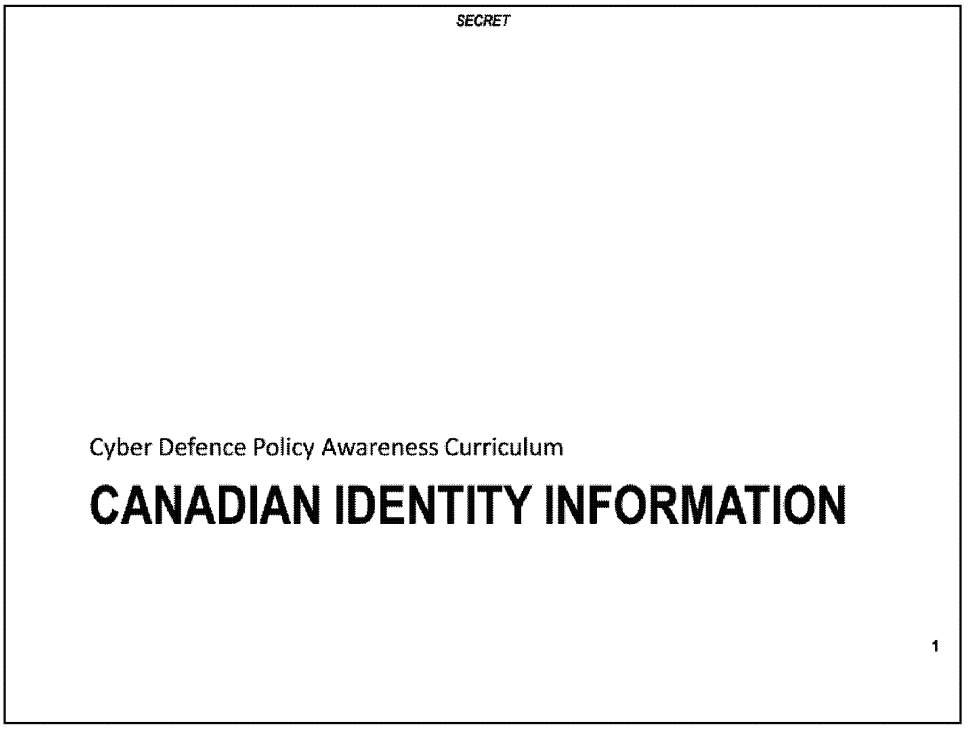
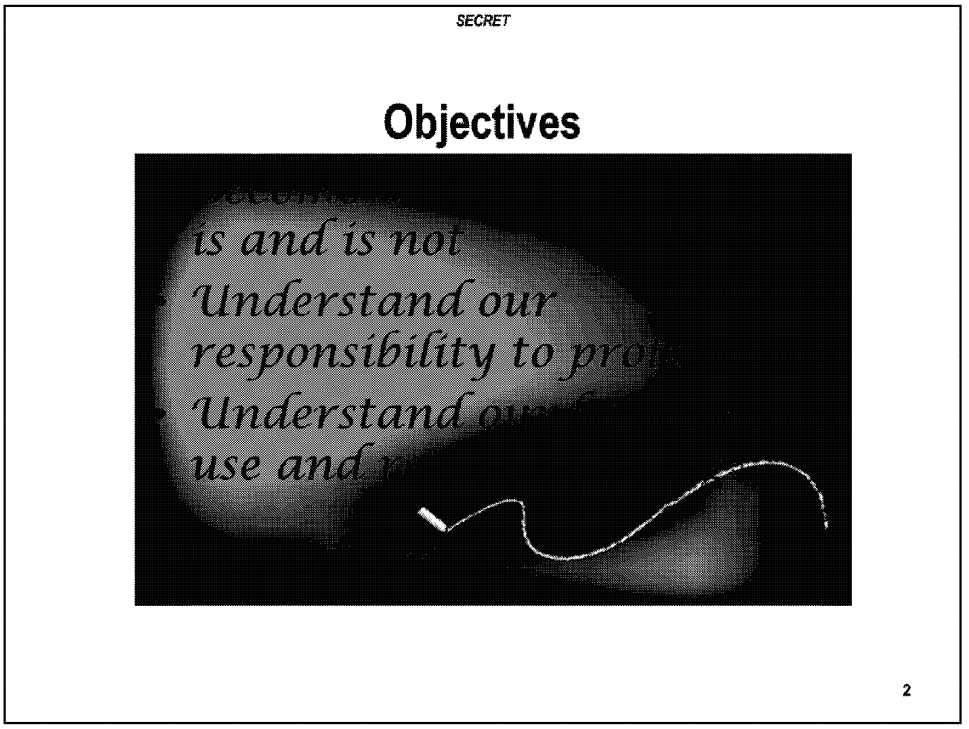


- Present the title of the workshop
- maybe give history on why IPOC decided this workshop was needed?



