When you hear us talk about private comms it's not just a "private" conversation or communication, a private comm is actually defined in the Criminal Code as a communication that has a sender or receiver geographically located in Canada.. So those are the intercepts we have to be very concerned about and which we need accurate metrics on. Also note that these must be intercepted while [redacted] to count under this PC definition. So for instance if you have [redacted] collection, you are [redacted] and you have [redacted] none of the [redacted] would be considered PCs because the data was [redacted]

data when we collected it. [redacted] So it's not considered a PC under the criminal code. Having said that two years ago OCSEC offered that we should be giving some type of extra protection to any [redacted] that is to or from a Canadian so we have instituted another type of rule to cover this data.

So you can see how things can start to get confusing really fast. The rules are changing depending on what type of collection collected it. Also in the privacy of Canadians category are communications of Canadians outside of Canada. Now these aren't considered private comms, not illegal to collect under the Criminal code, but CSE does afford extra protection to any comms we happen to pick up that are either to or from a Canadian outside of Canada. So the rules aren't quite as strict for these but still important. Finally we have the case of information about a Canadian. This is a communication in which two foreigners located outside of Canada are talking about a Canadian or a Canadian company. (For definition of Canadian see OPS -1). Also just want to give honourable mention to intercepted traffic that has one of our 2Ps partner's nationals as the sender or receiver. So first off, we don't target 5 eyes nationals. It's not against the Criminal Code to do that, at least I don't think it is, but it is contrary to our Five-Eyes Agreement. We don't target them, they don't target us. However, we may sometimes intercept one of our foreign targets talking to a 5-eyes national. If this happens the only special measure we have in place is that we won't name that 5-Eyes person in a report. So we don't have extra measures to protect the traffic in this case but we have extra measures to protect the naming of that person in SIGINT reports we write and send out.

Purge

Again this applies mainly to Raw SIGINT content, but any systems storing raw SIGINT content need to have a purge capability. The ability to purge data as required in a timely manner. The principle reason for this is that if have inadvertently collect a communication of a Canadian or person in Canada or a 5-Eyes person then we need to be able to find it quickly and purge it from the system. This can happen for a variety of reasons. Maybe we thought someone was a foreigner, they have a [redacted] number, are [redacted] but then we find out after a week of [redacted] this person that they are actually Canadian. When this happens there is a procedure analysts must follow which includes immediately detargeting the number and having the traffic purged and reports cancelled. So systems holding raw SIGINT traffic need to be able to purge.

Security Classification

Of course systems need to recognize the security access restrictions on various data items. I think in CSE we have this pretty well under control. But we also need to be able to change the classification on a piece of data if required. So much like the purge, we need to be able to find that piece of data and be certain that it's classification is changed and it's access is restricted to only those individuals who are allowed to see it. This is more a SPOR thing than

a SPOC thing.

Tracking Exported Data

After hearing about protecting data items or traffic that pertain to privacy of Canadians, the need to be able to purge or change classification you can probably imagine that this gets really tricky if copies of the data are located in more than one system or have been copied off on to the analyst's H Drive. This is a good spot to bring up [redacted] again, sorry one of my favourites. When [redacted] wanted to develop [redacted] they involved SPOC from that beginning so that we could ensure measures were in place to provide for the tracking of the data that would go to [redacted] to make sure it still followed all the rules it needed to follow. At the time we drafted a "stewardship agreement" that laid what we needed [redacted] to do in order to keep us compliant in handling the data. For instance, a copy of the data goes to [redacted] once the analytic has been run the copy if deleted from that server. So we still only have the one copy in CTR to worry about for purging. However, maybe an item that was used to produce a [redacted] result was subsequently purged from CTR, the analyst would have a result, let's say [redacted] chart, showing [redacted] purged after that result set was created. They would essential be using incorrect and uncompliant information. So [redacted] has built in a service that [redacted] if that item is purged at some point after the [redacted] the analyst is notified and told the delete their result set and [redacted] Bottom line is that we want all data to remain stored in the systems we are aware of that have the compliance measures built into them. Otherwise we could have traffic lying around or being used in reports that should have been purged.

