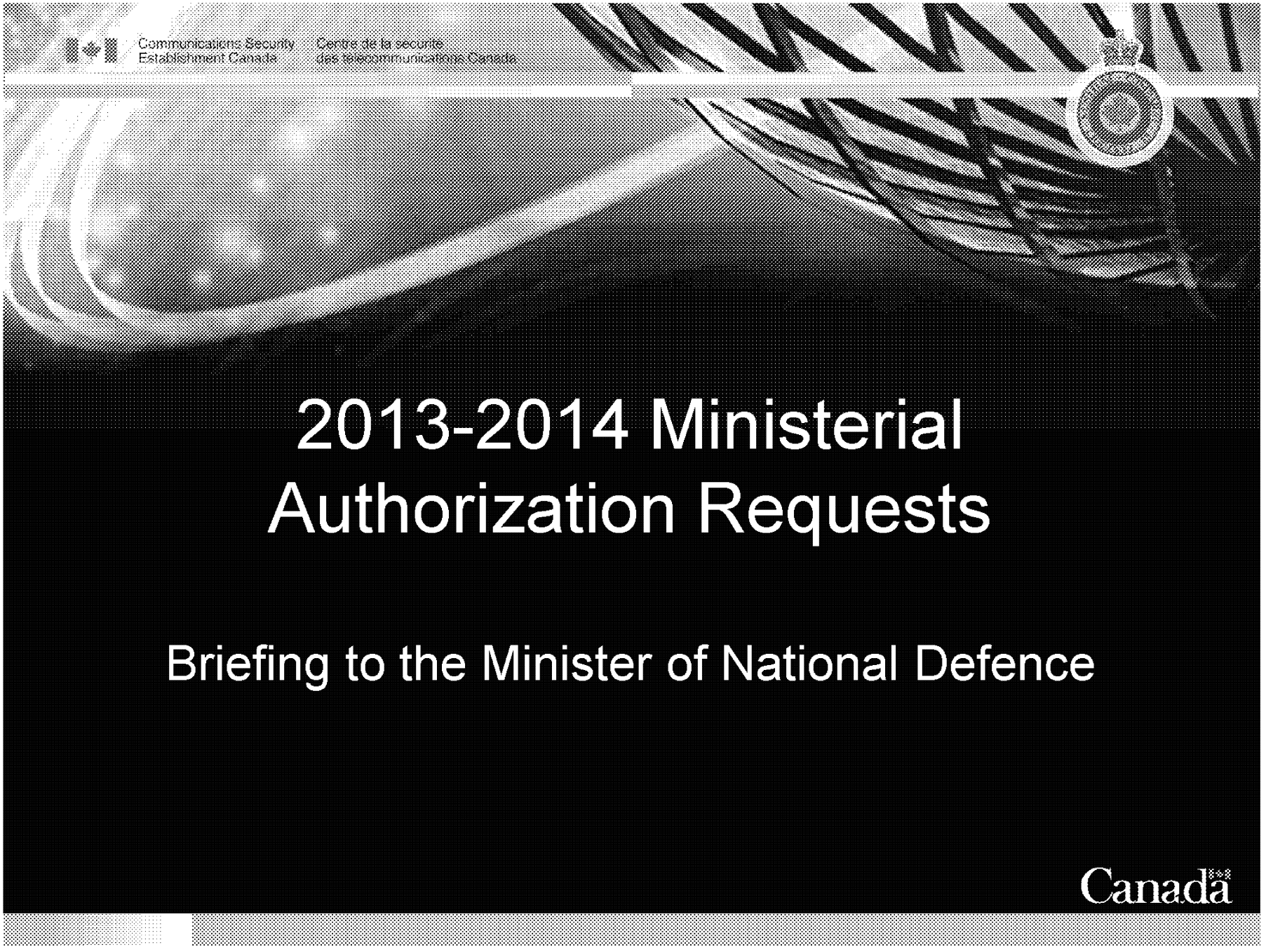
Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés



Objective of Today's Meeting

- Seeking your approval for the 2013-2014 SIGINT and ITS Ministerial Authorizations (MAs) and Ministerial Directives (MDs) on [redacted]
- There are four MAs to be renewed for 2013-2014
  - MAs authorize CSEC to undertake collection activities which risk the incidental interception of private communications
- There are five MDs to be renewed for 2013-2014
  - [redacted]

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Ministerial Authorizations (MAs): Overview

- MAs authorize CSEC to undertake activities or a class of activities to pursue its foreign intelligence collection or information technology security mandates when these activities risk contravention of the *Criminal Code* provision against the interception of private communications
- The MA regime also enables CSEC to conduct operations consistent with its foreign intelligence collection (SIGINT) and information technology security protection (ITS) mandates
- Without an MA in place, CSEC would be in violation of the *Criminal Code* if it intercepted a private communication in the conduct of its mandated activities

