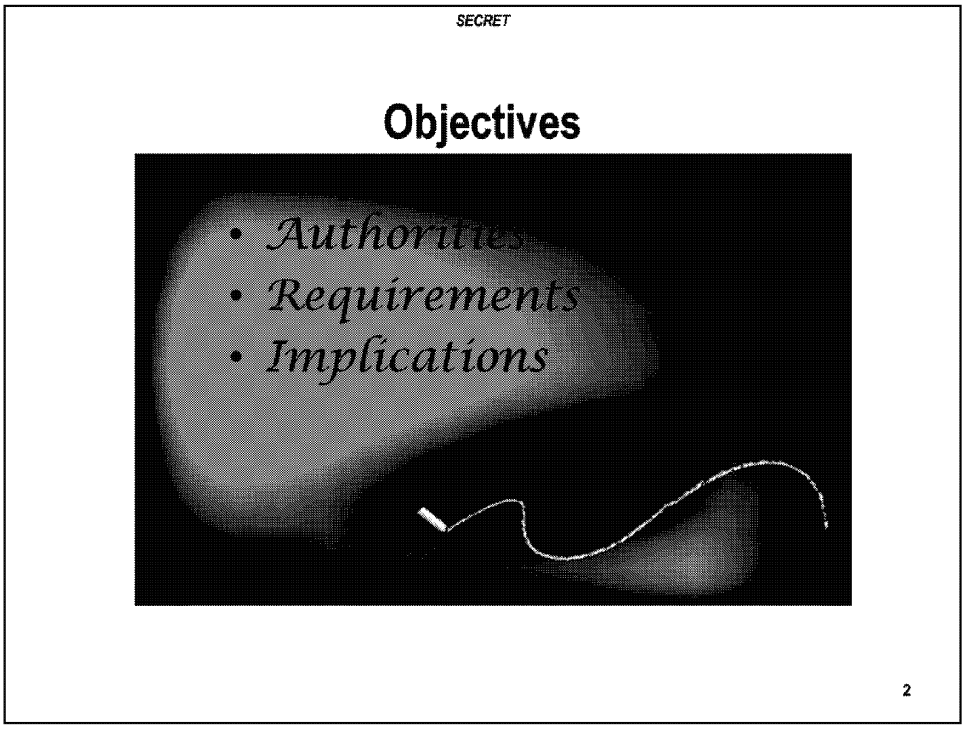
Cyber Defence Policy Awareness Curriculum

MA VS NON-MA

1



Introduction and Background to the Cyber Defence Policy Awareness Curriculum Workshop

Non-MA
Data Provided by System Owner (DPSO)

IRRELEVANT

Non-MA DPSO Requirements

IRRELEVANT

Principles of Sharing Non-MA DPSO data

IRRELEVANT

Non-MA DPSO Private Communications

IRRELEVANT

Additional Policy Requirements....

IRRELEVANT

Examples of Non-MA (DPSO)

