



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

TOP SECRET//SI//CEO

P.O. Box 9703  
Terminal  
Ottawa, Canada  
K1G 3Z4

C.P. 9703  
Terminus  
Ottawa, Canada  
K1G 3Z4

CERRID# 12185451

NOV 18 2014

**MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE**

**CSE [REDACTED] Collection Activities**

(For Approval)

**ISSUE**

The purpose of this Memorandum is to request a Ministerial Authorization for CSE's [REDACTED] collection activities that risk the interception of private communications.

The [REDACTED] Ministerial Directive authorizes CSE, within a rigorous assessment and approval framework, to conduct [REDACTED]

[REDACTED] Transformational changes in the global information infrastructure (GII) have made it much more difficult to collect communications and extract those of interest using traditional (i.e., [REDACTED]) collection methods. [REDACTED] assists in fulfilling CSE's legislated mandate by using more [REDACTED] methods to acquire specific, high-interest data and communications.

You may issue a Ministerial Authorization enabling [REDACTED] provided the conditions under subsection 273.65(2) of the *National Defence Act* (NDA) are met. Ministerial Authorizations are essential to the successful implementation of CSE's mandate; without them, the organization would be unable to collect the data from the GII that it requires to provide foreign intelligence, in accordance with the intelligence priorities of the Government of Canada (GC).

Although CSE cannot target Canadians or persons in Canada, and does not conduct [REDACTED] activities against [REDACTED] it may incidentally intercept private communications when conducting [REDACTED] activities. CSE may incidentally intercept a private communication when it uses [REDACTED] capability to intercept, [REDACTED] a communication of a foreign target that originates or terminates within Canada.

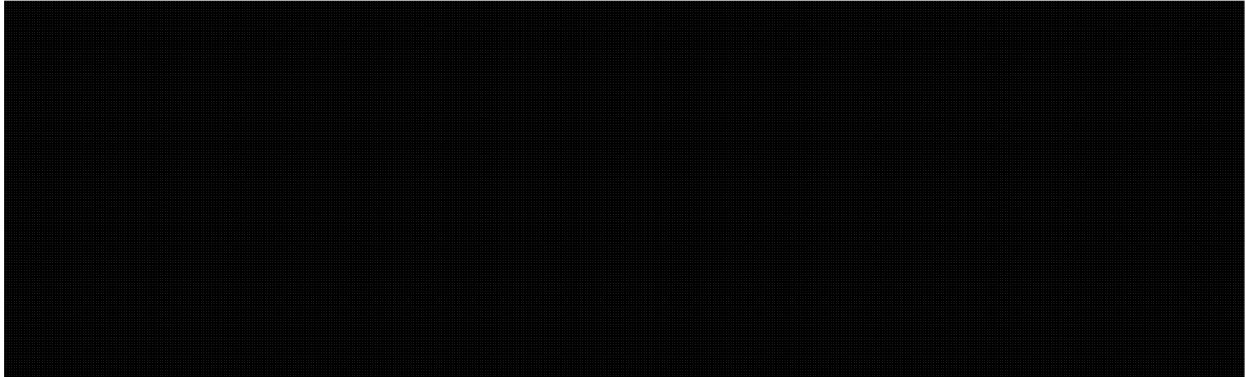
The interception of private communications – those that originate or terminate in Canada and where the originator has a reasonable expectation of privacy – is prohibited under Part VI of the *Criminal Code*. However, Part VI of the *Criminal Code* does not apply if, pursuant to subsection 273.65(1) of the NDA, you authorize CSE to intercept