Retention

Only keeping data for the length of time we are allowed to keep it is also very important. There are various rules depending on the type of data, source, authority under which it was collected, etc that tell us how long we can keep it. IRRELEVANT

IRRELEVANT

IRRELEVANT So there are lots of rules around retention that systems need to be able to implement. Again if data is held in private systems, or on private drives, it will likely not be deleted in accordance with it's established retention rules and if OCSEC finds it at some point it's a problem.

Access to Data viewed by versus used by

Another issue near and dear to our hearts is the difference between an analyst actually laying human eyes on a data item or piece of traffic and a process using the data to produce a result. The reason this is important comes back to the protection of the privacy of Canadians. The language in our policies says that we will annotate or mark a traffic item for protection with regard to privacy of Canadians when we "recognize" it to be a PC or communication of a

Canadian outside of Canada. In order to "recognize" it a human being has to determine first that it is one end Canadian, not just someone with a Canadian extension to their email address or vice versa a Canadian with a foreign email address for instance (analyst would be best positioned to know this) and second, they have to decide whether the item has Foreign Intelligence Value or not. We need to know whether the item has been "viewed" or not since this has implications as to whether it should have been annotated for privacy reasons. As you know our analysts don't view everything in the database. If no one saw an item that was to or from a person in Canada then it doesn't have to be recorded in our stats. So let's say OCSEC is reviewing some traffic and they notice that an item was not marked properly we would first have to determine if an analyst had laid eyes on it or not.

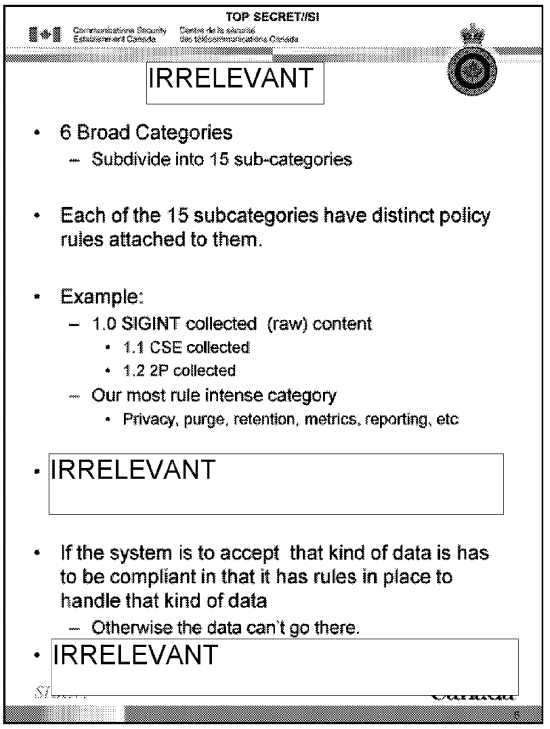
Going back to my favourite [redacted] again, if [redacted] uses a piece of traffic in a process it doesn't get annotated with a privacy annotation unless the analyst notices it in the output and then looks at it and annotates it. So we need to know the difference between viewed data and data that is accessed for a process and not actually looked at by human eyes. I believe this will be coming up in some [redacted] features as well. If you run a [redacted] from say an [redacted] shouldn't mark the data as viewed by until an analyst actually looks at that data.

Source of Data

Knowing the source of the data is always critical. You can't make any policy decisions until you know where the data came from. This is vital information when looking at data collected through SIGINT means but it is always very important for collateral data we get from other agencies. First off, if it's from another agency it falls under a completely different rule set and it is important to respect any rules the originator has imposed on the data as part of the sharing arrangement. For instance, we may get [redacted] and perhaps they have indicated that we are allowed to hold that data for 2 years, it is for our internal use only, and may not be reported. How are we going to keep track of those conditions? I think [redacted] made provision for that type of thing and if not I'll need to be certain they do!

