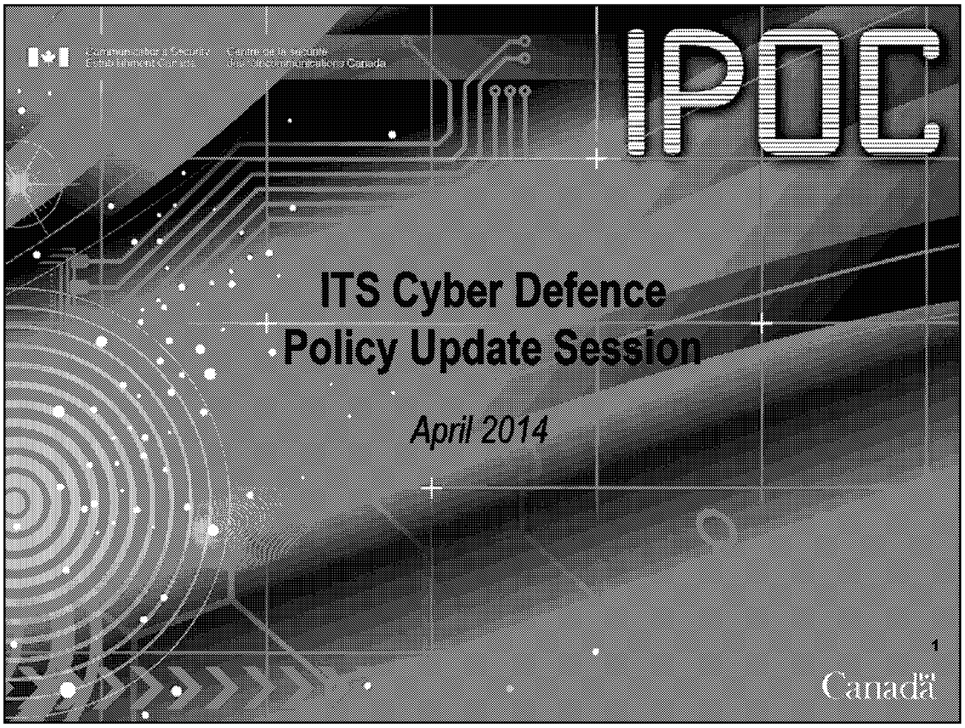


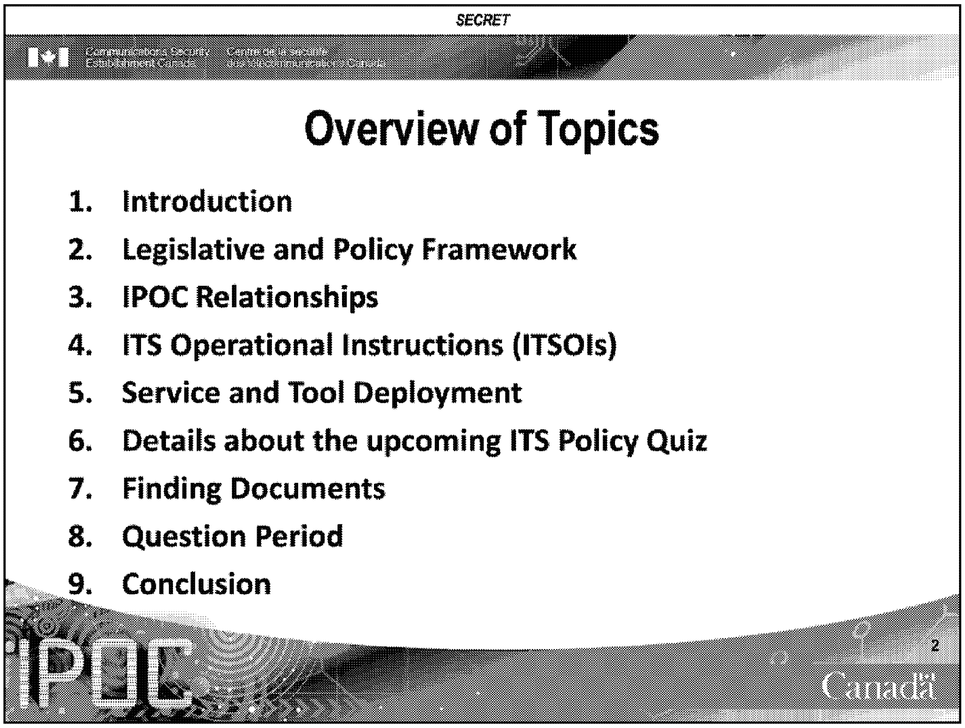
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

ITS Cyber Defence Policy Update Session

April 2014

1

Canada



SECRET

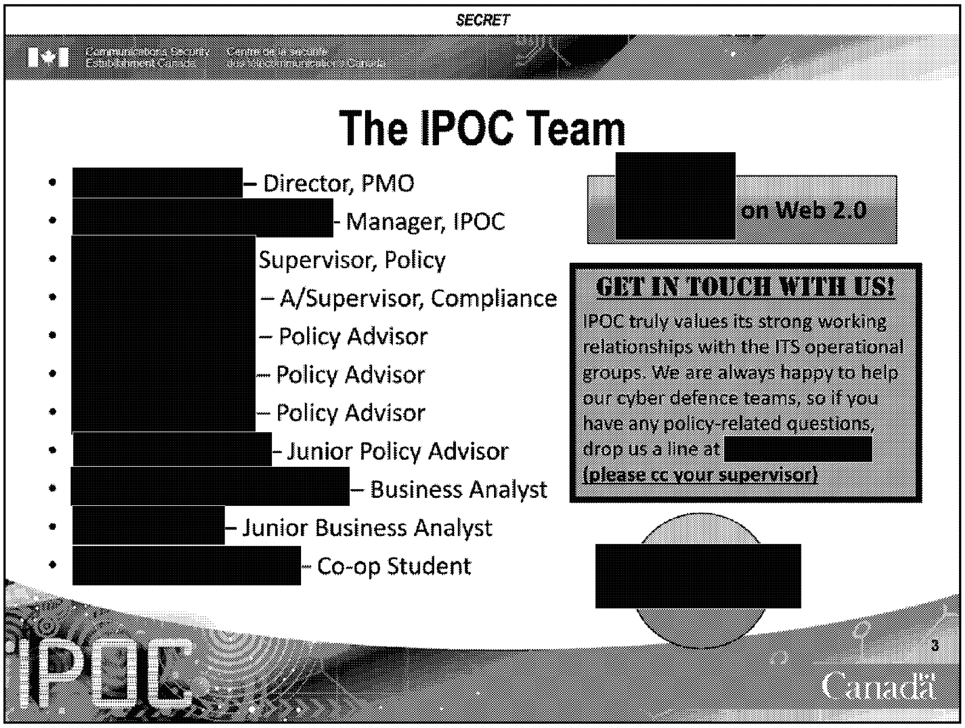
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Overview of Topics