Introduction and Background to the Cyber Defence Policy Awareness Curriculum Workshop

- Given our mandated mission to protect GC infrastructures of importance, it is impossible not to encounter Canadian Identity Information while conducting our Cyber Defence activities

- We have a legal responsibility to protect the privacy of Canadians in all our work at CSEC

- Essentially it comes down to a need to maintain the delicate balance between:
  - 1) upholding the most stringent protection policies possible; and,
  - 2) conducting the most advanced cyber defence operations that we can.

- The goal of this workshop is to provide you with the knowledge you need to be able to confidently make decisions about what to do with CII as you encounter it in your daily work

- Our presentation includes an overview of how policy at CSEC defines CII, where the requirement to protect CII comes from, and how we handle, use and retain CII

- Saying this, IPOC will remain available to assist if ever you require guidance on how to comply with policy requirements regarding CII

SECRET

What is Canadian Identity Information?

Canadian Identity Information (CII) is any specific piece of information that **identifies a Canadian**, and it "includes, but is not limited to, names, phone numbers, email addresses, IP addresses, and passport numbers."

OPS-1 (8.2)

3

Example for clarity and not to be confused with "Information ABOUT a Canadian": [redacted] was the victim of a successful malware deployment against its computer network.

The Information about a Canadian (IAC) = that an attack was suffered by a company in Canada

The Canadian Identity Information (CII) = that the company was [redacted]

So….this OPS 1 definition clarifies a type of information requiring CSE's care for the "**subject to measures to protect the privacy of Canadians in the use and retention of intercepted information**" (requirement set forth in NDA & MA)

Defining "Canadian"

'Canadian' can refer to:

- a person (e.g. John Doe)
- a corporation (e.g. Bridgehead), or
- an organization (e.g. Conservative Party of Canada)

4

We need to have a common understanding of what can be considered "Canadian Identifying Information".

For the purpose of these procedures, "Canadian organizations" **are also accorded the same protection as Canadian citizens and corporations.** A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada."

***NOTE** THAT THE NAME OF ANY **FEDERAL INSTITUTION** AND **ITS IP ADDRESSES ARE NOT CANADIAN IDENTITY INFORMATION** because they do not isolate a single Canadian

For Cyber Defence Activities.....

There are mainly 3 types of CII for Cyber Defence:

- Email addresses
- IP addresses
- Domain names

5

For Cyber Defence Activities……

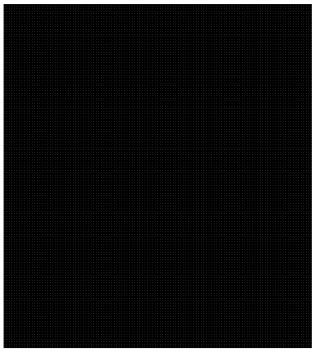
CII can get complicated:

- Email addresses are often spoofed
- .ca domains resolve to foreign Ips
- Legitimate company names are registered by foreign threat actors
- Is a signature "Canadian"?

6

SECRET

THE CHALLENGE:
Which are considered "Canadian Identity Information"?