Reporting

Rules on reporting also change depending on the type of data and source of data. Some data we aren't even allowed to report on we are only allowed to use it for target development purposes. Systems need to be able to track if data is used in reporting. For example [redacted] ties to CTR so we can look at a report in [redacted] and find the traffic items that went into that report. This is needed as we need to let the Minister and OCSEC know, on an annual basis how many PC traffic items were used in end product reporting. Also if traffic is used in a report it needs to be [redacted] retained.



So one day I'm sitting at my desk, my portfolio in SPOC is SIGINT Policy relating to "Tools and Tradecraft", I work mainly with SSD, [redacted] and [redacted] Group clients, and I realize that I keep getting the same kinds of questions over an over but with a slightly different twist. I'm trying to make my life easier so I tried to come up with all the possible types of data I've been asked about or know about and my plan was to find the policy box each one fell into. That way when someone asked I'd just point them to that box. I collaborated with a SPOC colleague who is really good at research and finding the right policy documents to cover various activities and we came up with 6 Broad categories that SIGINT data would fall into from a policy perspective.

Part "a" data

1. SIGINT collected Content (raw)
2. SIGINT collected Metadata (bulk)
3. [redacted]
4. [redacted]
5. Open Source

IRRELEVANT

But unfortunately we couldn't stop there as different rules applied depending on which agency collected the data, which agency shared the data, or what happened to the data before or after it got here. So those 6 categories were further broken down into

1. SIGINT Collected Content (raw)
   - 1.1 CSEC Collected
   - 1.2 2P collected SIGNT on behalf of CSEC

2. SIGINT collected Metadata (raw [redacted] see definition)
   - 2.1 CSEC Collected
   - 2.2 2P collected
   - 2.2.1 [redacted]

3 CSEC assessed (not raw) SIGINT data
   - 3.1 Transcripts
   - 3.2 End Products
   - 3.3 Working Aids

4. Non-SIGINT CSEC acquired data (part "a")
   - 4.1 From Other Government Departments
   - 4.2 [redacted]
   - 4.3 ELINT

5. Open Source

6. IRRELEVANT
   - 6.1
   - 6.2
   - 6.3

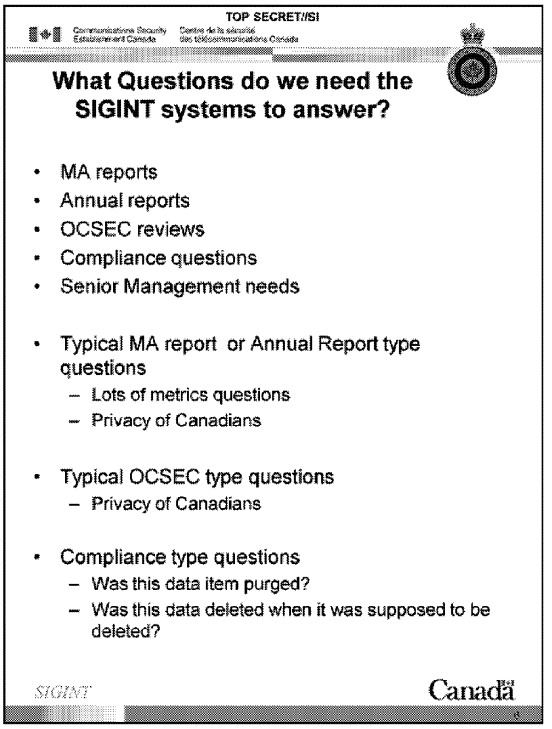
So I'll just walk you through an example, the category we are most concerned with and has the most rules attached to it, is the SIGINT collected (raw) content category. This category of data is directly linked to section 273.64(a) of the National Defence Act, by all three of our

SIGINT Mas, by 6 Ministerial Directives, the Government of Canadian Intelligence Priorities, 4 CSE Ops Documents and 2 CSOIs. Which means we need to be aware of the provisions that apply to this data contained in all of those documents to be certain we are handling the data in a compliant manner. The rules are slightly different within this category depending on whether CSE collected this data or if 2Ps collected the data on our behalf so we need to be aware of that detail when our systems handle the data. We need to provide lots of stats on this type of data. This category also has the greatest amount of overhead relating to privacy annotations and markings, purge requirements, and specific senior management sign-off for reports generated from this data where there is a Canadian angle to the traffic.