1. Introduction
2. Legislative and Policy Framework
3. IPOC Relationships
4. ITS Operational Instructions (ITSOIs)
5. Service and Tool Deployment
6. Details about the upcoming ITS Policy Quiz
7. Finding Documents
8. Question Period
9. Conclusion

2

Canada



SECRET

Communications Security Establishment Canada   Centre de la sécurité des télécommunications Canada

The IPOC Team

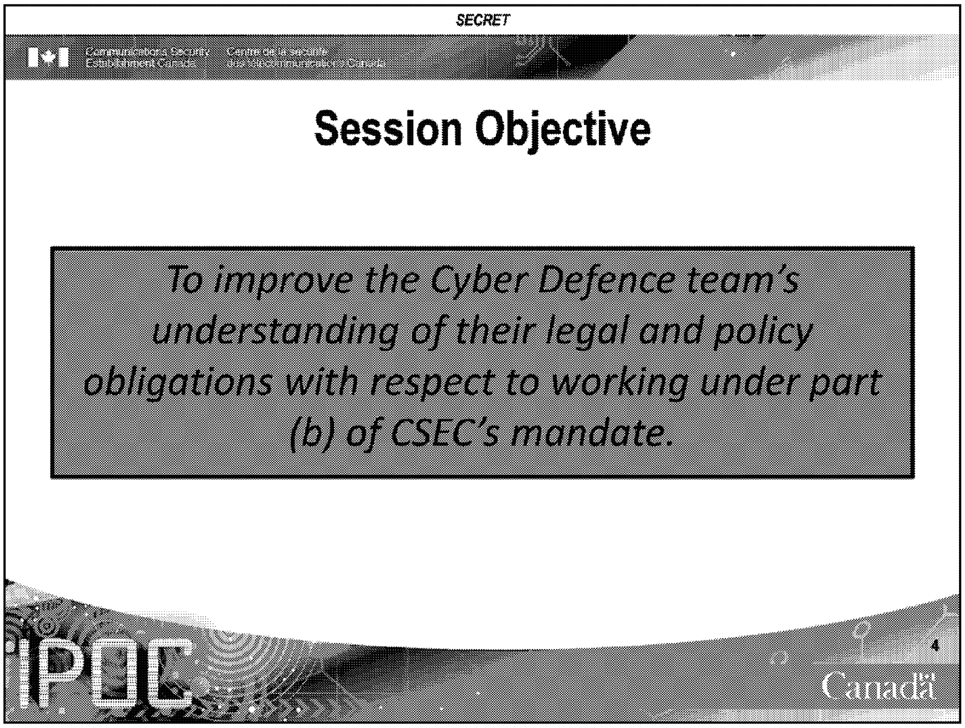
- [redacted] – Director, PMO
- [redacted] - Manager, IPOC
- [redacted] Supervisor, Policy
- [redacted] – A/Supervisor, Compliance
- [redacted] – Policy Advisor
- [redacted] – Policy Advisor
- [redacted] – Policy Advisor
- [redacted] - Junior Policy Advisor
- [redacted] – Business Analyst
- [redacted] - Junior Business Analyst
- [redacted] - Co-op Student

[redacted] on Web 2.0

GET IN TOUCH WITH US!

IPOC truly values its strong working relationships with the ITS operational groups. We are always happy to help our cyber defence teams, so if you have any policy-related questions, drop us a line at [redacted] **(please cc your supervisor)**

[redacted]



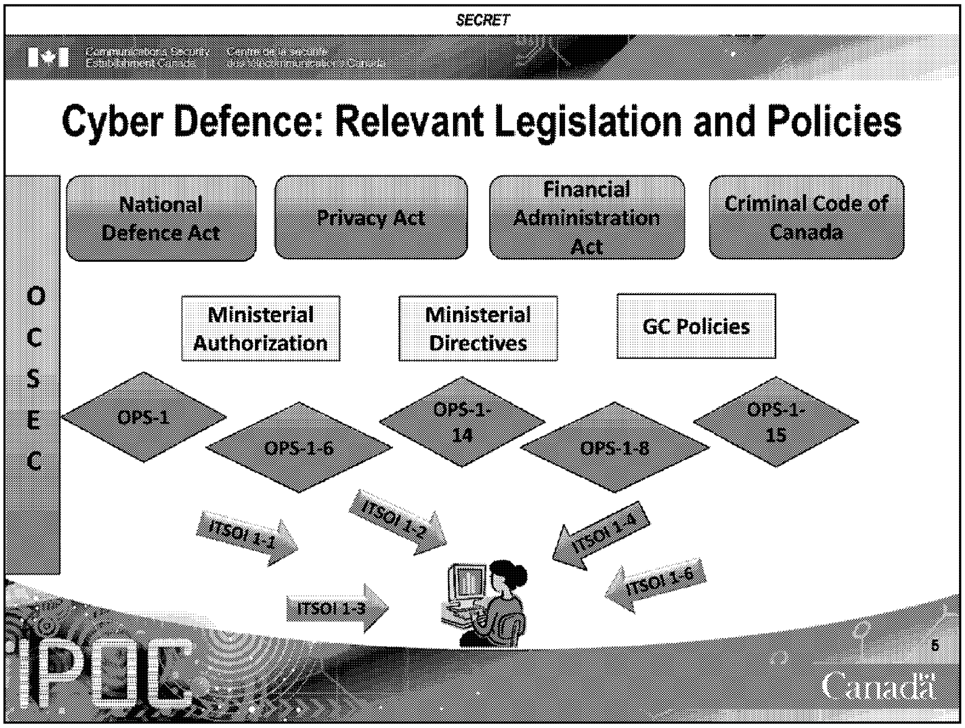
SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Session Objective

To improve the Cyber Defence team's understanding of their legal and policy obligations with respect to working under part (b) of CSEC's mandate.