7

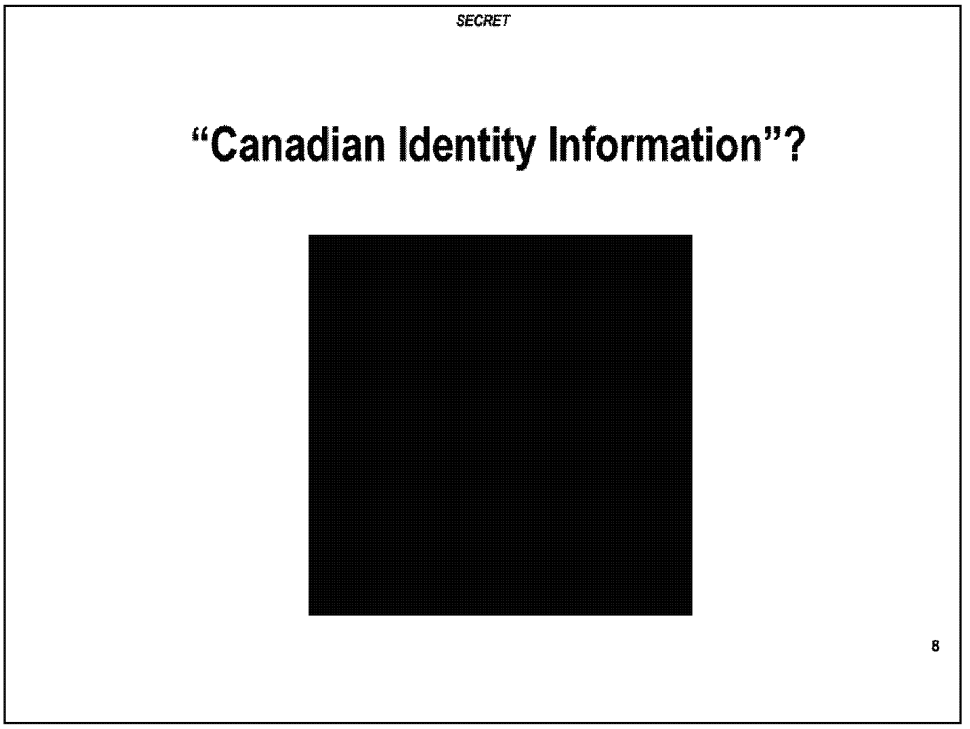
One of the three examples constitutes "Canadian Identity Information", according to CSE policy. Remember, this is considered sensitive personal information about a Canadian, so please treat accordingly.

Q1: Can you tell which one? - **C -** … correct (sort of… it's apparently a gateway so technically not CII). Now,

Q2: Who is the "identifiable individual" to whom this information relates?

Don't worry, even though this constitutes a disclosure of personal information, we have that person's consent.

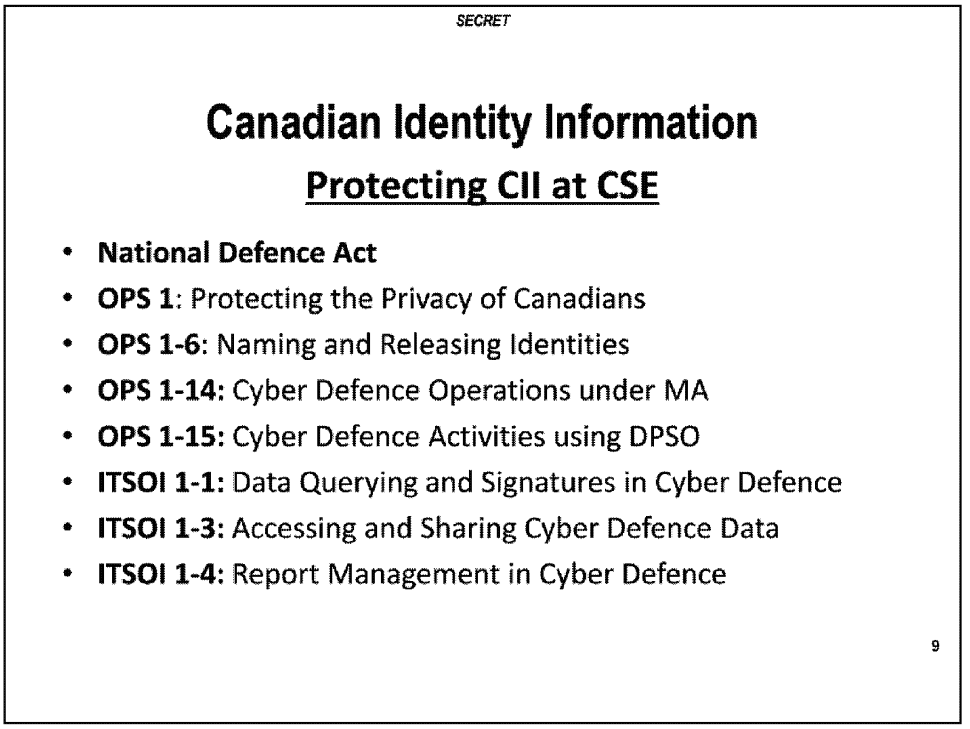
(first is [redacted] second is [redacted] third is "Canadian")