IRRELEVANT

Where do I find what the rules are for each type of data?

SPOC is working on a document that will probably take the form of annexes to a CSOI for data handling. Each annex will describe the type of data, the authorities that pertain to it and details on the compliant collection, use, storage, and sharing of that type of data.



I will focus on the Ministerial reporting, OCSEC review, and compliance questions since those are the ones I work with every day. But we are aware that Management also asks questions of data for operational reasons that I won't get into here.

We used to have 6 Ministerial authorities the Minister signed every year to cover all our collection activities last year it was condensed into 3 which makes a lot of sense and is much easier to manage. So the three MA s cover 1. [redacted] We have to submit a report every year with certain details pertaining to these various programs. If we are not seen to be answering these questions reliably and honestly then the Minister may not sign the next year's MA and our collection would cease until we got things cleaned up.

<u>These are called our MA reports</u>. So the type of information we need our SIGINT systems to provide for these reports are as follows; Between 1 Dec and 30 November for a given year,

How many intelligence reports did we produce based on traffic from this source

What topics did these reports cover

How many Canadian clients saw these reports

What are the departments of these Canadian clients

How many reports were seen by each department

What rating did the clients give to each of these reports

Of this total # of reports how many were based in whole or in part on private communications (traffic items annotated as INCA)

Of this total # of reports how many were based in whole or in part on solicitor clients communications (Canadian solicitor)(traffic items annotated INCAS)

Of this total # of reports how many were based in whole in in part on one-end Canadian communications (traffic items annotated OUCA)

How many reports were produced by 2P partners based in whole or in part on Canadian collection

A detailed list of these reports by 2Ps will be made available on request

How many total communications were intercepted

How many of those were PCs (how many marked INCA or INCAN at some point – but don't double count)

How many of those were Solicitor clients communications (how many marked INCAS or INCASN at some point but don't double count)

How many of those PCs were annotated for deletion, how many were kept, and how many were used in FI reports (and which reports were they used in)

Details on anything new or upcoming in the Collection area being reported on (ie [redacted] initiative was mentioned in the 2013-14 MA report)

A list including the title, what department saw it and the rating it received for every report produced by CSE for this source.

A list of all reports that used PCs

Total number of PCs intercepted

Total number of PC deleted

Total number of Solicitor client comms intercepted

Total number of solicitor client comms deleted

Total number of traffic items collected by CSE on behalf of 2p targeting and sent to them

<u>Fiscal Year report to the Minister</u>

How many items did we collect through [redacted] that were one-end Canadian email (AM Marking)

<u>OCSEC Review type questions</u>

We don't issues annual or regular reports to OCSEC, how OCSEC works is that they give us a work plan and tell us what activities they plan to "review" in the coming year. How many recognized private communications did you record in total

Of that total how long was each item kept that wasn't used in an EPR

How many were used in EPRs

How many were marked for deletion immediately upon recognition

How many were deleted each month

Number of traffic items with information about Canadians used in reporting (can't do this, no marking for it)

Number of traffic items of Canadians outside of Canada, intercepted, kept, deleted, used in reporting (OUCA, OUCAN, RPT or not)

Number of traffic items deleted as they contained information about Canadians (by source)

Provide background and information on the Privacy Picker tool

Provide background and information on the [redacted] in [redacted]

They like to have details on any privacy protection measures we are building into systems, so if you create these please keep a record of what you did and why.