IPOC
4
Canada

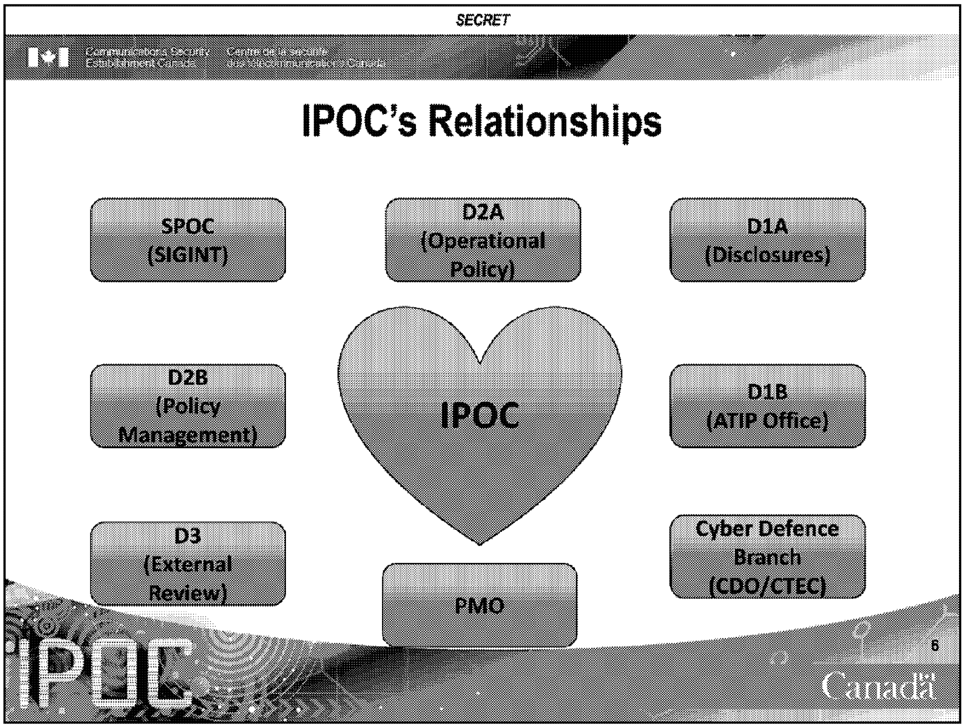


SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Cyber Defence: Relevant Legislation and Policies

OCSEC
National Defence Act
Privacy Act
Financial Administration Act
Criminal Code of Canada
Ministerial Authorization
Ministerial Directives
GC Policies
OPS-1
OPS-1-6
OPS-1-14
OPS-1-8
OPS-1-15
ITSOI 1-1
ITSOI 1-2
ITSOI 1-4
ITSOI 1-6
ITSOI 1-3
IPOC
5
Canada



SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

IPOC's Relationships

SPOC (SIGINT)

D2A (Operational Policy)

D1A (Disclosures)

D2B (Policy Management)

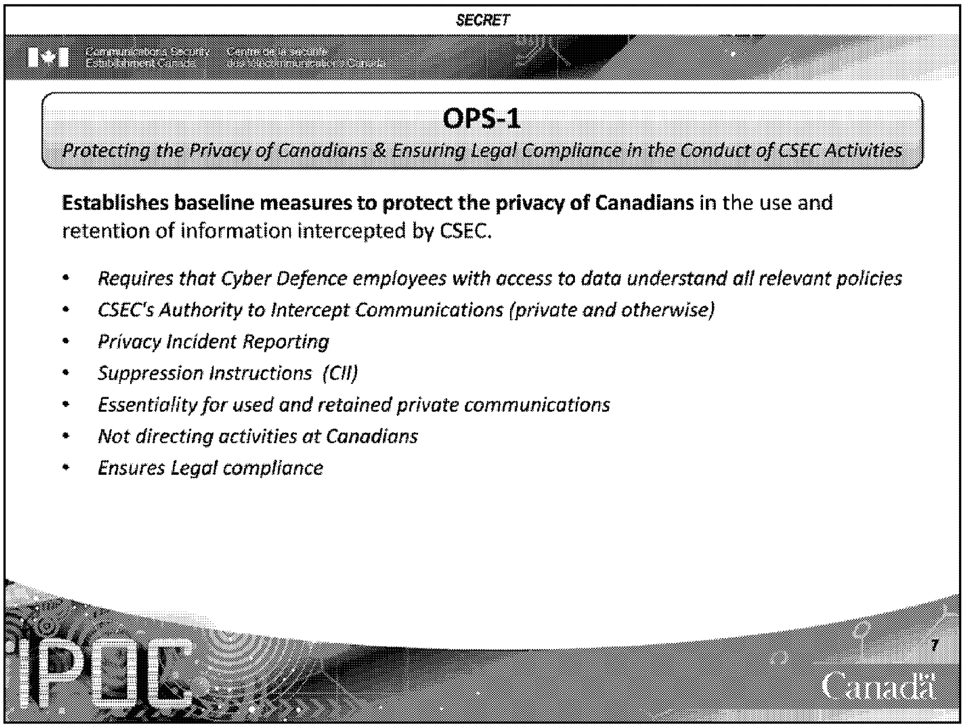
IPOC

D1B (ATIP Office)

D3 (External Review)

PMO

Cyber Defence Branch (CDO/CTEC)



SECRET

Communications Security Establishment Canada   Centre de la sécurité des télécommunications Canada

OPS-1

Protecting the Privacy of Canadians & Ensuring Legal Compliance in the Conduct of CSEC Activities

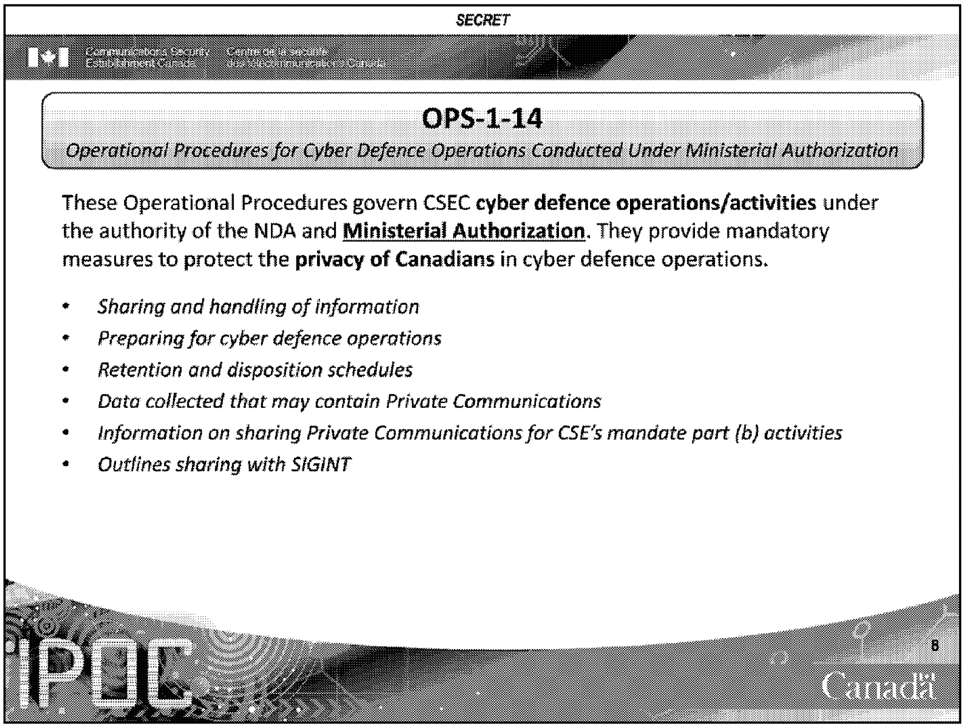
Establishes baseline measures to protect the privacy of Canadians in the use and retention of information intercepted by CSEC.

