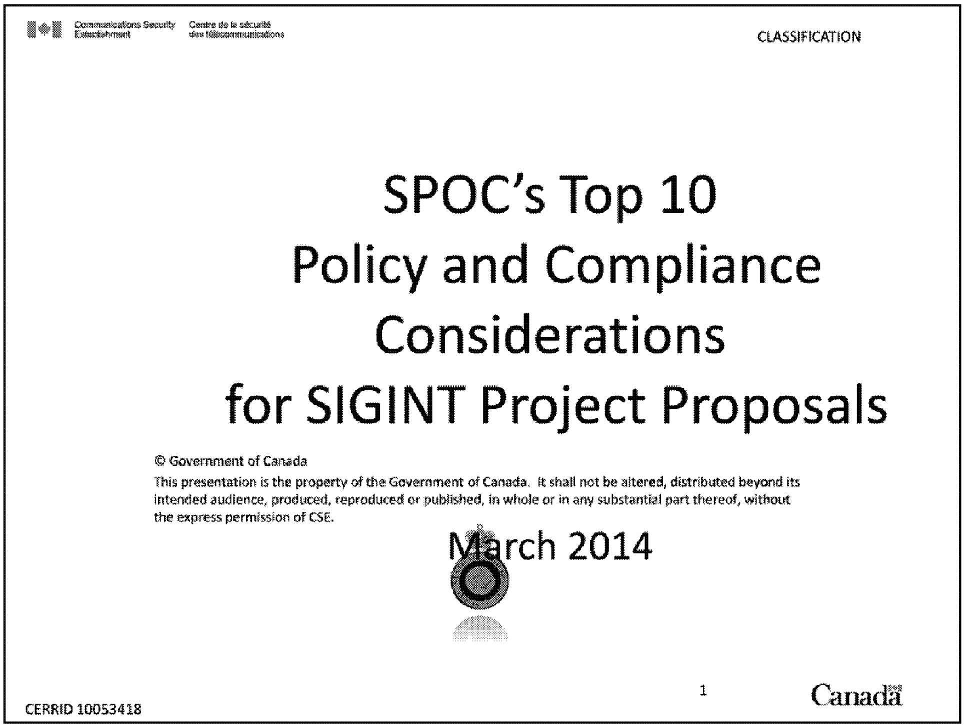


Communications Security Establishment
Centre de la sécurité des télécommunications

CLASSIFICATION

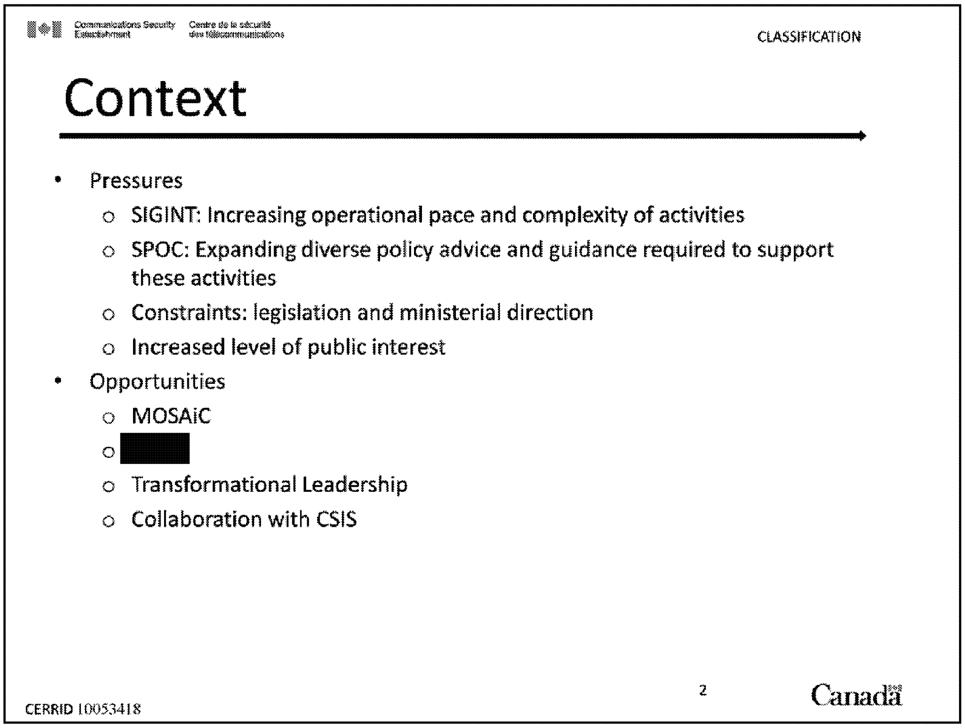
SPOC's Top 10 Policy and Compliance Considerations for SIGINT Project Proposals