Canada

Ministerial Authorizations (MAs): Overview (cont'd)

- The *National Defence Act* outlines specific criteria that CSEC must meet before an MA can be issued; the protection of the privacy of Canadians is paramount in all CSEC activities

- All activities conducted under MAs are reviewed by the CSE Commissioner

- In his latest report, the Commissioner once again concluded that CSEC continues to act lawfully in the conduct of its current activities

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

SIGINT Ministerial Authorizations: 2013-2014

CSEC is requesting the approval of three SIGINT MAs which target foreign data and communications:

1. [redacted] Targets foreign communications [redacted]

2. [redacted] targets foreign communications [redacted]

3. [redacted]

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Conditions to be Satisfied: SIGINT MAs

You may issue a SIGINT Ministerial Authorization only if you are satisfied that CSEC has met four conditions:

Condition	How the Condition is Met
1. The interception will be directed at foreign entities located outside Canada	CSEC uses "selectors" (communications addresses such as phone numbers, email addresses) as well as other precise search criteria to target foreign entities located outside Canada. Analysts conduct in-depth research on targets and selectors to confirm they are foreign.
2. The information to be obtained could not be reasonably obtained by other means	CSEC's targets are foreign entities who conceal information that is required by the Government of Canada—whether terrorist plans [redacted] Except for a human intelligence asset, intercepted communications are the only potential source for the information being sought.

Canada

Conditions to be Satisfied: SIGINT MAs (cont'd)

Condition	How the Condition is Met
3. The expected foreign intelligence value of the information that would be derived from the interception justifies it	CSEC collection activities provide unique intelligence on all Cabinet-approved intelligence priorities. The Request Memorandum for each MA activity also includes a description of the value of its intelligence collection. Year-end metrics will also be provided for each collection activity in early 2014 in the MA Year-End Report to MND.
4. Satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security	CSEC conducts its activities in accordance with all relevant legislation, Ministerial Directives and operational policies in order to protect the privacy of Canadians. Examples of specific measures which protect privacy are: access to databases which may contain Canadian information is highly restricted; identities of Canadians are suppressed in intelligence reports so nobody can identify them; and communications to, from or about Canadians with no foreign intelligence value are purged from CSEC systems.

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

ITS Ministerial Authorization: 2013-2014

CSEC is requesting the approval of one Information Technology Security MA:

1. Cyber Defence Activities (CDA): Upon request from a client department, CSEC will undertake cyber operations to detect threats and vulnerabilities in Government networks and systems and to mitigate malicious cyber activity directed at Government networks and systems

Canada

Conditions to be Satisfied: ITS MA

You may issue an IT Security Ministerial Authorization only if you are satisfied that CSEC has met five conditions:

Condition	How the Condition is Met
1. The interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks	CSEC identifies and mitigates cyber threats on Government computer systems and networks in accord with its IT security mandate. Because CSEC is monitoring Government networks it is likely that CSEC will intercept private communications in the course of its activities as malicious activity directed against GoC computer systems and networks is often disguised as normal or legitimate files or network traffic.
2. The information to be obtained could not be reasonably obtained by other means	It is impossible to effectively identify and prevent potential cyber threats from harming GoC computer systems or networks without acquiring and analyzing a copy of suspicious files, computer processes or network traffic.

Canada

Conditions to be Satisfied: ITS MA (cont'd)

Condition	How the Condition is Met
3. The consent of persons whose private communications may be intercepted cannot reasonably be obtained	While CSEC obtains the consent of the requesting federal institution, it is impossible to obtain the consent of all persons outside the federal institution network. Obtaining this advance consent may also alert malicious actors to CSEC's activities.
4. Satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained	CSEC only conducts Cyber Defence Activities on the networks of requesting departments or agencies. In addition, CSEC [redacted] deletes all network data not used or retained for reporting.
5. Satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information	Examples of specific measures which control the use of network information include suppression of Canadian identities in reporting, highly restricted access to databases containing Canadian information.

Canada

Ministerial Directives: [redacted]

- Five Ministerial Directives (MDs) related to the CSEC [redacted] Program require your signature.
- These MDs govern [redacted]
- MDs are renewed annually.
- [redacted]
- The [redacted] collection that is enabled by [redacted] MD is essential to the CSEC SIGINT program.
  - In the 2011-12 MA year [redacted] intelligence reports generated by CSEC, CFIOG and Five Eyes partners based on CSEC [redacted] collection.