- *Requires that Cyber Defence employees with access to data understand all relevant policies*
- *CSEC's Authority to Intercept Communications (private and otherwise)*
- *Privacy Incident Reporting*
- *Suppression Instructions (CII)*
- *Essentiality for used and retained private communications*
- *Not directing activities at Canadians*
- *Ensures Legal compliance*

IPOC

7

Canada



SECRET

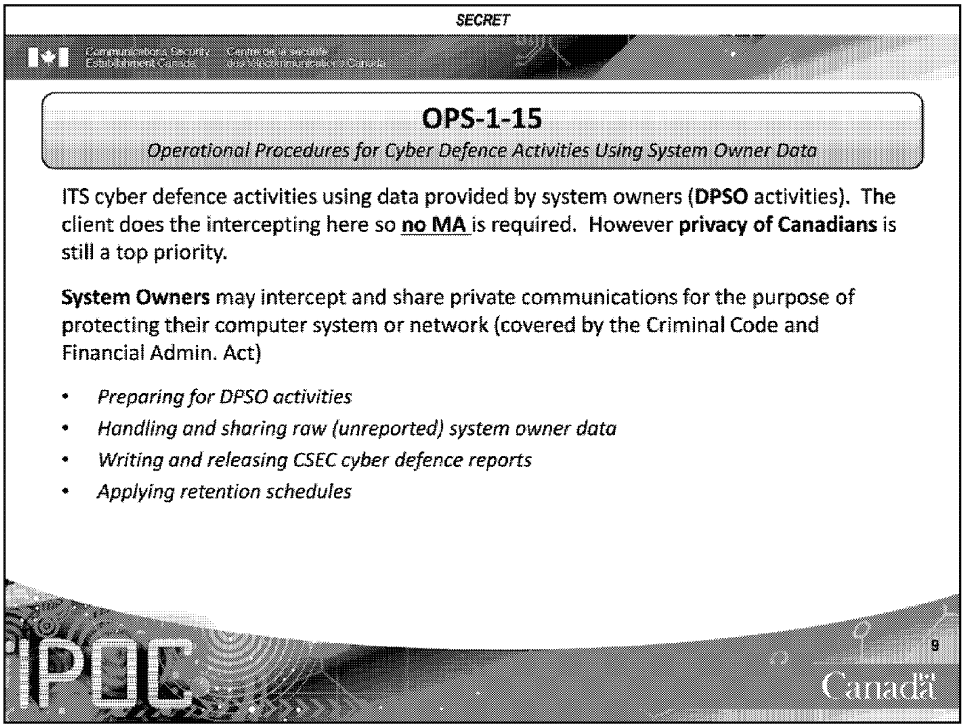
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

OPS-1-14

Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization

These Operational Procedures govern CSEC **cyber defence operations/activities** under the authority of the NDA and **Ministerial Authorization**. They provide mandatory measures to protect the **privacy of Canadians** in cyber defence operations.

- *Sharing and handling of information*
- *Preparing for cyber defence operations*
- *Retention and disposition schedules*
- *Data collected that may contain Private Communications*
- *Information on sharing Private Communications for CSE's mandate part (b) activities*
- *Outlines sharing with SIGINT*



SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

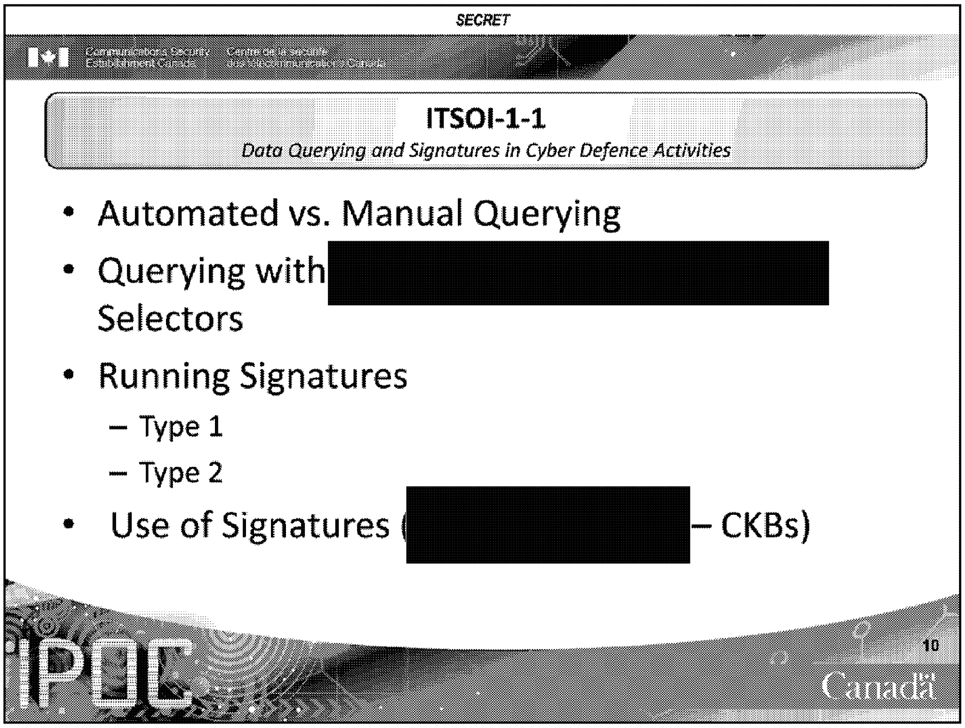
OPS-1-15

Operational Procedures for Cyber Defence Activities Using System Owner Data

ITS cyber defence activities using data provided by system owners (**DPSO** activities). The client does the intercepting here so **no MA** is required. However **privacy of Canadians** is still a top priority.