March 2014

1

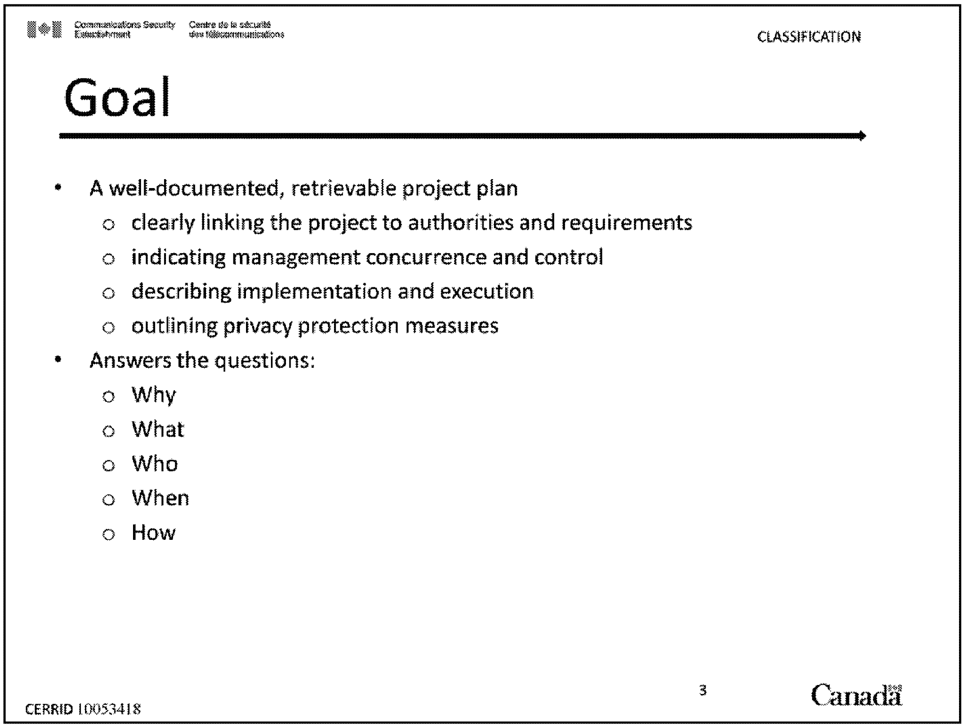
Canada

CERRID 10053418



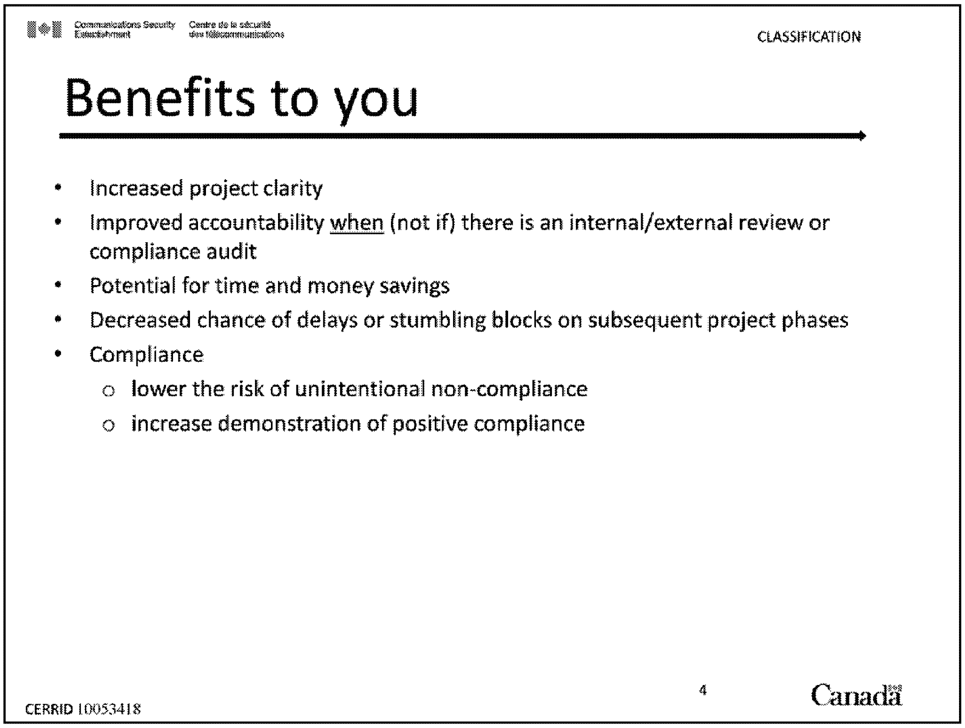
Context

- Pressures
  - SIGINT: Increasing operational pace and complexity of activities
  - SPOC: Expanding diverse policy advice and guidance required to support these activities
  - Constraints: legislation and ministerial direction
  - Increased level of public interest
- Opportunities
  - MOSAiC
  - [redacted]
  - Transformational Leadership
  - Collaboration with CSIS



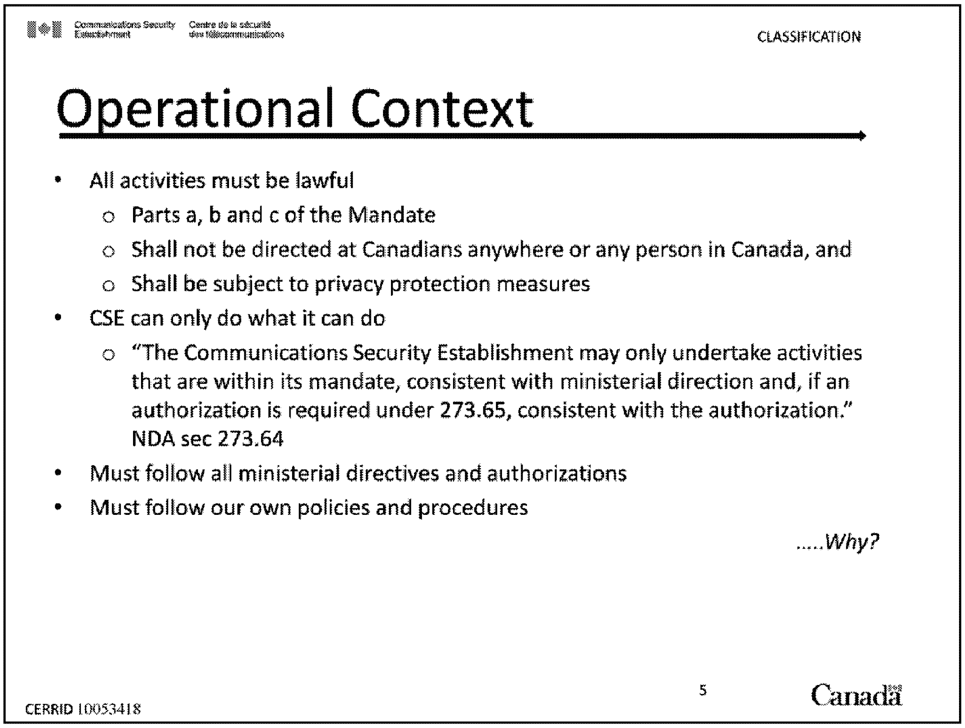
Goal

- A well-documented, retrievable project plan
  - clearly linking the project to authorities and requirements
  - indicating management concurrence and control
  - describing implementation and execution
  - outlining privacy protection measures
- Answers the questions:
  - Why
  - What
  - Who
  - When
  - How



Benefits to you

- Increased project clarity
- Improved accountability when (not if) there is an internal/external review or compliance audit
- Potential for time and money savings
- Decreased chance of delays or stumbling blocks on subsequent project phases
- Compliance
  - lower the risk of unintentional non-compliance
  - increase demonstration of positive compliance



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

Operational Context

- All activities must be lawful
  - Parts a, b and c of the Mandate
  - Shall not be directed at Canadians anywhere or any person in Canada, and
  - Shall be subject to privacy protection measures
- CSE can only do what it can do
  - "The Communications Security Establishment may only undertake activities that are within its mandate, consistent with ministerial direction and, if an authorization is required under 273.65, consistent with the authorization." NDA sec 273.64
- Must follow all ministerial directives and authorizations
- Must follow our own policies and procedures

.....Why?