Canada

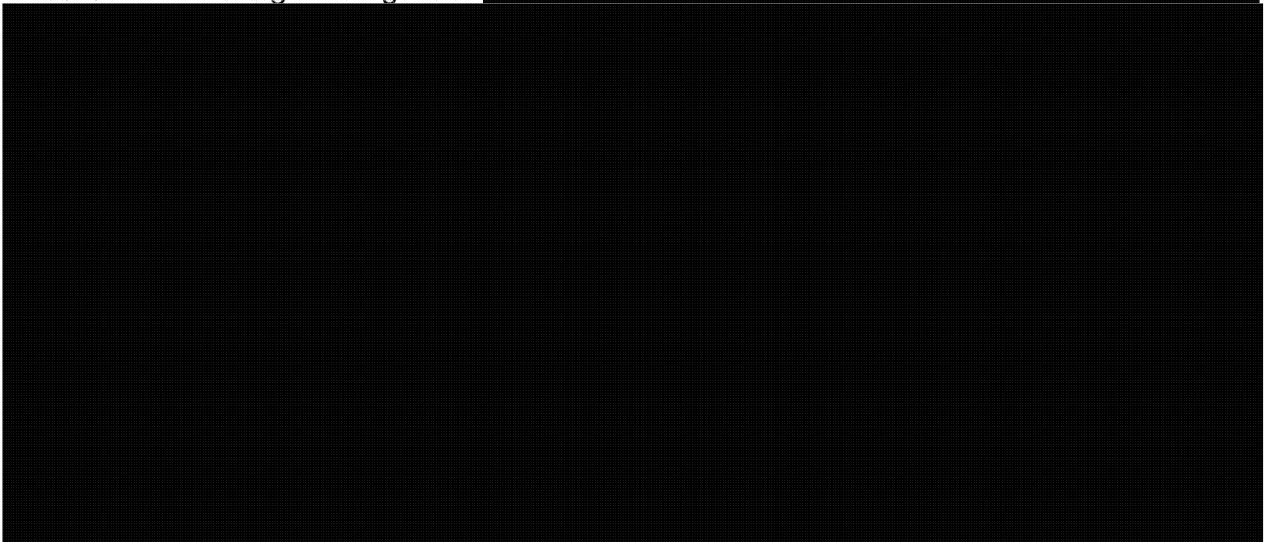
TOP SECRET//SI//CEO

private communications in relation to an activity or class of activities for the sole purpose of obtaining foreign intelligence.

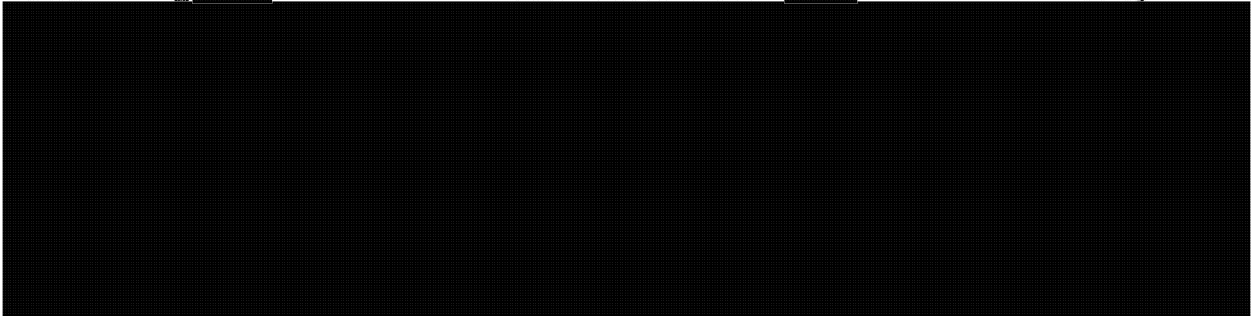
**CLASS OF ACTIVITIES TO BE AUTHORIZED: [REDACTED] COLLECTION**



**Rationale for CSE [REDACTED] Collection Activities:** Recent transformational changes to the GII, such as [REDACTED] have made it increasingly necessary for CSE to rely on [REDACTED] capabilities for the collection of foreign intelligence. [REDACTED]



**Conducting [REDACTED] Collection Activities:** CSE conducts [REDACTED] collection activities by [REDACTED]



[REDACTED]

CSE's [REDACTED] Selection Process: All CSE [REDACTED] collection activities acquire [REDACTED]

[REDACTED]

**Interception of Private Communications:** In accordance with Part VI of the *Criminal Code*, any communication that originates or terminates in Canada, where the originator has an expectation of privacy, constitutes a private communication. Given that [REDACTED] collection techniques are [REDACTED]

[REDACTED]

To date, there have been [REDACTED] reported intercepts of a private communication in the course of conducting a [REDACTED] collection activity. However, there is a [REDACTED] risk of intercepting private communications when a [REDACTED] technique results in the acquisition of a communication [REDACTED]

[REDACTED]

As a result, CSE requires a Ministerial Authorization to undertake [REDACTED] activities that risk the interception of private communications, as without lawful authority it is a criminal offence to intercept private communications.