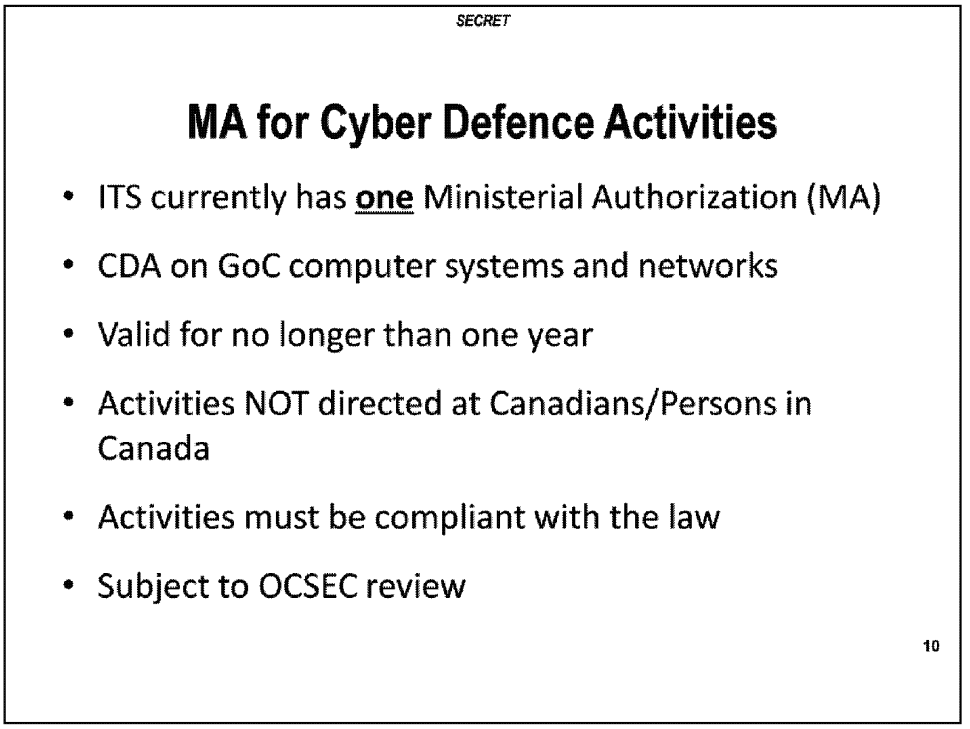
IRRELEVANT

Ministerial Authorization for CDA

Subsection 273.65(3) of the NDA permits the Minister to issue a Ministerial Authorization allowing CSEC to intercept private communications for the sole purpose of protecting computer systems or networks of the GC from mischief, unauthorized use or interference.

9

Note: **NOT** 'for systems of importance to GC' – (ie. critical infrastructure) MA only possible for GC systems and networks as it is currently worded in the NDA.



- The ITS MA is currently "**Ministerial Authorization for CSE Cyber Defence Activities**"

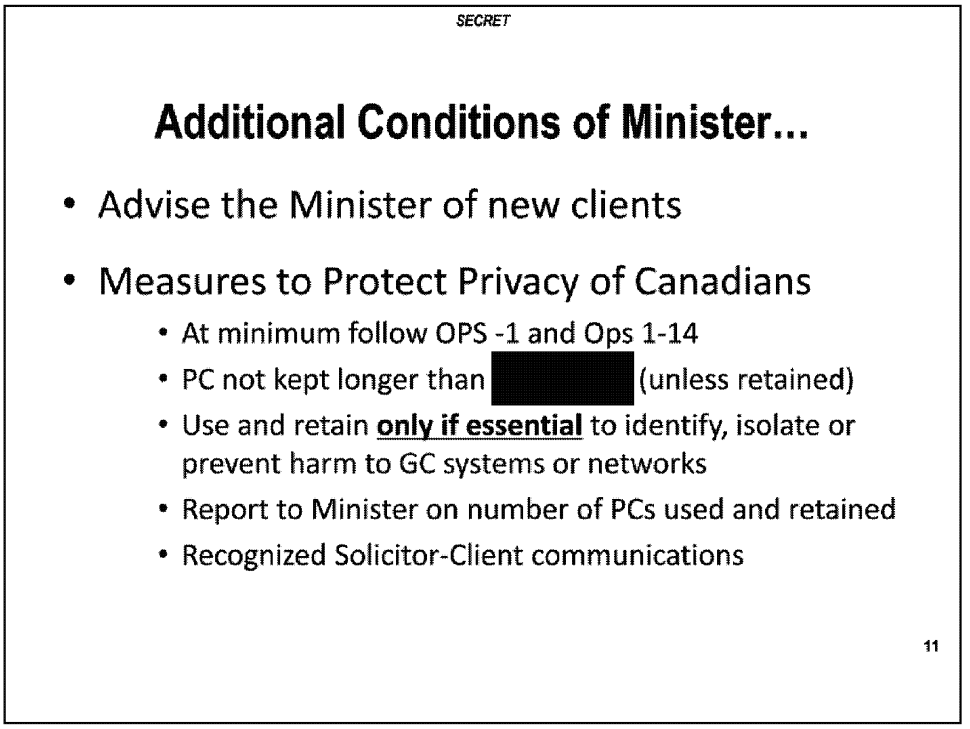
- Authorization for CSE to engage in cyber defence activities on **Government of Canada computer systems and networks** (that risk the interception of private communications) - This is a "Legislative Shield" from the Criminal Code (sec 184 – interception normally illegal)

- The MA for CDA is valid for up to 12 months (NDA requires MA's to be no longer than 12months – can be for smaller periods of time)

- Note: we look for the threat…our target is the threat…however, Canadians or Persons in Canada may be implicated in threat discovery, as such, we must be very mindful about how we direct our activities to ensure we are not "targeting Canadians". We will get into more detail about this shortly.