CERRID 10053418

5

Canada

SIGINT is a system…dynamic and always in flux…thinking about SIGINT as a system is not just about the different parts, it's about how those parts interact.

Every step is related to another. Subject matter experts need to be concerned not only about their particular area of expertise but in how that relates to other parts of the SIGINT system.

Every activity is subject to review – from the idea, through its development, implementation, execution and winding up with an evaluation or a review.

Principles for Conducting CSE Activities

SECRET

Cerrid # 1316 70

Lawfulness/Privacy:

Activities are in accordance with the law e.g. NDA, Privacy Act, Charter, Criminal Code, international law/conventions

Activities are within CSE's mandate

o Fl in accordance with GC Requirements, or o Helping to protect systems of importance to the GC

Authority

Activities consistent with MDs, MAs

Satisfactory measures are in place to protect the privacy of Canadians

Activities are not directed at Canadians/persons in Canada

Only relevant/essential information is used or retained

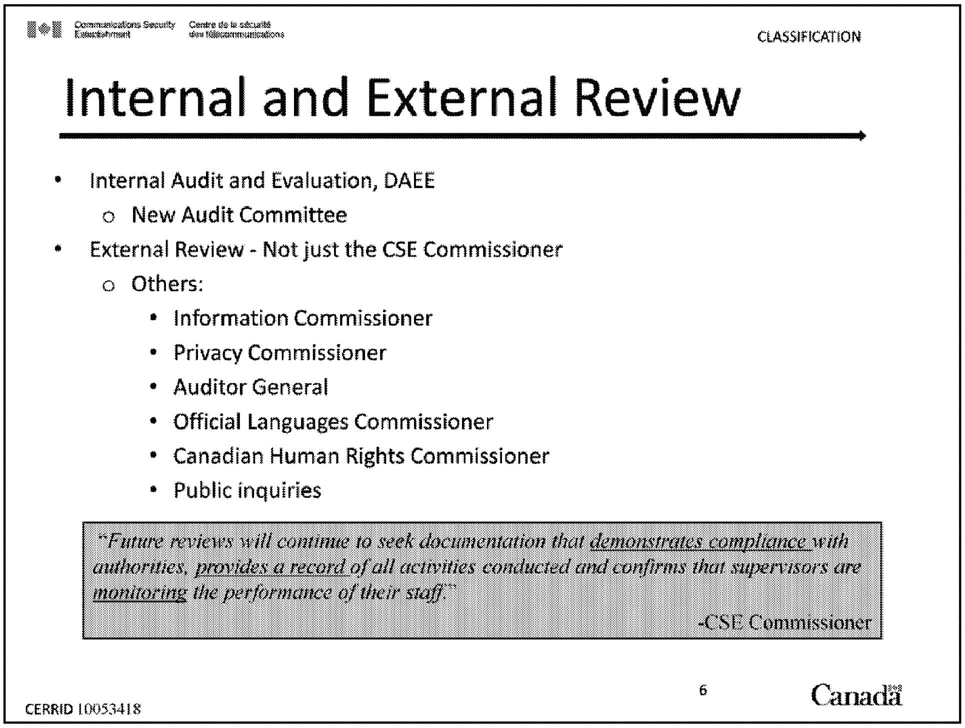
Core values of the Public Service are recognized

o Sharing information related to criminality

o Protecting Human Rights

o Placing greater importance on Solicitor-Client Privilege than private communications

- Public interest
- We have to demonstrate the above



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

Internal and External Review

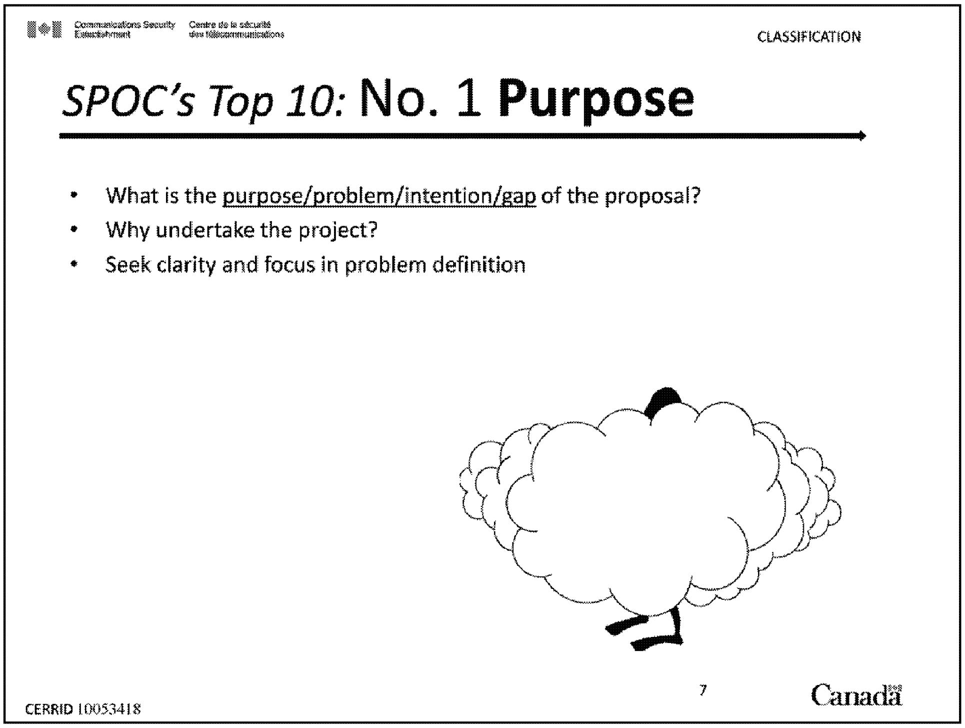
- Internal Audit and Evaluation, DAEE
  - New Audit Committee
- External Review - Not just the CSE Commissioner
  - Others:
    - Information Commissioner
    - Privacy Commissioner
    - Auditor General
    - Official Languages Commissioner
    - Canadian Human Rights Commissioner
    - Public inquiries

> *"Future reviews will continue to seek documentation that demonstrates compliance with authorities, provides a record of all activities conducted and confirms that supervisors are monitoring the performance of their staff."*
>
> -CSE Commissioner

6

Canada

CERRID 10053418



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10: No. 1 **Purpose**

- What is the <u>purpose/problem/intention/gap</u> of the proposal?
- Why undertake the project?
- Seek clarity and focus in problem definition

7

CERRID 10053418

Canada

Be clear and specific about what you're proposing to do – <u>What is your intention?</u>