System Owners may intercept and share private communications for the purpose of protecting their computer system or network (covered by the Criminal Code and Financial Admin. Act)

- *Preparing for DPSO activities*
- *Handling and sharing raw (unreported) system owner data*
- *Writing and releasing CSEC cyber defence reports*
- *Applying retention schedules*



SECRET

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

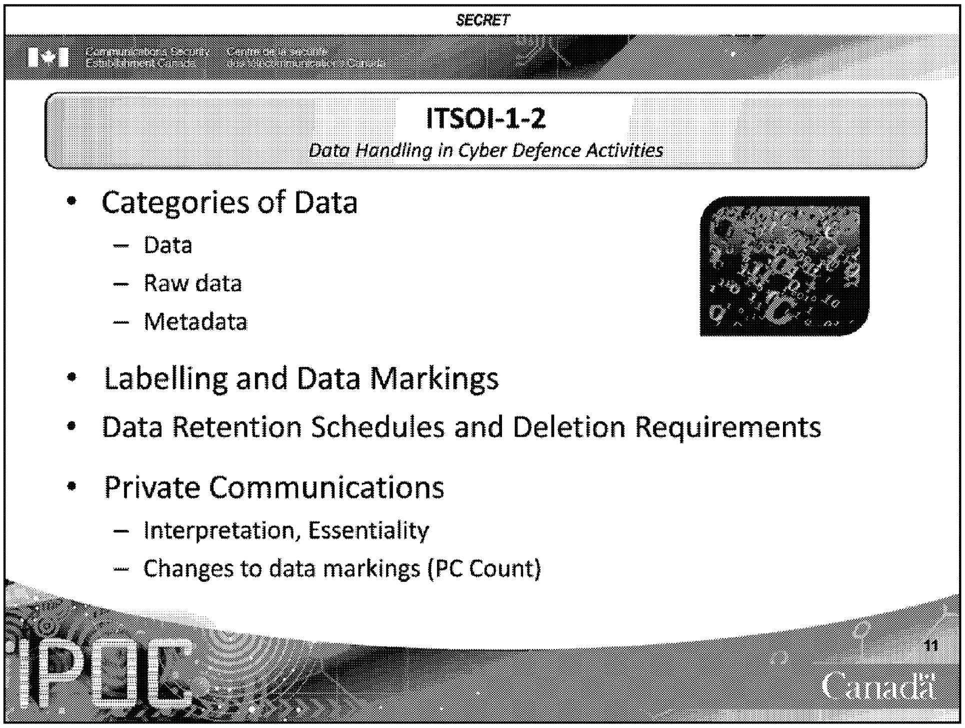
ITSOI-1-1

Data Querying and Signatures in Cyber Defence Activities

- Automated vs. Manual Querying
- Querying with [redacted] Selectors
- Running Signatures
  - Type 1
  - Type 2
- Use of Signatures ([redacted] – CKBs)

10

Canada



SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

ITSOI-1-2

Data Handling in Cyber Defence Activities

- Categories of Data
  - Data
  - Raw data
  - Metadata
- Labelling and Data Markings
- Data Retention Schedules and Deletion Requirements
- Private Communications
  - Interpretation, Essentiality
  - Changes to data markings (PC Count)

Categories of Data

Data [redacted] under Part b, content and associated metadata)

Raw data (not used and retained)

Metadata (info associated with a telecommunication to ID, describe or route…)

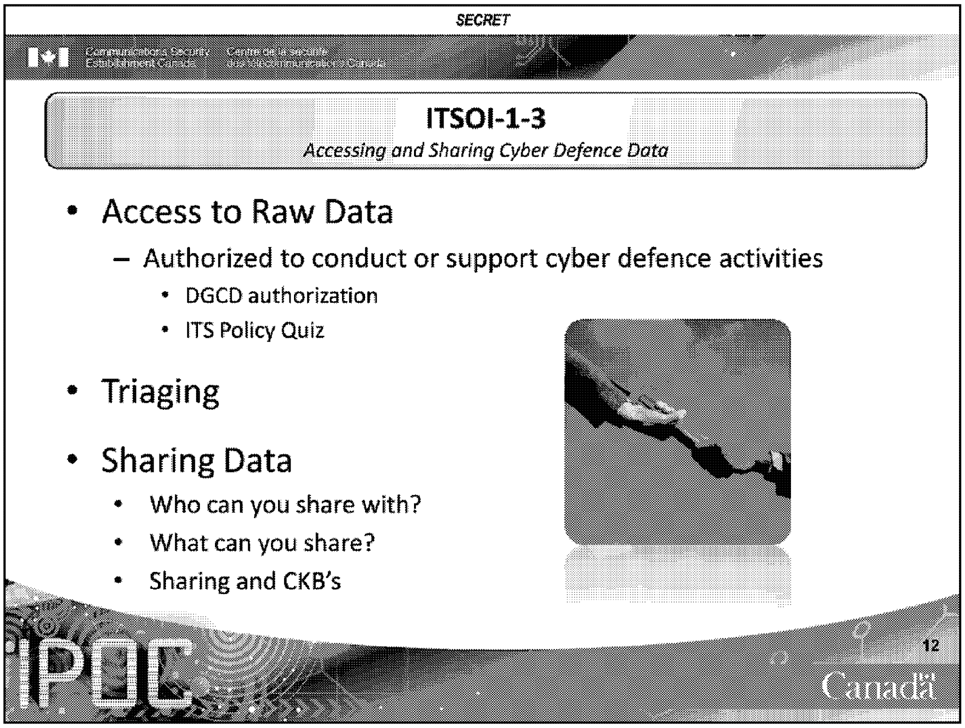
- Labelling and Data Markings (Important to label, determine data source, time stamp for how to treat the data for retention, category of data…)
- Data Retention Schedules and Deletion Requirements (Must adhere to retention and deletion conditions based on data category)

- Private Communications

  Interpretation, Essentiality (justification is provided)

  Changes to data markings (PC Count) – Please tell IPOC

  - IPOC submits quarterly reports on PC count and reports annually to the Minister of National Defence – changes can impact the count
  - We have an automated script to detect some changes but policy dictates that you MUST inform IPOC



SECRET

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

ITSOI-1-3

Accessing and Sharing Cyber Defence Data

- Access to Raw Data
  - Authorized to conduct or support cyber defence activities
    - DGCD authorization
    - ITS Policy Quiz
- Triaging
- Sharing Data
  - Who can you share with?
  - What can you share?
  - Sharing and CKB's