Compliance Questions

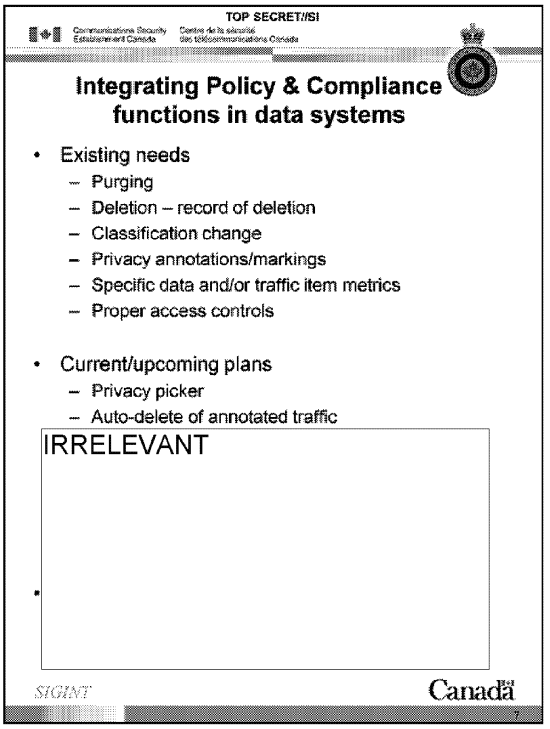
How many privacy incidents were there and details on each one

How many items were purged due to privacy incidents

How many items did we ask 2Ps to purge, did we receive acknowledgement for those

Did the systems delete the records they were supposed to – proof that the system are working properly?

Was data only accessed by people authorized to access it



Existing features/capabilities

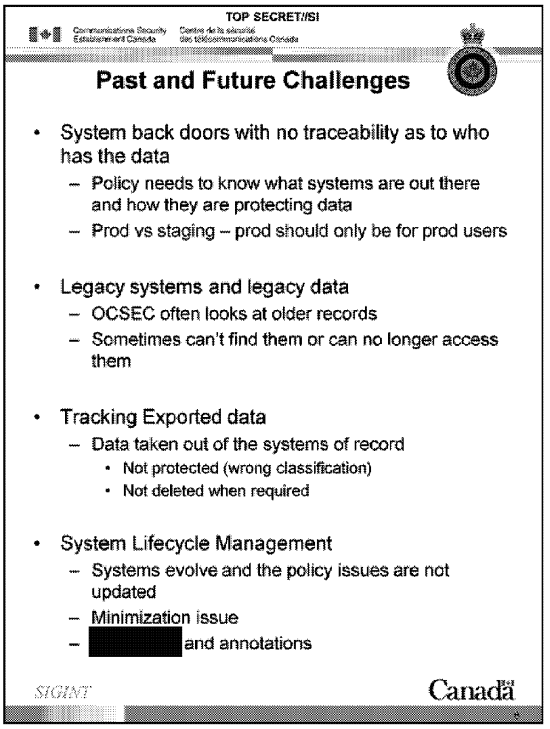
Some systems have already integrated policy compliance features. For example CTR is capable of purging data when we need it to be immediately purged, records are regularly deleted according to various privacy markings or other restrictions that have been written into the code. CTR provides analyst the privacy annotation feature so analysts can mark data which allows us to collect stats for our reports mentioned earlier. Most systems hopefully have proper access controls built into them before any data actually flows in.

Current/Upcoming plans

A fairly recent policy feature developed in SPOC was added to [redacted] to help analysts choose the appropriate privacy annotation for their traffic. The rules were so complicated, in order to cut down on the number of errors made by analysts, SPOC developed a tool to help them follow the rules more easily. We would like to have system designed in such a way that our policy concerns can be addressed automatically by the system whenever possible. Another feature we would like to see added to CTR is an "auto-delete" function for traffic items that have been marked for deletion and have not been used within a [redacted] time frame. This was an idea brought up by an analyst during a 2013 OCSEC review. OCSEC personally interviewed each analyst that had marked a PC for retention that year and had not used it in an End Product Report. The analyst had to explain why they marked the

item, what FI value it had to them. In most cases analysts legitimately marked the items of interest but then never got back to marking them for deletion when the project was over or the target was no longer of interest. This prompted the idea of an auto-delete and notification to analyst function. At the [redacted] after annotation of a Privacy item for retention the item will automatically be changed to not required for retention and a notification will be sent to the analyst. If the analyst still needs the item they can re-mark it and the [redacted] will begin again. OCSEC will be thrilled to hear of this once it's in place and the analysts are also happy as it makes less work for them.