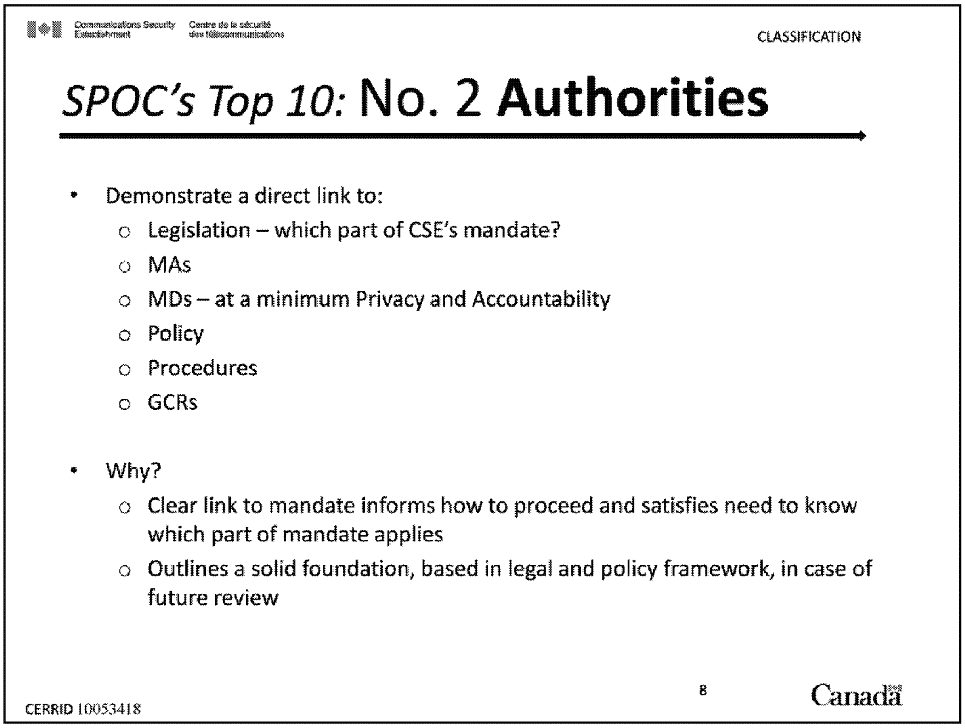
Work through the fog/clouds of information so that you're really clear about your purpose so that the project is of reasonable scope.

For example,

I'd like to set up an analytical database – to do what? For whom? With what data? Data from where? Using what tools? Will you share results? With whom? Through a report? How will you store the data? How will it be annotated? When will you purge it, and how? How long will you retain it? Does it touch on Canada or Canadians in any way? What will the client do with the info you provide?

However you write it up – use plain language. Write clearly so that someone outside of SIGINT could understand. Keep it simple.

Simple does not mean simplistic. It does mean clear, direct and unambiguous.



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10: No. 2 **Authorities**

- Demonstrate a direct link to:
  - Legislation – which part of CSE's mandate?
  - MAs
  - MDs – at a minimum Privacy and Accountability
  - Policy
  - Procedures
  - GCRs
- Why?
  - Clear link to mandate informs how to proceed and satisfies need to know which part of mandate applies
  - Outlines a solid foundation, based in legal and policy framework, in case of future review

8

CERRID 10053418

Canada

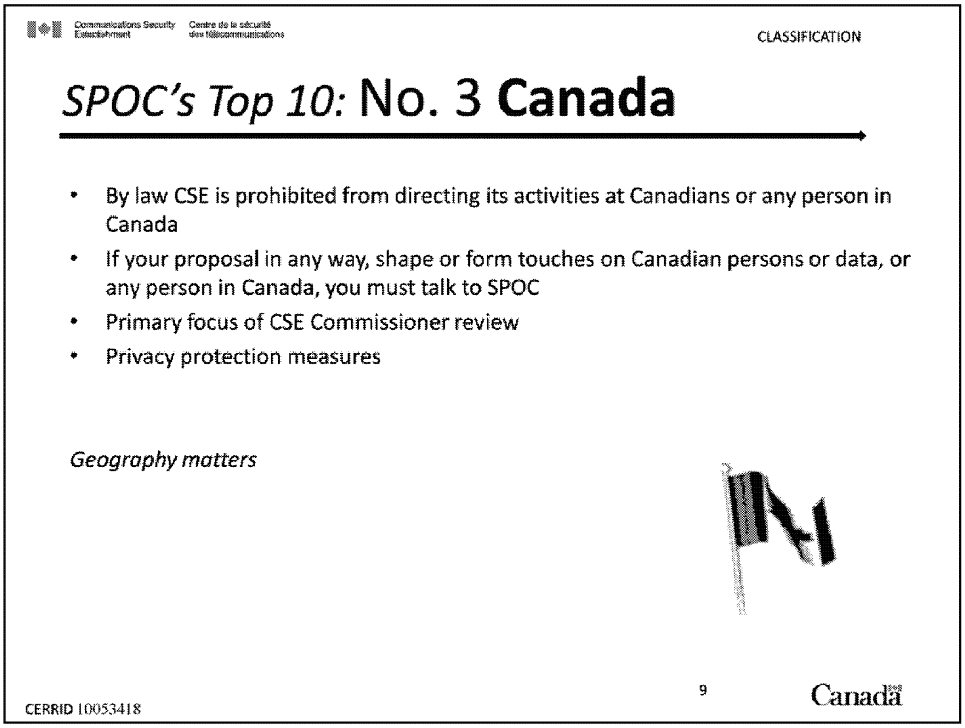
The CSE Commissioner has, in the past, expressed concern about knowing under which part of the mandate CSE is carrying out its activities.

Solicitor-Client Privilege

When we know under which part of the mandate we're working, we know which policies and part of policies apply.

If an MA does not apply – that is, if there is no interception or interaction with a private communication - specify that and explain why.

Identifying the relevant GCRs aligns the SIGINT activity with a Government of Canada identified intelligence priority.