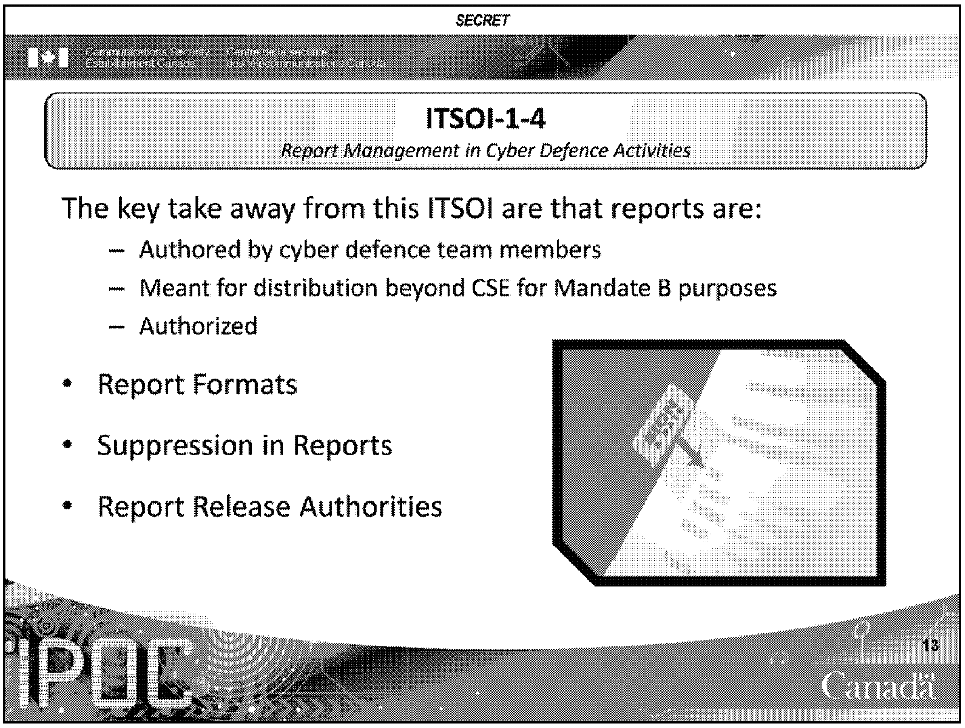
IPOC
12
Canada

Triaging

Ensure that any shared data is tracked

SIGINT has to delete it when finished (no Part a use!)

Designed to help ITS prioritize activities



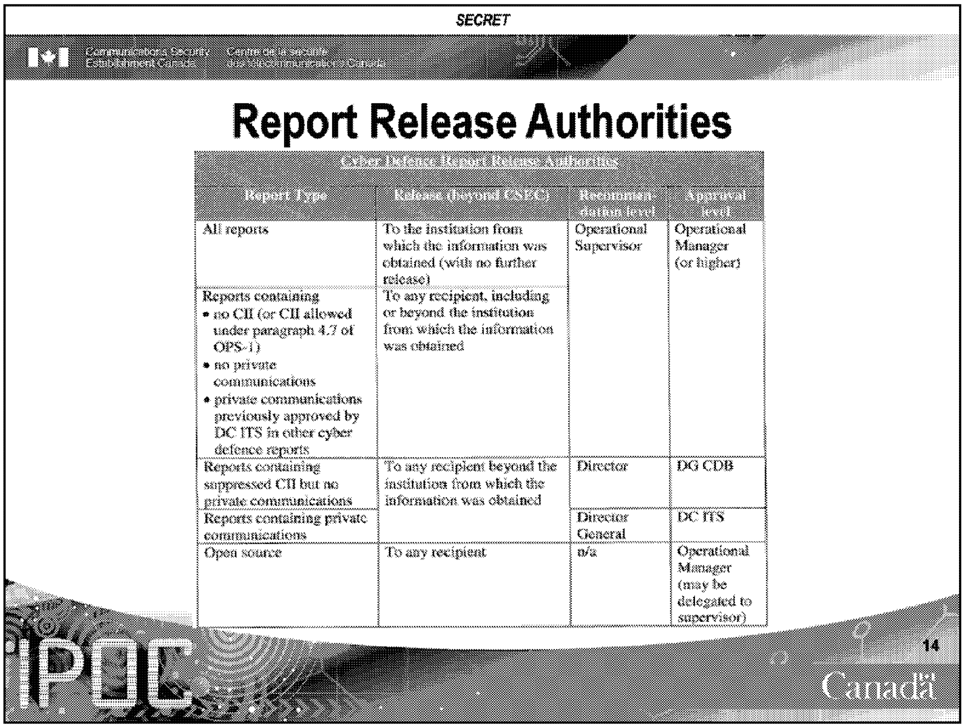
ITSOI-1-4

Report Management in Cyber Defence Activities

The key take away from this ITSOI are that reports are:

- – Authored by cyber defence team members
- – Meant for distribution beyond CSE for Mandate B purposes
- – Authorized

- Report Formats
- Suppression in Reports
- Report Release Authorities

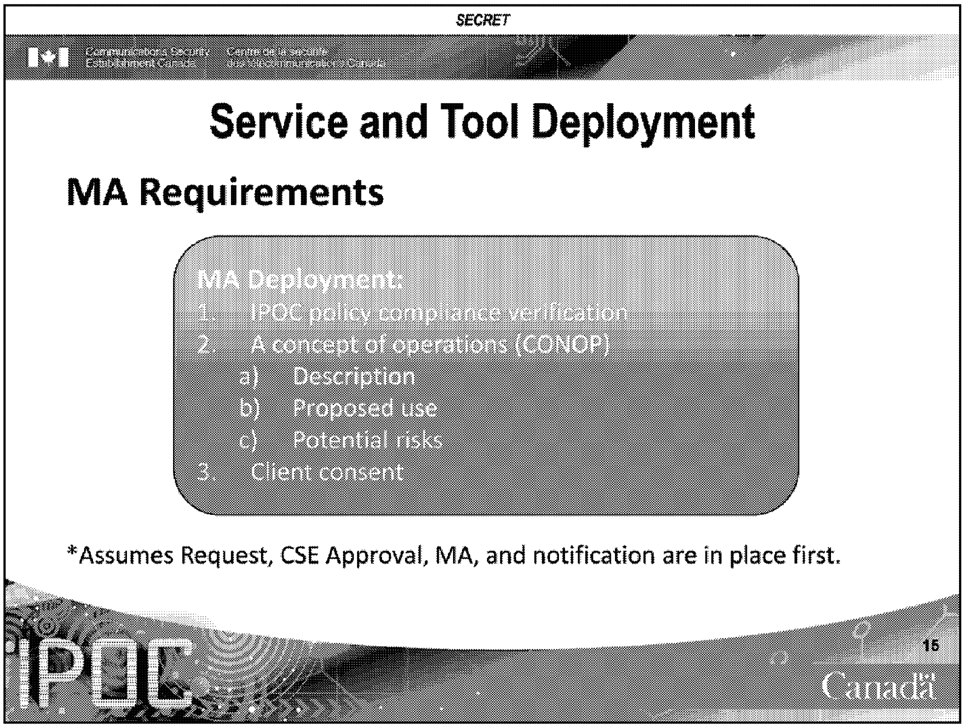


SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Report Release Authorities

Cyber Defence Report Release Authorities			
Report Type	Release (beyond CSEC)	Recommendation level	Approval level
All reports	To the institution from which the information was obtained (with no further release)	Operational Supervisor	Operational Manager (or higher)
Reports containing • no CII (or CII allowed under paragraph 4.7 of OPS-1) • no private communications • private communications previously approved by DC ITS in other cyber defence reports	To any recipient, including or beyond the institution from which the information was obtained		
Reports containing suppressed CII but no private communications	To any recipient beyond the institution from which the information was obtained	Director	DG CDB
Reports containing private communications		Director General	DC ITS
Open source	To any recipient	n/a	Operational Manager (may be delegated to supervisor)



SECRET

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

Service and Tool Deployment

MA Requirements

MA Deployment:

1. IPOC policy compliance verification
2. A concept of operations (CONOP)
   a) Description
   b) Proposed use
   c) Potential risks
3. Client consent

*Assumes Request, CSE Approval, MA, and notification are in place first.

