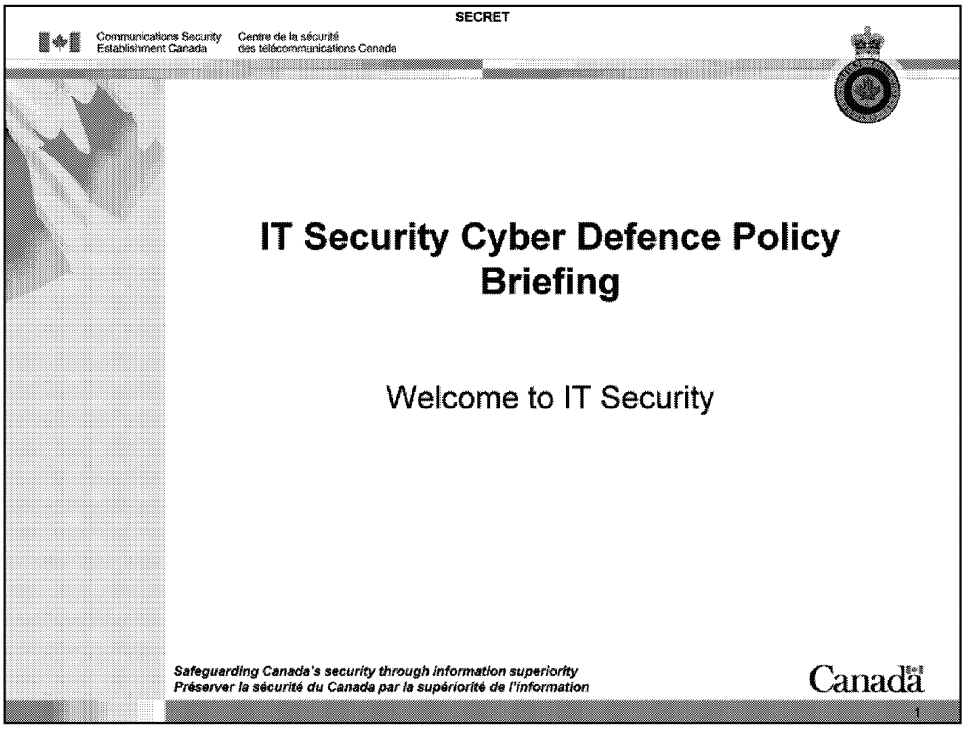


Notes from [redacted] on briefing requirements:

Types of data collected

2nd party model

What is a PC?

Types of info

Targeted audience

About IPOC

- ITS Policy Oversight and Compliance (IPOC)

- Policy Advice and guidance
- Policy Development
- Compliance
- Review facilitation (OCSEC, Internal Audit…)
- Contact: [redacted]

Overview of Briefing

- National Defence Act
- Ministerial Authorizations
- PC v. PI
- Private Communications
- OPS-1
- OPS-1-14
- OPS-1-15
- Questions

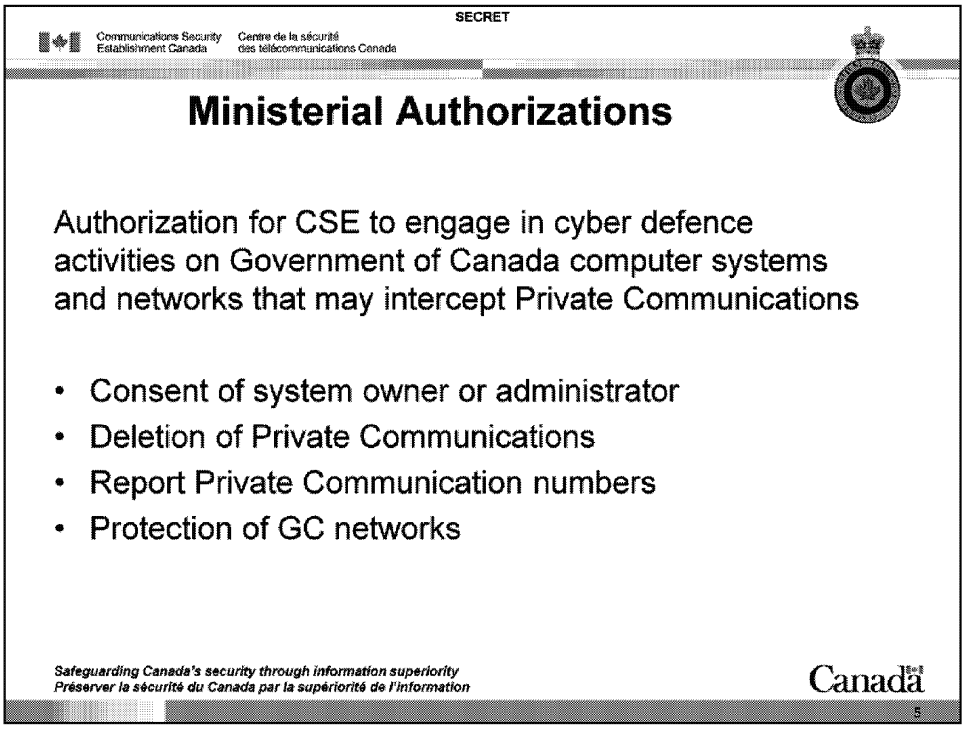
Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