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10: No. 3 **Canada**

- By law CSE is prohibited from directing its activities at Canadians or any person in Canada
- If your proposal in any way, shape or form touches on Canadian persons or data, or any person in Canada, you must talk to SPOC
- Primary focus of CSE Commissioner review
- Privacy protection measures

Geography matters

CERRID 10053418

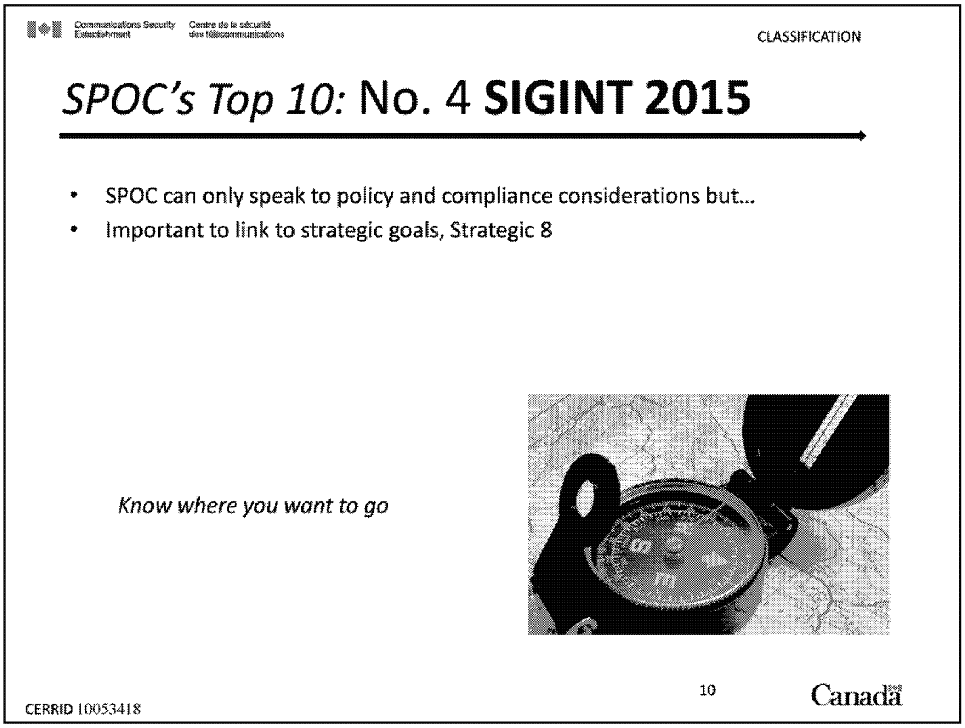
9

Canada

Having any kind of Canadian angle to your project makes it more attractive for review by the Commissioner.

The Commissioner's primary role is to ensure that CSE's activities are not directed at Canadians or at any person in Canada.

That's what policies and instructions lay out - For example:
Targeting —CSOI-4-4
CC– OPS-1-10
Reporting – all in line with OPS-1 and OPS-1-7 and CSOI-4-1
Retention – all in line with OPS-1-11



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10: No. 4 **SIGINT 2015**

- SPOC can only speak to policy and compliance considerations but…
- Important to link to strategic goals, Strategic 8

Know where you want to go

CERRID 10053418

10

Canadä

Prioritization has been figured out…Strategic direction has been set by senior management in

SIGINT 2015:

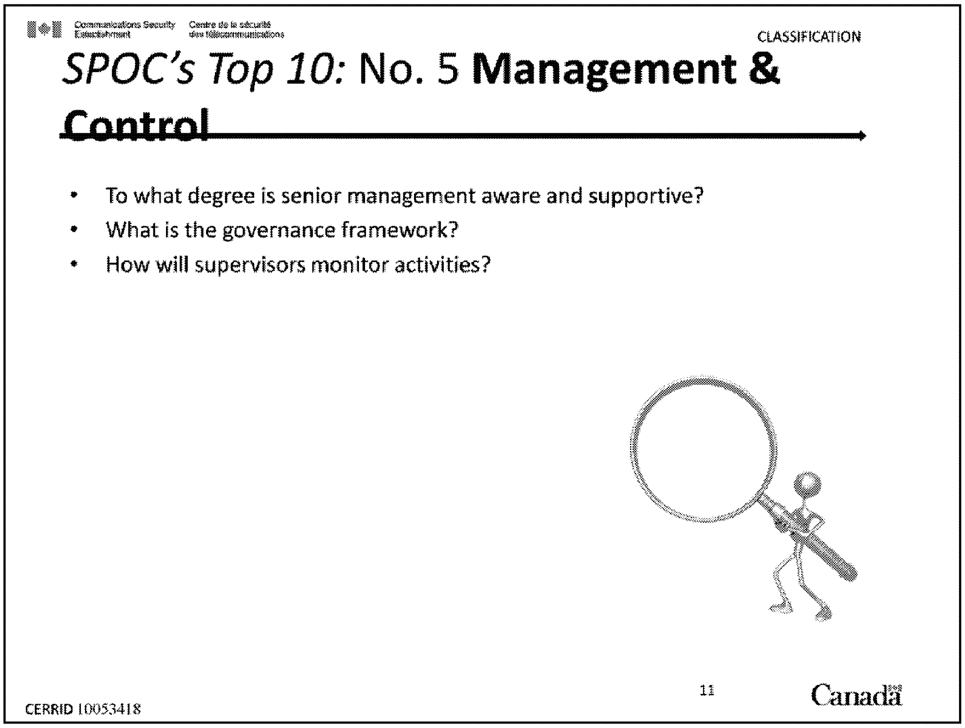
Data Acquisition

Analytical Tradecraft

Automation

Cabinet Cc

Partnerships



SPOC's Top 10: No. 5 **Management & Control**

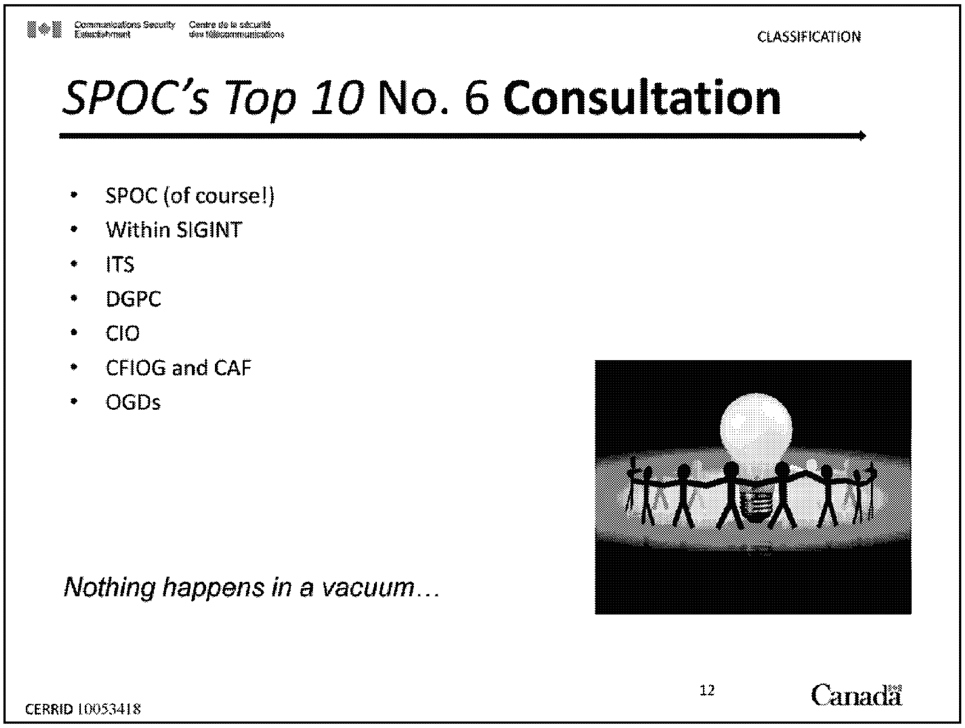
- To what degree is senior management aware and supportive?
- What is the governance framework?
- How will supervisors monitor activities?