For service and tool deployments under MA, ,there are several policy requirements that must be met:

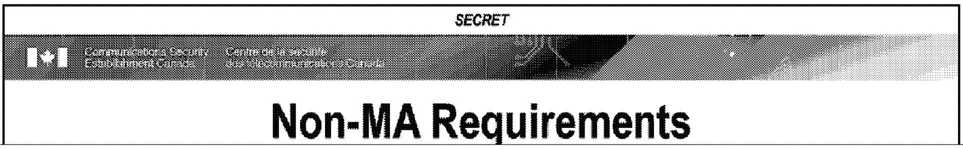
1) The purpose of IPOC's policy compliance verification is to assess any potential privacy of Canadian impacts. IPOC has a cyber defence activities service and tool privacy verification form that we require filled out for any new deployments of tools or capabilities.
2) Concept of Ops, we'll get to that in a minutes, but it must be provided to the client
3) Client consent, we need this documented. The client consent can be built into the original MOU, or it could be a new document. Either way, this must be saved.

Note – IPOC is not responsible for maintaining the client files and ensure all the required documents are saved properly, that is on the business side. IPOC can help you determine what documents you need to save and what you are missing, but we don't manage the client files. We have created some working aids that are available to assist you in making sure you have all meet all the policy requirements, so the sooner you contact IPOC the better.

For policy, a Concept of Operations must contain three things:

1) A description of the tool or service
2) Its proposed use on the client system/network
3) Any potential risks it poses to the client system/network

The form it takes is irrelevant, as long as those three pieces of information are provided to the client and documented. In fact, it could be done in 3 separate documents as well.



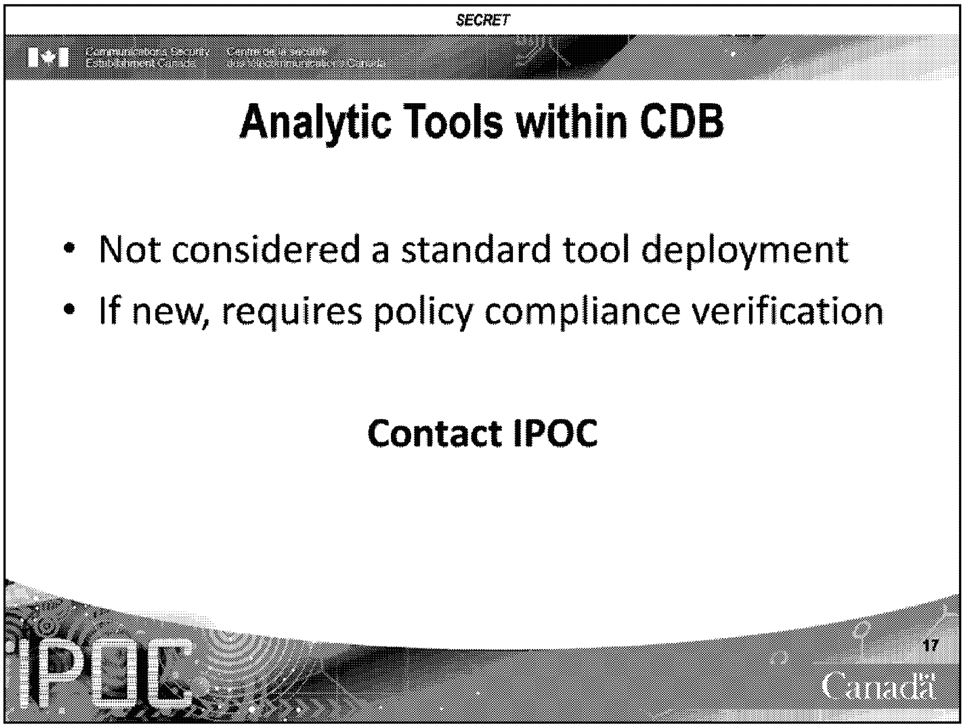
SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Non-MA Requirements

IRRELEVANT

IRRELEVANT



SECRET

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

Analytic Tools within CDB

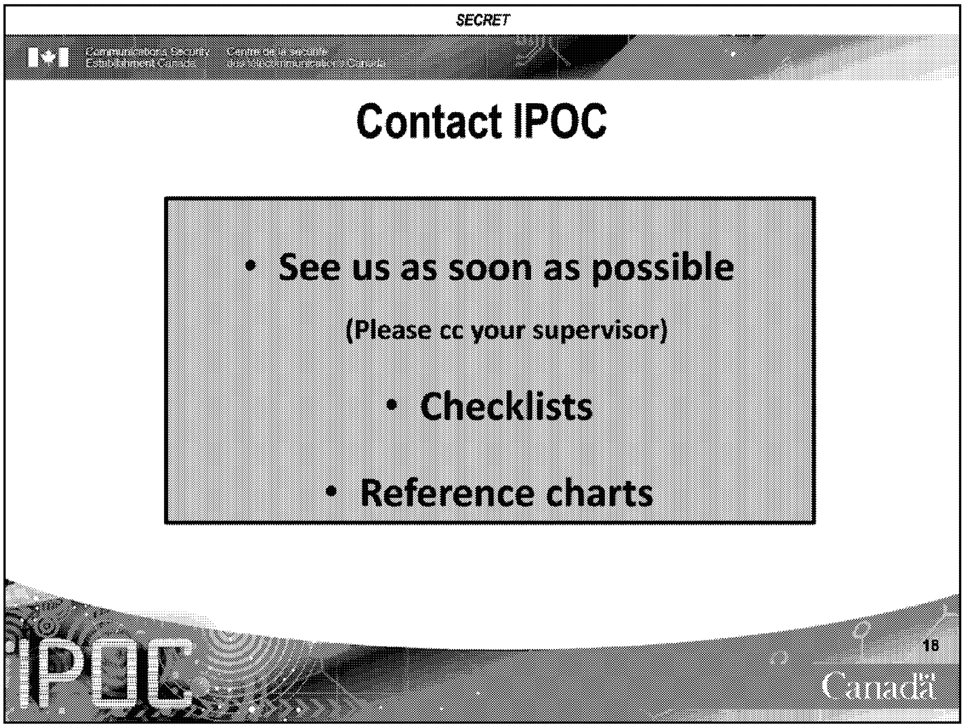
- Not considered a standard tool deployment
- If new, requires policy compliance verification

Contact IPOC

17

IPOC
Canada

Policy verification required to determine whether there is a privacy impact (personal information, raw data storage etc), and how to address it.



SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Contact IPOC

- See us as soon as possible

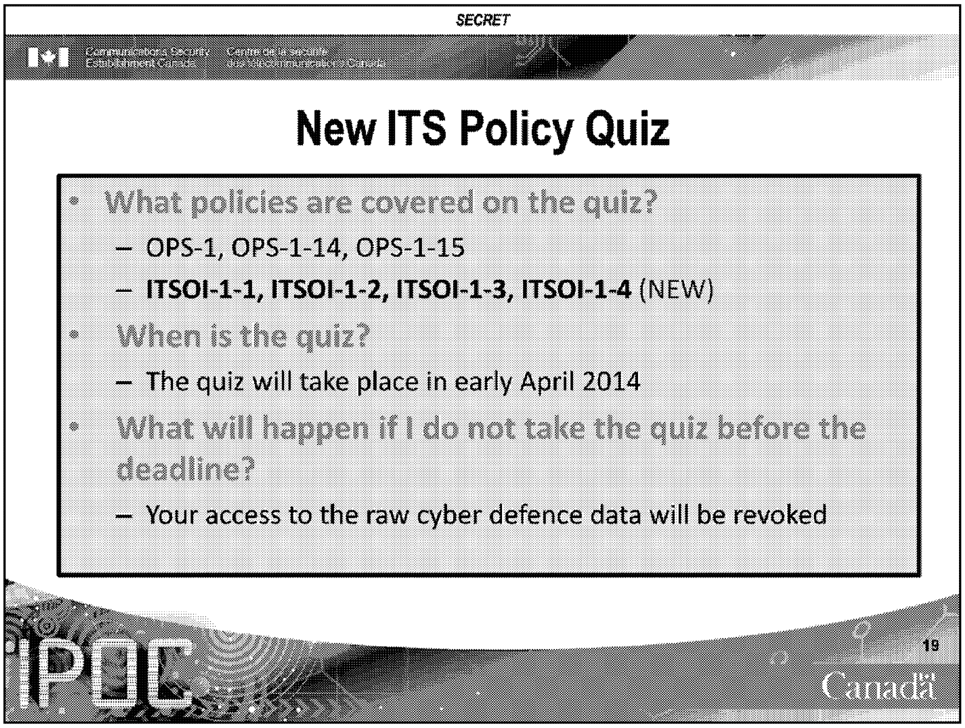
(Please cc your supervisor)

- Checklists
- Reference charts

IPOC
18
Canada

In closing, I just want to emphasize that the earlier you contact us the better. Even if you don't' have the exact details or requirements it doesn't matter. The sooner we can get the information, the sooner we can give advice. Policy does not want to hold you back from doing your job, s help us help you.

We have checklists and references that can guide to you make sure you hit all the policy requirements. As well, we can outline what are policy requirements and what are business decisions. This will help you find out who you need to talk to for each requirement.



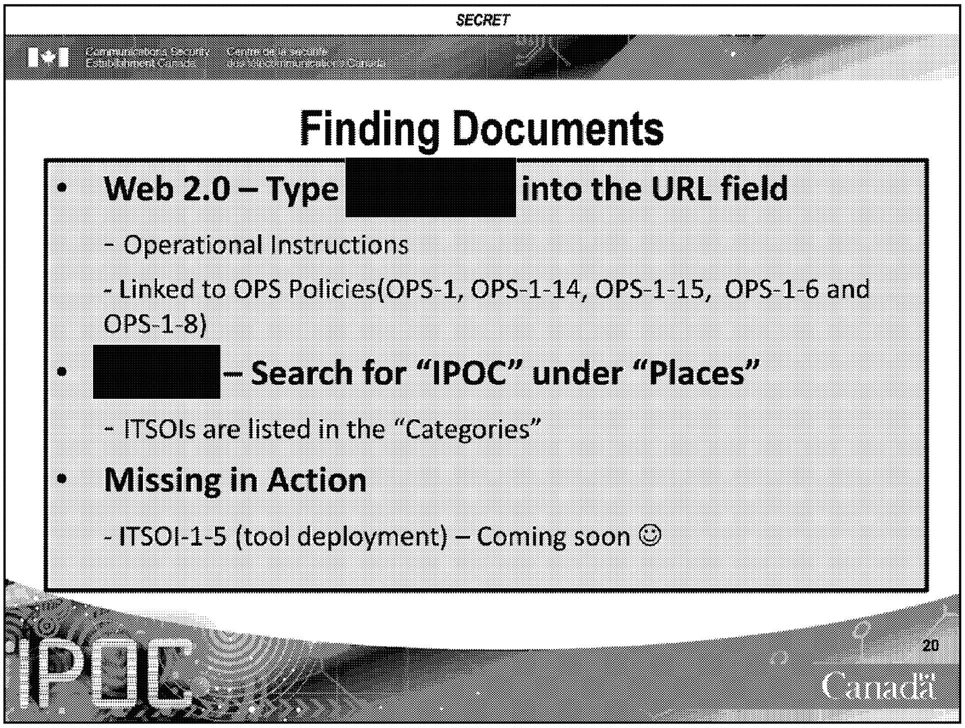
SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

New ITS Policy Quiz

- What policies are covered on the quiz?
  - OPS-1, OPS-1-14, OPS-1-15
  - **ITSOI-1-1, ITSOI-1-2, ITSOI-1-3, ITSOI-1-4** (NEW)
- When is the quiz?
  - The quiz will take place in early April 2014
- What will happen if I do not take the quiz before the deadline?
  - Your access to the raw cyber defence data will be revoked

Canadä



SECRET

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Finding Documents

- **Web 2.0 – Type [redacted] into the URL field**
  - Operational Instructions
  - Linked to OPS Policies(OPS-1, OPS-1-14, OPS-1-15, OPS-1-6 and OPS-1-8)
- **[redacted] – Search for "IPOC" under "Places"**
  - ITSOIs are listed in the "Categories"
- **Missing in Action**
  - ITSOI-1-5 (tool deployment) – Coming soon ☺

IPOC
20
Canada

SECRET

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

21

Canada