- Compliant with the law—we referenced laws that impact our operations –Criminal Code, Privacy Act, Financial Administration Act, National Defence Act – but no laws of Canada are to be contravened during our operations. An example of other laws to be mindful of --- our Mandate is for very specific purposes, we are not an investigative body. IRRELEVANT

IRRELEVANT



According to the NDA:

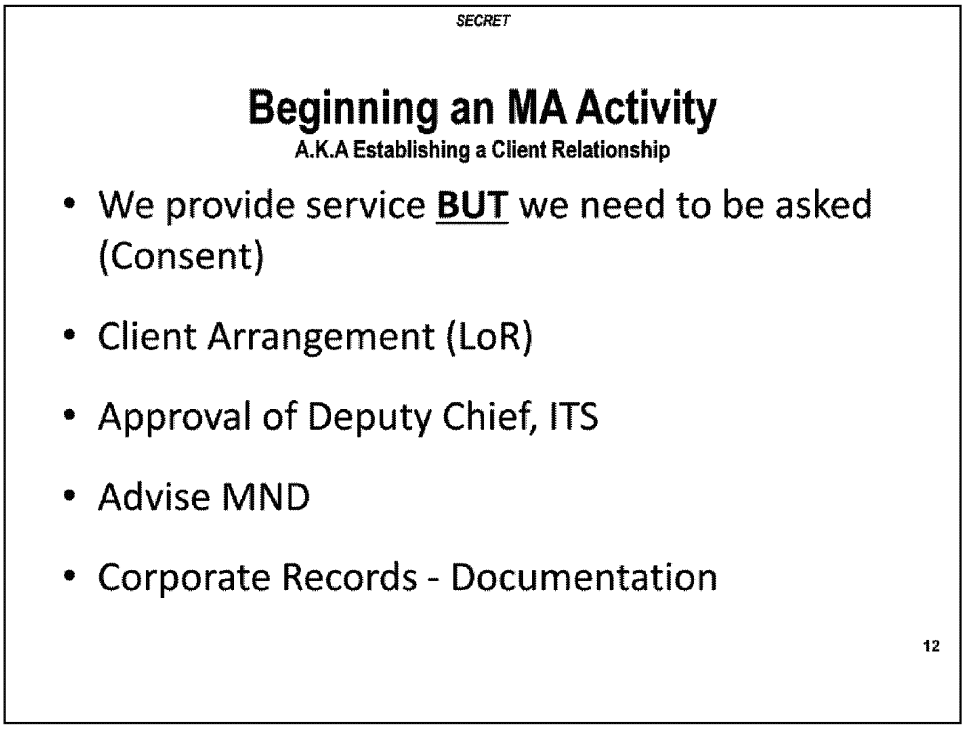
- CSE needs a letter of request from the Federal institution for our services under MA – and subsequent MOU follows to solidify the specifics of the arrangement for CSE services under MA

- CSE **must advise the minister on each new client** (Letter of Request). This used to be a requirement before beginning activities, but can now be done afterwards.

- The MA may contain **additional conditions that the Minister considers advisable to protect the privacy of Canadian**, including additional measures to restrict the use and retention, access to and disclosure of information derived from Private Communications

- *** PCs in their 'raw' state – **NOT to be kept longer than** [redacted] Our MA only allows us to have them in this raw state for a maximum of [redacted] If you want to keep it longer – it must be 'used and retained' – and as noted earlier – must be 'essential'. So – this is significant because this is actually part of our 'conditions' of our MA that the Minister is imposing. Therefore – retention around PC is serious business.

- Private communications used and retained by CSE **must be counted and reported to the Minister** (It's pretty apparent, PCs are serious business to the Minister and ultimately to us)



OPS 1 (4.2) Precondition Consent: **Before conducting cyber defence activities** with or without an MA, **CSE requires the consent of a system owner**, or must be satisfied that the system owner has given consent if the requesting institution is an intermediary (eg.SSC or Public Safety)

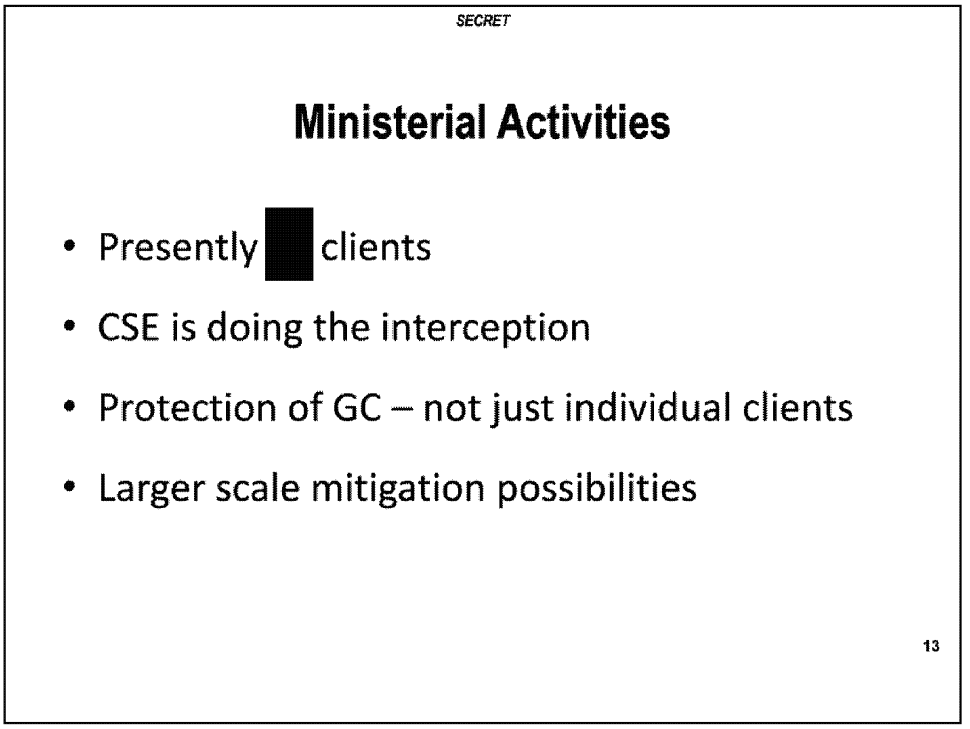
OPS 1-14 (2.1) – Details the documentation requirements