This links back to the NDA in sec 273.62(2) "The Chief…has the management and control of the Establishment and all matters relating to it." and to the priorities set in SIGINT 2015.

Accountability is the obligation to answer for the exercise of responsibilities within the delegated authorities conferred. It's so important that the Minister has issued a Directive on it.

Accountability is a fundamental principle and given CSE's new status as a stand-alone agency within the Defence Portfolio (PinG), it's important that all new projects are developed with accountability in mind because any activity or project can come under intense scrutiny.

Purpose is not to stifle innovation or collaboration or agility, but rather to ensure that sr mgmt can be accountable for activities in their areas of responsibility and in line with priorities.



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10 No. 6 **Consultation**

- SPOC (of course!)
- Within SIGINT
- ITS
- DGPC
- CIO
- CFIOG and CAF
- OGDs

Nothing happens in a vacuum…

12

Canadä

CERRID 10053418

Problems/gaps/opportunities – these kinds of things are always multi-dimensional. Your specific problem may have arisen from a decision in another part of SIGINT and the solution to your problem may impact on another group in SIGINT. Each activity has interdependencies within SIGINT

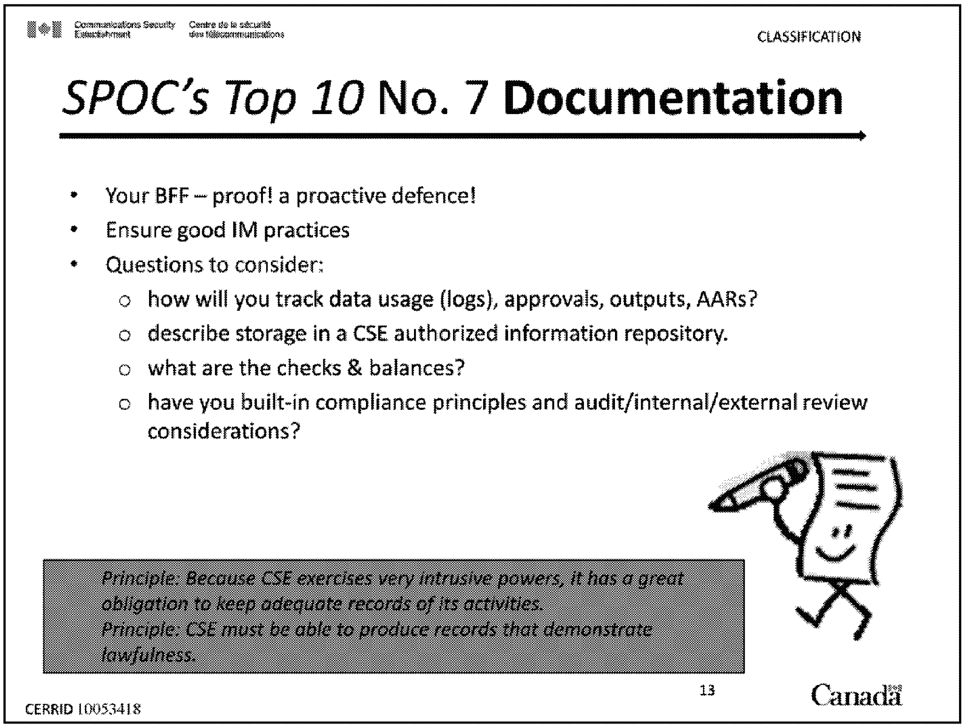
So we encourage you to situate your issue within a larger context.

Who have you already talked to help develop the project? Who else can you talk to? Who else *must* you talk to?

For example, DGPC/D2/SPOC for privacy considerations

Chances are there are lots of people who'd like to help you get your bright idea off the ground.

Also a fundamental principle of MOSAiC – collaboration – a successful SIGINT project is the result of many interactions



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10 No. 7 **Documentation**

- Your BFF – proof! a proactive defence!
- Ensure good IM practices
- Questions to consider:
  - how will you track data usage (logs), approvals, outputs, AARs?
  - describe storage in a CSE authorized information repository.
  - what are the checks & balances?
  - have you built-in compliance principles and audit/internal/external review considerations?

Principle: Because CSE exercises very intrusive powers, it has a great obligation to keep adequate records of its activities.
Principle: CSE must be able to produce records that demonstrate lawfulness.

13

Canadä

CERRID 10053418

Answer all the standard questions –
Who – accountability and responsibility
What – get at the facts and information
Where – where is the data from? Are private communications implicated?
Why – seeks to understand reasons and the rationale – foundation in mandate and policy
When – timing and sequences
How - process
Could – explore the subject

Records can include: Emails, CERRID docs, Logs and audit trails, Sr mgmt approval, Project charters

It's not enough for CSE to say that it complies with the law and our own policies – we have to be able to prove it. So, it's important to have the facts laid out. The more facts that are clearly documented, the less room there is later on for faulty interpretation. In the not so distant past, CSE senior management identified corporate record keeping as a risk. And, DGAEE has done an audit touching upon the importance of keeping corporate records in order to meet our obligations as a government department – e.g. ATIP and Privacy Act requests. Even more recently, the Commissioner pointed to it in his Annual Report.

When a document trail is available, it's easy for anyone – including a reviewer – to understand what the problem was, what was done, how it was done, why it was done, when and by whom. Keeping records is not useless or a pointless exercise, because…

.

When records aren't available, all the best intentions in the world won't make a difference as there will be no proof.

As the Commissioner said in his 2011-2012 Annual Report:
…the creation and retention of records is one of the main means by which CSEC can account for its activities and provide assurance that its activities comply with legal, ministerial and policy requirements.