IRRELEVANT



OK so I thought I would take some time at the end here to air some dirty laundry and talk about some of the problems we've seen that have caused us grief in the past and also talk about some of the challenges we're currently working on.

In one OCSEC review the issue had come up in which an analyst exported a bunch of rows of data from CTR, removed the classification, and shared it with 2 parties. So that wasn't good and it resulted in the thinking that all data should stay in the database because if it's there we can be certain that compliance issues are addressed. However, we later found out someone [redacted] could have exported data from CTR and no one would have known about it anyway. This back door was subsequently closed. All to say that we need systems to have the proper measures in place to protect the data we collect and we need to make analyst aware of their responsibilities if they take data out of the "corporate" repositories. We also had a problem a couple years ago when [redacted] the prod system for [redacted] development work and made quite a large error that affect [redacted] So very important that development is done on staging not on prod! Not sure if there are any policies business rules in place for system development in general in CSE that speak to these issues, we don't really see them as SPOC type issues but they are extremely important nonetheless and I think this might be a bit of a gap..

Legacy systems

Something we've run into a lot with OCSEC reviews is our inability to produce legacy data or stats on legacy data. OCSEC always reviews a "past" time period and it seems like we are also migrating to a new system and then we can't get an accurate picture of what happened to data before that system was in place. We are asking that when new systems are built someone needs to save documentation on what happened to the data that was held in the previous system. For instance an OCSEC review last year was looking for records of some CSIS messages that were sent to us. We log these in spreadsheets which have links to the actual documents themselves. Well the links only work for the last few years, any links prior to that are broken and CIO can't find the messages, fortunately for me OCSEC didn't specifically ask for any of those messages as I wouldn't have been able to produce them. IRRELEVANT

IRRELEVANT

When OCSEC can't find what they need

Just wanted to quickly inject what happens when OCSEC can't find what they need. At the end of each review OCSEC writes a report. This report goes to the Minister of National Defence. So for instance IRRELEVANT

IRRELEVANT

The idea I mentioned earlier of an "auto-delete" function for PCs that aren't used was borne out of an OCSEC recommendation. They actually recommended that we provide more stats, more than once a year, to the minister on PCs we keep. However, we felt that an auto delete function would be more effective in protecting Canadian privacy than providing more stats so we are addressing this recommendation with a slightly different solution. So we do have some leeway in addressing their recommendations but we do have to discuss that with them up front.

Tracking Exported Data

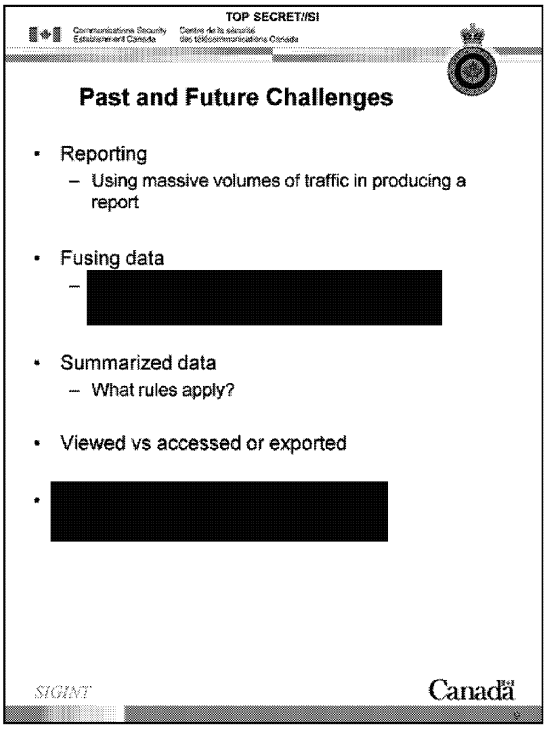
So we're getting better at this but this is something we are educating our analysts about. If you take data out of a "corporate" repository then YOU are responsible for all the policy baggage that goes along with that. For instance say an analyst saves a copy of a piece of traffic to his H Drive, what happens if that item turns out to be from a Canadian or person in Canada and needs to be deleted. The analyst won't necessarily know that and that item might stay in his H Drive for a year or so. Then another analyst uses that information in target development and ends up targeting a Canadian. Bad things can happen when analysts save data outside of the corporate system that has the policy pieces built into it.