Canada

Ministerial Directives: [redacted]

- There are two types of Ministerial Directives that govern the [redacted] Program:
  1. Overarching 2012 Ministerial Directive on [redacted] Program (This is a standing MD and does not require annual renewal)
  2. Five [redacted] MDs (renewed annually)
- The five [redacted] MDs are listed below. Each [redacted] is referred to by a cover name:
  1. MD on [redacted]
  2. MD on
  3. MD on
  4. MD on
  5. MD on

Canada

Privacy Protection: Overview

- CSEC is prohibited by law from directing its foreign intelligence activities against Canadians anywhere or any person in Canada
- CSEC applies rigorous protections to inadvertently collected private communications
  - Dedicated Operational Policy unit focused largely on privacy protection
  - Embedded Department of Justice team to provide advice to CSEC staff
  - External review by the CSEC Commissioner and Privacy Commissioner
- Ministerial Directive (MD) sets out Minister's expectations for the protection of the privacy Canadians
  - Privacy of Canadians MD: revised MD nearing completion

Canada

Privacy Protection: Specific Measures

- Specific measures taken by CSEC to protect the privacy of Canadians include:
  - Access to 'raw SIGINT' databases is restricted within CSEC; allies and domestic partners do not have access to CSEC-collected raw intelligence which may contain Canadian information
  - Canadian information in both cyber defence and SIGINT reporting is suppressed so no Canadian can be identified by domestic partners or allies
  - The release of a Canadian identity to a domestic or allied partner requires a rigorous justification; there are no exemptions or blanket approvals to release Canadian information
  - All network data derived from cyber defence activities is deleted [redacted] unless specifically marked for retention by a CSEC analyst; a similar process exists in SIGINT for information to, from or about a Canadian
  - For both SIGINT and cyber defence activities, CSEC conducts regular internal monitoring and auditing to ensure policies and procedures are being implemented diligently
  - All metadata associated with a Canadian that is shared with Five Eyes partners is "minimized" so our allies cannot identify the Canadian

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Information Sharing

- Strict policy controls on sharing of information about Canadians with domestic and allied partners
- Domestic: CSEC shares intelligence with several Canadian security and intelligence organizations (e.g. CSIS, RCMP, CAF, CBSA, DFATD)
  - Any information that could identify a Canadian is removed from all CSEC intelligence reports
  - Domestic partners may request the release of the identifying information, but must provide a thorough justification and an explanation of how that information will be used
- International: Agreements with allies regulate sharing of Canadian information with Five Eyes partners
- CSEC guided by MD on Risks in Foreign Information Sharing

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Summary

- A table of significant changes to the MAs and Memoranda has been provided for your reference (Annex A)
  - From the 2012-13 MAs and Memos to the 2013-14 versions there have been minimal changes to the MAs and the activities they authorize
- The CSE Commissioner has found CSEC to be lawful in all activities conducted under Ministerial Authorization
  - The CSE Commissioner reviews CSEC activities under MA on an annual basis
- CSEC will return to you immediately should any serious issues arise in the conduct of MA activities

Canada

Released under the ATIA - unclassified information
Divulgué en vertu de la LAI - renseignements non classifiés

Recommendation

- It is recommended that you approve by Nov 30
  1. CSEC's 2013-2014 requests for new Ministerial Authorizations, and
  2. CSEC's 2013-2014 requests for new Ministerial Directives on [redacted]
- CSE will return with an enhanced Ministerial Directive on the Privacy of Canadians in the near future

Canada

Annex A: Changes to 2013-2014 MAs and Memos

MA	The change	Reason for change
Cyber Defence Activities	1. "on which it intends to act." Added to clarify when CSEC would notify the Minister of a Letter of Request. 2. "Letter of Request" replaced with "request in writing". 3. "signed by an appropriate individual acting on behalf of the requesting federal institution." Removed to clarify language.	Previously, the wording suggested that CSEC should go to the Minister whenever it received a Letter of Request, even if it did not intend to act on it. Therefore the change was to clarify that CSEC would only go to the Minister when it received a request on which it had decided to act. Additionally, the wording "Letter of Request" was replaced with "request in writing" as there was concern that the former wording was too limiting.

All Memos: All statistics and metrics were updated for 2013-2014.

[redacted]

Cyber Defence Activities (CDA) Memo: Cyber incident stats were updated with 2012 statistics. There was a notable decrease in cyber threat incidents in 2012 in comparison to 2011 due to improved mitigation efforts, but there was concern that this misrepresented the threat environment (making it appear as if cyber threats were diminishing), therefore 2011's cyber threat incident numbers were not included in this year's memo. (p.2 para 1)

Canada