Answer: all except [redacted]

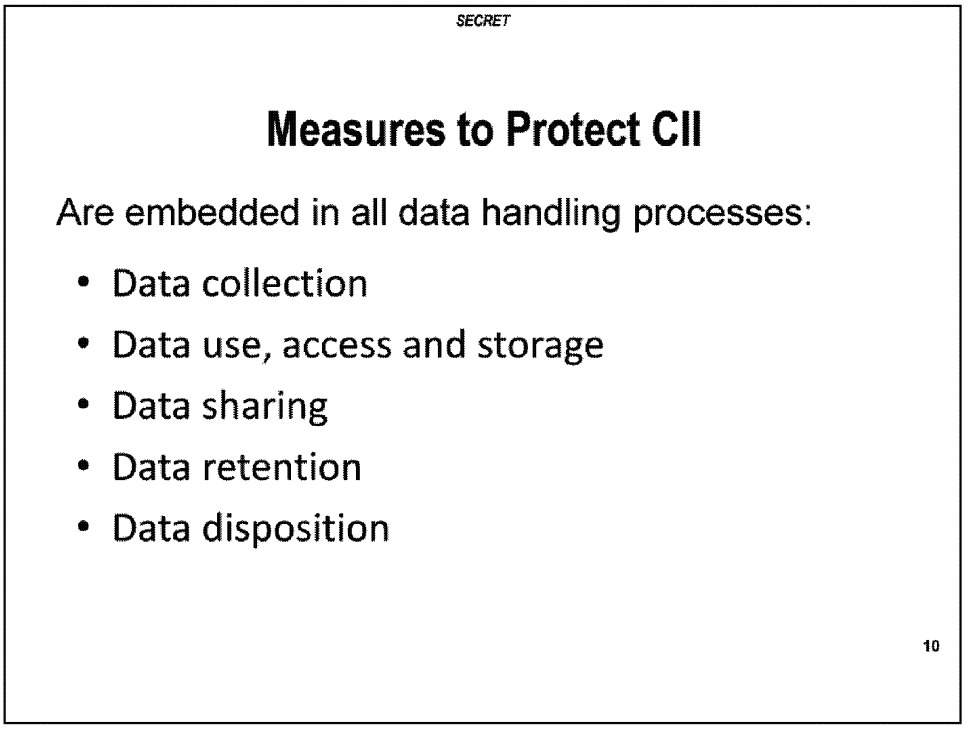
If discussion on these topics has not already occurred, bring up the point of:

[redacted]

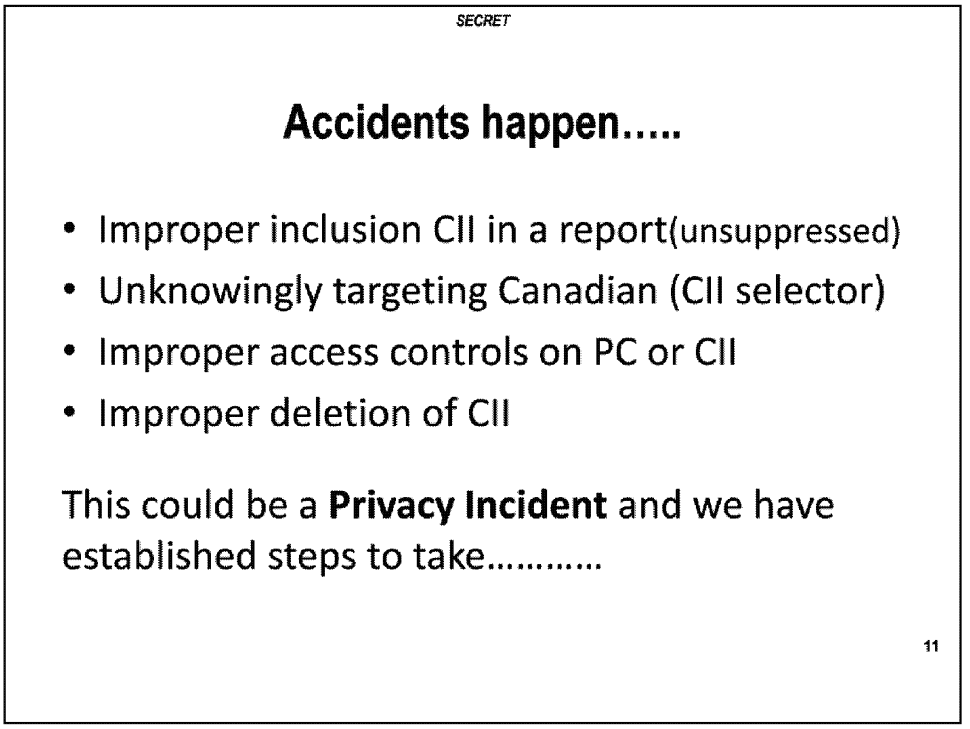


Obviously Protecting Canadian Identity Information is important and sometimes complicated business at CSE