And as he said in 2007-2008:

"Future reviews will continue to seek documentation that demonstrates compliance with authorities, provides a record of all activities conducted and confirms that supervisors are monitoring the performance of their staff."

It's all laid out in OPS-1, Section 6:

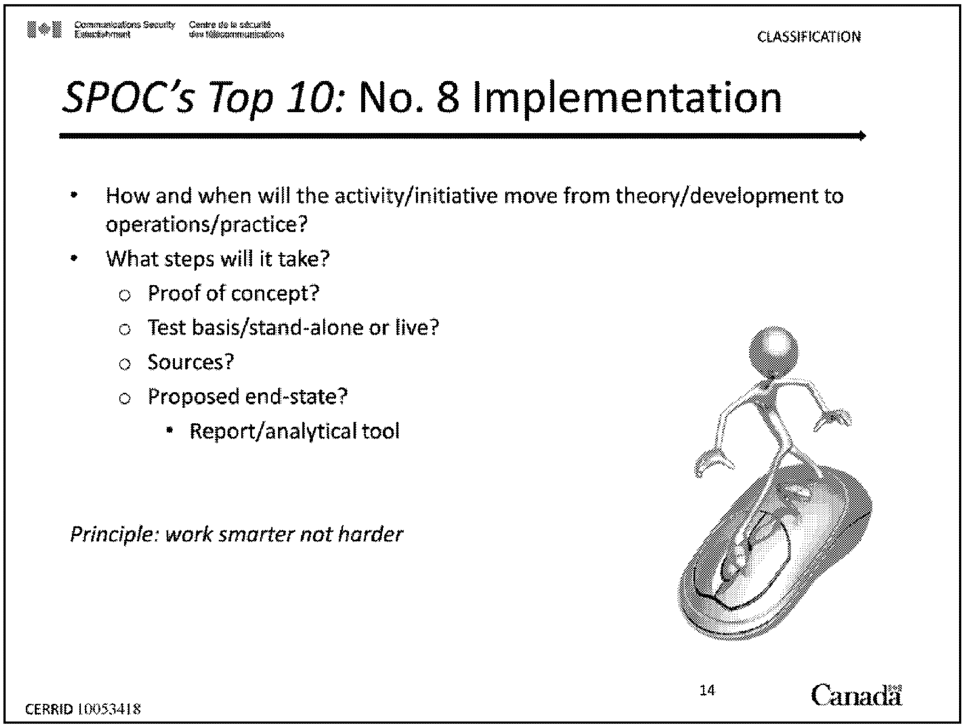
CSE is better placed to demonstrate evidence of its legal and policy compliance when it is able to retrieve and make available records that:

- demonstrate compliance with authorities and any associated conditions or constraints (for example, legal, MD, MA, policy, etc.) that could have lawfulness or privacy implications
- record management decisions and rationales, especially those related to operational, legal, and policy issues
- provide a record of management decisions
- confirm that supervisors and managers are monitoring compliance with conditions established in authority documents, and
- demonstrate CSEC's identification of any non-compliance issues and associated corrective actions (for example, Privacy Incidents File).

Retrieved from [redacted]

Your documentation can show your theory, assumptions and line of reasoning – your judgement and expertise in arriving at a method or conclusion – that is invaluable for future endeavours and for evaluation and review processes.

But in order for the records to be helpful, you have to be able to find and retrieve them so follow CSE's IM principles and practices – consult the CIO toolkit [redacted]



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10: No. 8 Implementation

- How and when will the activity/initiative move from theory/development to operations/practice?
- What steps will it take?
  - Proof of concept?
  - Test basis/stand-alone or live?
  - Sources?
  - Proposed end-state?
    - Report/analytical tool

Principle: work smarter not harder

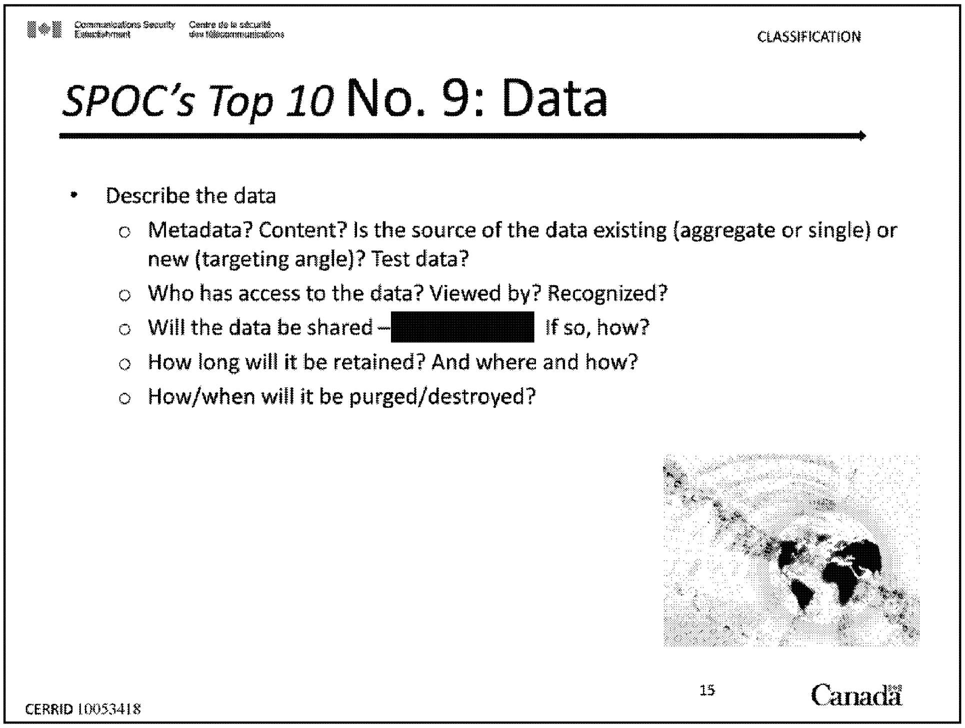
CERRID 10053418

14

Canada

One thing that we have to have is clear information about WHEN it has moved from theory/dev to ops/practice

This was a huge issue with a certain database/tool that I think we need to better manage. It is nice to lay out all of the states and steps but we need to know specifically when a project has shifted state. In line with this we also need to ensure that whatever scale is used to determine a change in state does not introduce contradictory information into the system. In the case of a certain database/tool under the IM/IT way of looking at things it was clearly still in development as it has not "passed on" to a steady state management or "production" state. This although from a SIGINT (and compliance) POV it had clearly moved from a "development" state to use within "production" as it had numerous users and was being used as the basis of reporting. These two different definitions for the same "states" caused nothing but problems in the past.



