



Part I

2012-2013 Ministerial Authorization Requests

Briefing to the Minister of National Defence
20 November 2012

*Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information*

Canada 



Ministerial Authorizations (MAs): Overview

- MAs authorize CSEC to undertake activities or a class of activities to pursue its mandate 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 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
- The National Defence Act outlines specific criteria that CSEC must meet before you can issue an MA. The protection of the privacy of Canadians is paramount in all CSEC activities
- All activities conducted under MAs are reviewed by the CSE Commissioner
- To date, CSE Commissioner has determined that all of CSEC's activities that he has reviewed have been lawful

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada



2012-13 MA Rationalization

- CSEC undertook a significant effort over the past year to rationalize application of the CSEC MAs to ensure they are applied against classes of activities, as specified in the legislation
- The MA Request Memos this year better describe how mandated activities risk interception of private communications and how CSEC mitigates this risk
- The intent of this new approach is to provide you with a more fulsome understanding of the value of each Class of Activity and to locate the risk of intercepting private communications
- This has reduced the number of SIGINT MAs from six to three
- MAs will no longer be used to approve new programs and these will be authorized in accordance with existing authorities, and if relevant, an updated Annex will be submitted to the Minister



CSEC 2012-2013 Ministerial Authorization (MA) Request Package

Program	2011-12 MAs	2012-13 MAs
SIGINT (A Mandate)	[REDACTED]	[REDACTED] Collection
	5. Support to Canadian Mission in Afghanistan	[REDACTED] Collection
	[REDACTED]	[REDACTED] Collection
IT Security (B Mandate)	7. Cyber Defence Operations	Cyber Defence Activities
	8. Active Network Security Testing (Discontinued in 2012)	

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada



SIGINT Ministerial Authorizations: 2012-2013

CSEC is requesting three new SIGINT MAs:

1. [REDACTED] Targets foreign communications [REDACTED]
[REDACTED]
 - This new MA incorporates activities that were previously conducted under the MAs for [REDACTED] Interception Activities Involving [REDACTED] and Interception Activities [REDACTED]

2. [REDACTED] Targets foreign communications
[REDACTED]
 - This MA includes activities that were previously conducted under the [REDACTED] [REDACTED] as well as an MA for collection activities [REDACTED]

3. [REDACTED]



Conditions to be Satisfied: SIGINT MAs

- You may issue a Ministerial Authorization only if you are satisfied that CSE has met four conditions:
 1. The interception will be directed at foreign entities located outside Canada;
 2. The information to be obtained could not be reasonably obtained by other means;
 3. The expected foreign intelligence value of the information that would be derived from the interception justifies it; and
 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.
- How CSEC meets these conditions is outlined in the enclosed SIGINT MA request memos



Conditions to be Satisfied: SIGINT MAs

- CSE minimizes the inadvertent interception of private communications through application of selection criteria to collected data or targeted foreign [REDACTED]
- CSE cannot know in advance if the targeted foreign entities will communicate with persons in Canada,
 - CSE may end up intercepting a one-end Canadian communication originating or terminating with the foreign entity
- CSE has measures 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



ITS Ministerial Authorizations: 2012-2013

CSEC is requesting one Information Technology Security MA:

1. Protection of Government of Canada Computer Systems and Networks: 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
- The previous Active Network Security Testing (ANST) MA is not being renewed since CSEC ceased offering this program during the past year



Conditions to be Satisfied: ITS MAs

- You may issue a Ministerial Authorization only if you are satisfied that CSE has met five conditions:
 1. the interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks;
 2. the information to be obtained could not reasonably be obtained by other means;
 3. the consent of persons whose private communications may be intercepted cannot reasonably be obtained;
 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; and,
 5. satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.
- How CSEC meets these conditions is outlined in the enclosed CDA MA Request Memo

*Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information*

Canada



Conditions to be Satisfied: ITS MAs

- CSE cyber defence activities are conducted on Government of Canada systems and networks
- All communications transmitted on those systems and networks between two or more persons are private communications
- Suspect communications may be intercepted for further analysis by CSE cyber defence personnel
- All information obtained by CSE from a federal institution's network or system during cyber defence activities is used or retained in accordance with established policies and procedures



Recommendation

- It is recommended that you approve CSEC's 2012-2013 requests



Part II

Ministerial Directives: Request for Signature

*Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information*

Canada



Ministerial Directives:

- Four Ministerial Directives (MDs) related to CSEC [REDACTED] activities require your signature.
- These MDs govern CSEC [REDACTED]
- These (ECI) MDs are:
 1. MD on [REDACTED]
 2. MD on [REDACTED]
 3. MD on [REDACTED]
 4. MD on [REDACTED]



MD on Accountability Framework

- Replaces 2001 Accountability Framework MD to reflect CSEC's new stand-alone status.
- Responds to Prime Minister's directive that relevant CSEC MD be amended.
- This MD was specifically highlighted as one requiring updating by the Prime Minister.
- CSEC revision do not alter fundamental direction but streamline the Chief's reporting to the MND.



MD updates

- The following MDs were also updated to reflect CSEC's new stand-alone status.
 - MD on Privacy of Canadians
 - MD on [REDACTED]
 - MD on [REDACTED]
 - MD on [REDACTED]
 - [REDACTED] (ECI)



MD on Intelligence Priorities

- Proposed changes to 2005 MD reflect evolving threat environment where sharing of foreign metadata between business lines is needed for cyber defence
- The updated MD will enable SIGINT to provide ITS cyber defence personnel access to a subset of unsuppressed foreign metadata for cyber defence purposes.
- CSEC's reporting structure and disclosure procedures remain adequate to protect the privacy of Canadians
- As a priority, all relevant Operational Policies will be updated before this MD is operationalized
- CSEC will return to you should there be any issues with operationalizing the MD



Recommendation

- CSEC recommends that the Minister of National Defence approve the following Ministerial Directives:
 - Four (ECI) [REDACTED] MDs;
 - Six PinG update MDs;
 - The annual Intelligence MD; and
- It is recommended you approve the eleven proposed Ministerial Directives