System owners have their own authority to monitor their networks, for CSE to be assisting or acting on their behalf, **we must be invited in**. Therefore we need to document the request. **NOTE**: it must be signed by the 'appropriate' client authority. (we do not verify who that is, it is to the department to determine that.)

Prior to deploying the tool or service, ITS establishes a client relationship to document a service agreement. This is now done through a Letter of Request (LoR) and a CSE response. This is to be approved by DCITS.

Sometime after or before deploying the initial service/tool – we **MUST** advice the Minister of the new client (this is the MA requirement and is further captured in OPS 1-14)

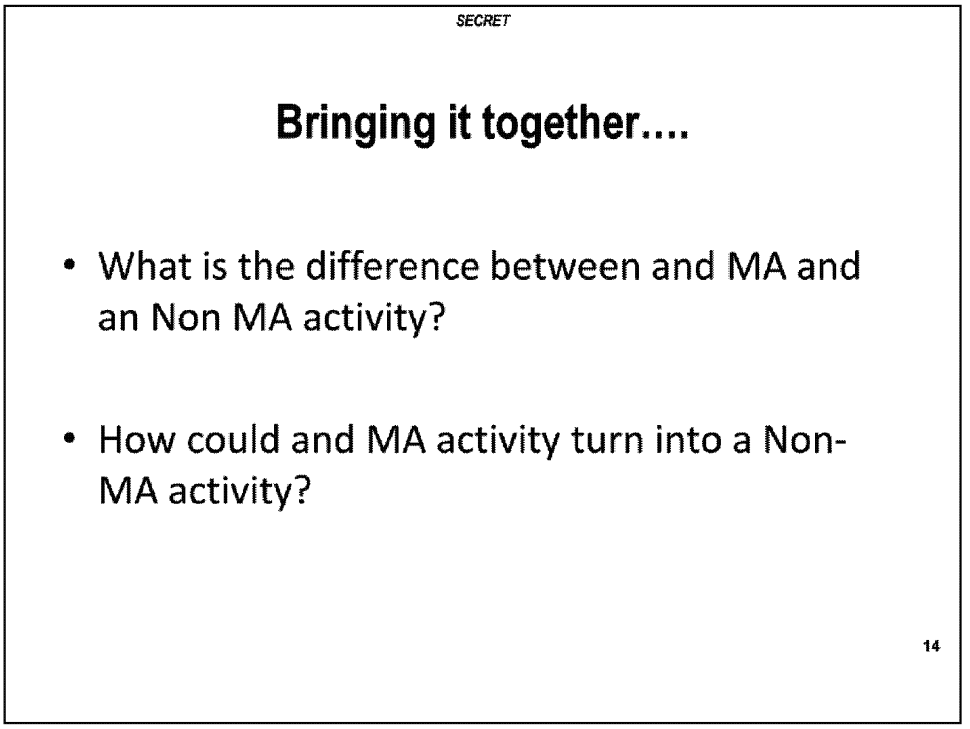
As these are either Policy or Ministerial Authorization requirements – we MUST **keep proper documentation** in the Client file in the Corporate Record system (CERRID). They must be retrievable for Compliance, OSCEC or other review requirements.



Current Clients: CSE , NRCAN, SSC, NRC, [redacted] (DND), [redacted] [redacted] DFATD, [redacted]

Explain why CSE needed to be a client…as on the surface that seems odd.

The MA gives a greater flexibility for Sharing and use of intercepted PC for the protection of the greater GC---not just protection of the ONE system from which data came. (which is the limitation of the CCC/FAA authority).



Illustrate the difference of requirements in with an example of malcode received in an email to Kerri at DFATD (under MA) vs Kerri working at [redacted] (Non-MA). Privacy consent…sharing restrictions etc.…