System Lifecycle Management

This is related to the legacy system issue but it's more than that as well. If you are upgrading

or changing a system that handles SIGINT data please let SPOC know! We've recently had a huge problem with [redacted] The original system had all the right information in it, the right fields that needed [redacted] But over the years collection systems changed and the fields that needed [redacted] and eventually [redacted] Big, big problem because [redacted] It's important to make sure the policy implications have been looked at when upgrading/building new systems.

Even when new features are added it sometimes impacts policy. For instance [redacted] recently added the [redacted] functionality to [redacted] Didn't seem to be a policy issue so SPOC wasn't consulted. But later on we discovered that this new feature has a potentially huge impact on privacy annotations. The feature allows you to look at [redacted] The problem is what if the analyst has to annotate those for privacy reasons? The analyst has to go back one by one and annotate. Then what it they want to change the annotation? Now I'm not saying that we will be ahead of the ball all the time because maybe we wouldn't have even thought about this at the time, but it never hurts to pass your ideas by SPOC so we can try to think of any policy issues that might be important to consider.



Future Challenges

Reporting

Linking massive volumes of traffic used in a given report is a problem we see coming very soon and in fact is here already. I believe

Fusing Data

More and more we're seeing folks using a bit of data from this source and that source and combining it together in the production of an EPR. So the question is what rules apply to that data? IRRELEVANT

IRRELEVANT

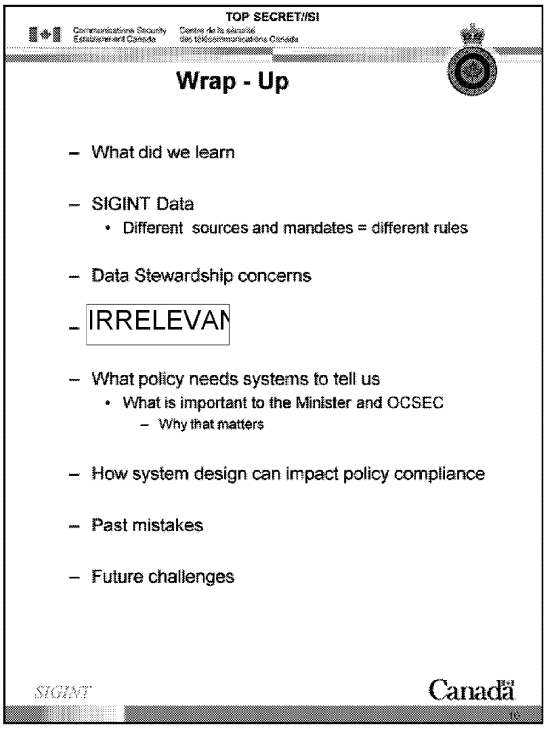
Summarized Data

IRRELEVANT

Viewed vs Accessed or Exported

So this is something that has recently come up with [redacted] If I run the data through [redacted] I don't want it marked as "viewed" because once I do that I am responsible to annotate it for privacy reasons and if I've just sent it to [redacted] I haven't actually looked at it so I can't make the FI determination nor the Canadianness of it so I can't annotate and haven't officially "recognized" it. OCSEC could come back and say, they viewed that Canadian PC why didn't they annotate it? If I don't know that it was just accessed by [redacted] and not actually viewed then I can't explain why this happened to OCSEC.

IRRELEVANT



Get them to tell you what they learned.

Put your bullets up after to see if we covered each of those.