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10 No. 9: Data

- Describe the data
  - Metadata? Content? Is the source of the data existing (aggregate or single) or new (targeting angle)? Test data?
  - Who has access to the data? Viewed by? Recognized?
  - Will the data be shared – [redacted] If so, how?
  - How long will it be retained? And where and how?
  - How/when will it be purged/destroyed?

CERRID 10053418

15

Canada

What do we mean by metadata? The MD definition, that is "information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content."

That does not include enrichment.

Big SPOC concerns:
Classification
Retention
Sharing
Annotating
Reporting
Purging/Destroying
Privacy
Possibility of over-collect
Equities [redacted]

Also:

Purging

Retention

Annotation

Access

Syncing with the System of Record

Fused Data Results

Data Storage

Data used in Reports

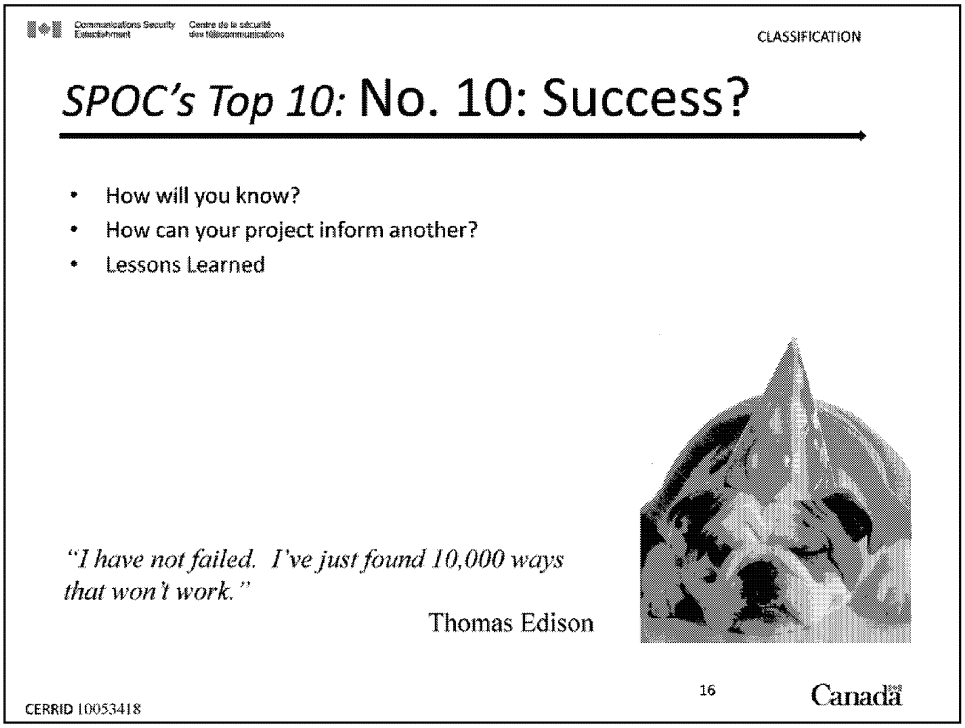
Data used by an automated system

Data viewed by

Retention of logs for view by/used by

New – Stewardship agreements – see Stewardship Agreements (ppt to SMF 5 Dec 2012) CERRID 1104975

SPOC continues to work on more detailed checklists on data (see SPOC's work on rules sets, etc)



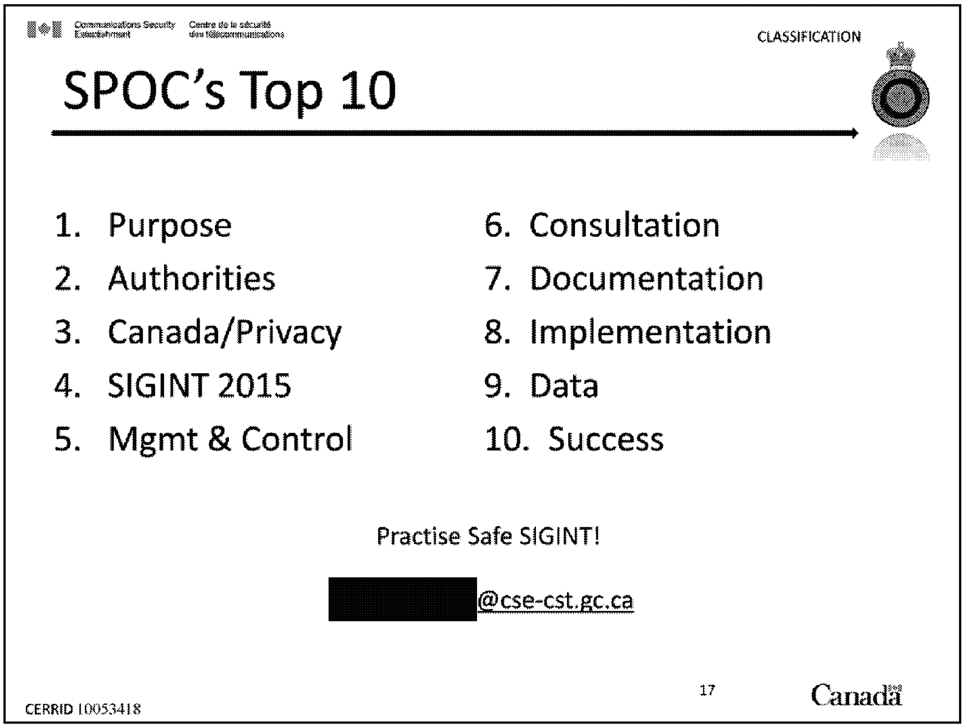
SPOC's Top 10: No. 10: Success?

- How will you know?
- How can your project inform another?
- Lessons Learned

"I have not failed. I've just found 10,000 ways that won't work."

Thomas Edison

How will you celebrate? Not so much a policy or compliance consideration but SPOC appreciates a good party as much as anyone else.



Communications Security Establishment Centre de la sécurité des télécommunications

CLASSIFICATION

SPOC's Top 10

1. Purpose
2. Authorities
3. Canada/Privacy
4. SIGINT 2015
5. Mgmt & Control
6. Consultation
7. Documentation
8. Implementation
9. Data
10. Success

Practise Safe SIGINT!

[redacted]@cse-cst.gc.ca

17

Canada

CERRID 10053418