National Defence Act (NDA)

- CSE's Mandate (Parts a, b IRRELEV
- Part (b): to provide advice, guidance and services to help ensure the protection of:

- Electronic information and of information infrastructures of importance to the GC

- Ministerial Authorization (requirements)



- Authorization for CSE to engage in cyber defence activities on Government of Canada computer systems and networks that may intercept Private Communications
- Federal institutions must submit a "Letter of Request" to CSE
- Raw data containing Private communications can only be retained for [redacted] from

the date of collection

- Count and report on private communications used or retained

PC v. PI

- **Private Communications**
- Any oral or telecommunication sent with the expectation that it will not be intercepted
- Min. one end Canadian
- Sharing restrictions deriving from the Criminal Code

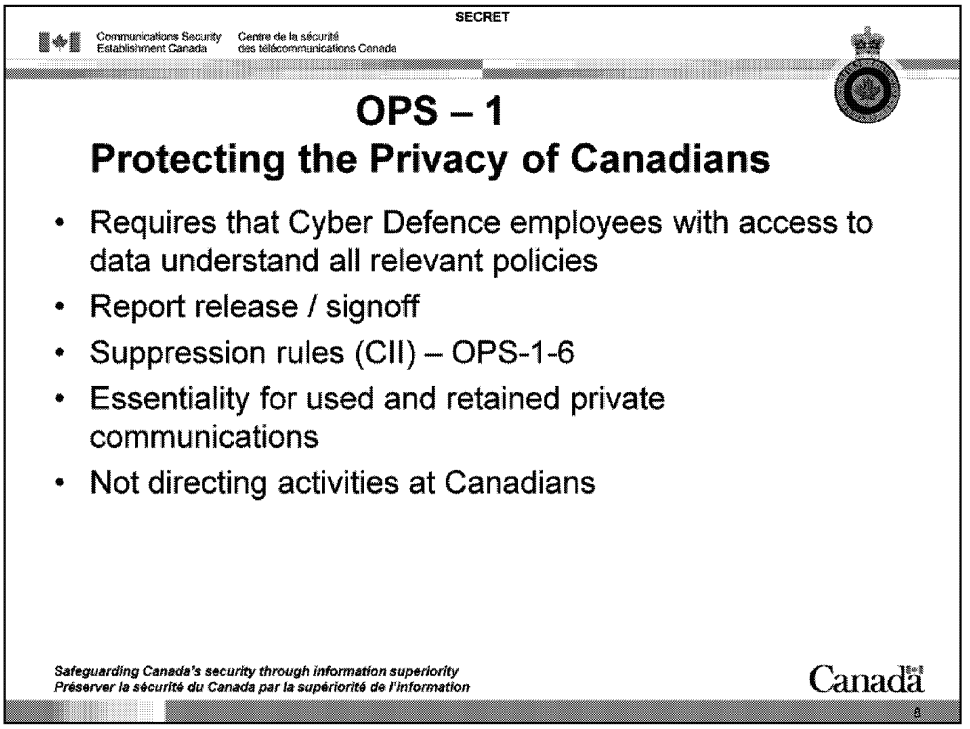
- **Personal Information**
- Includes individuals and corporations
- Canadian Identifying Information (CII) – suppressed when required

Intercepted Private Communications

- Intercepted [redacted]
- Includes all parts of the communication

Example: The malicious attachment in a phishing email

Private Communication is "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it."



Review the Cyber Defence Report Release Authorities for different report types! (OPS-1, 4.15)

OPS 1-14
Cyber Defence Operations

- Cyber Defence Operations conducted under Ministerial Authorization
- Covers the data collected under the MA that may contain Private Communications
- Information on sharing private communications for CSE's mandate part (b) activities

OPS 1-15

- Data is provided to ITS by a **system owner** or an intermediary (i.e. Public Safety) to address a perceived cyber threat
- ITS does not intercept private communication for these activities – no MA is required
- **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)

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

Principles for sharing System Owner Data

- Requestor (client) consent must always be obtained in order to share data or reports
- Expressed recipient consent must be obtained for sharing data from a private communication when the **purpose** is other than mitigating the cyber threat affecting the system owner (e.g. malware repository, situational awareness)
- Exception – can share with CSIS and RCMP for their mandates.