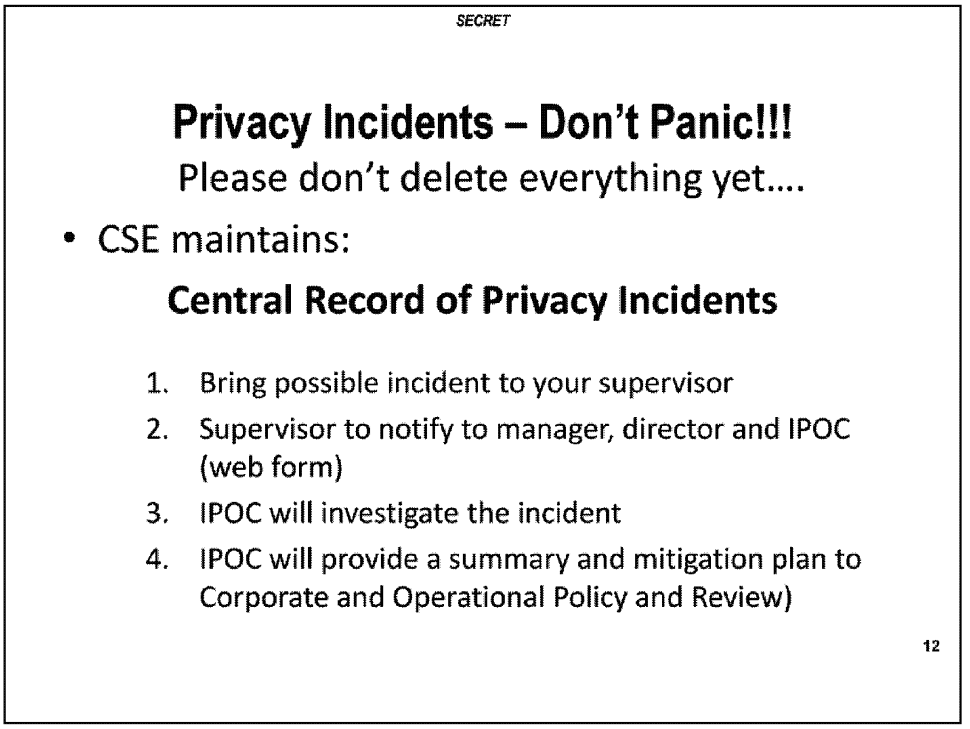
- This is just a sampling of a well defined framework that governs our work with CII. – you don't have to memorize all of this! Just be aware, **CII is important business and we have it covered**. We will get into more detail shortly.



- As mentioned, we have a pretty large framework in place to ensure we protect CII properly in the course of our cyber defence activities. Handling CII is an embedded consideration at each phase of our operations.



Of course there could be other possibilities, so if you are not sure, always check!

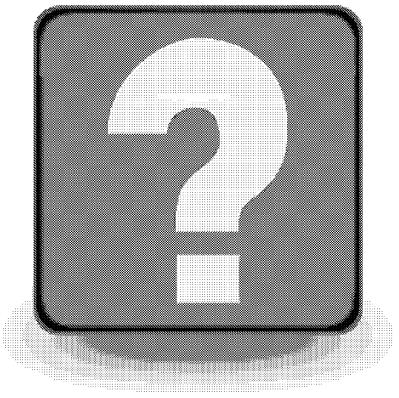


Really important that you understand – we know '**privacy incidents' will happen**. Given the volume of CII we encounter in our [redacted] on Canadian Government networks.

We hope to make you more aware of their potential and to encourage you to promptly follow the established procedures to enable us to control the extent of damage and to take timely corrective measures.

At some point all of our activities are reviewed by OCSEC – We rather find these things ourselves than in the course of a review.

SECRET



13