**Foreign Intelligence Value of [REDACTED] Collection Activities:** Communications data that is [REDACTED] important source of foreign intelligence produced by CSE [REDACTED]. From December 2013 to May 2014, [REDACTED] collection was the [REDACTED] Canadian source for CSE-produced intelligence reports. Specifically, this program has provided intelligence on [REDACTED]

[REDACTED] Going forward, it is expected that this program will continue to provide intelligence on a broad range of issues including: [REDACTED]

[REDACTED] CSE will also continue to [REDACTED] targets of interest.

### **CONDITIONS TO BE SATISFIED**

You may issue a Ministerial Authorization only if you are satisfied that CSE has met the following four conditions set out in subsection 273.65(2) of the *NDA*.

- The interception will be directed at foreign entities located outside Canada;
- The information to be obtained could not be reasonably obtained by other means;
- The expected foreign intelligence value of the information that would be derived from the interception justifies it; and,
- 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.

In order to demonstrate in advance of conducting [REDACTED] activities that CSE has appropriate measures in place to meet each of these conditions, CSE uses a reasonableness standard that takes into account the particular context of the class of activity being authorized.

These conditions are met respectively as follows:

#### ***1. The interception must be directed at foreign entities located outside Canada***

CSE follows detailed procedures that provide reasonable grounds to suspect that interception activities are directed at foreign entities of foreign intelligence interest located outside of Canada. Intelligence analysts are required to prepare a written assessment<sup>1</sup>, to identify a foreign intelligence priority and to draft a justification to

<sup>1</sup> A foreign assessment must include an assessment of the nationality and location of an entity of foreign intelligence interest, [REDACTED]

outline the expected value of a collection activity, prior to initiating any [REDACTED] activities.

## ***2. The information could not be reasonably obtained by other means***

The nature of CSE's signals intelligence activities is such that the collected information (including any private communications) would not be shared voluntarily by the targeted foreign entity. In fact, many foreign targets make deliberate efforts to [REDACTED] information about their activities, capabilities, and intentions [REDACTED] from intelligence agencies, and specifically from CSE. As such, information [REDACTED] is often the only potential source for the intelligence being sought by the GC, and may only be obtainable by CSE [REDACTED] collection activities.

## ***3. The expected value of the interception would justify it***

Activities conducted under this Ministerial Authorization provide CSE with unique access to information about foreign entities and their activities, intentions, and capabilities, in accordance with GC intelligence priorities. Although there have [REDACTED] [REDACTED] incidentally acquired private communications from CSE's [REDACTED] activities to date, [REDACTED] provide unique foreign intelligence that meets GC priorities and assists Government decision-making, given the [REDACTED] of this collection program.

After the expiration of the current Ministerial Authorization for [REDACTED] activities, CSE will report to you on the full period of the authorization, in accordance with the reporting requirements outlined in the Ministerial Authorization.

## ***4. Satisfactory measures are in place to protect the privacy of Canadians***

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. A private communication is considered to be essential if it contains information that is necessary to the understanding of a target's identity, location, [REDACTED] capabilities or intentions, and is necessary for comprehension of that information in its proper context.

CSE's policies relating to accountability, the privacy of Canadians, and the conduct of [REDACTED] collection activities are outlined in the following Ministerial Directives and the associated operational policies:

- [REDACTED] Ministerial Directive;
- Collection and Use of Metadata;
- Accountability Framework Ministerial Directive; and,
- Privacy of Canadians Ministerial Directive.


CSE employees must conduct activities in accordance with the most current version of these Ministerial Directives and the associated operational policies. CSE will advise you of significant revisions to policies and procedures that have an impact on measures to protect the privacy of Canadians. OPS-1 is CSE's foundational policy on the protection of the privacy of Canadians and all other operational policies must comply with it. A copy of OPS-1 has been provided for your reference.

Where CSE incidentally intercepts a solicitor-client communication, it can only be used or retained if it is deemed essential to international affairs, defence, or security. This means that intercepted solicitor-client communications will be treated in an exceptional manner, as set out in the conditions in the Ministerial Authorization.

The use and retention of any recognized intercepted private communications essential to foreign intelligence will be reported to you in accordance with the reporting requirements outlined in the Ministerial Authorization. CSE's activities are subject to annual review by the CSE Commissioner to ensure their lawfulness.

### RECOMMENDATION

Ministerial Authorizations are vital legal instruments that enable CSE to fulfill its mandate without risk of criminal liability for the incidental interception of private communications. This Ministerial Authorization will permit CSE to continue its [REDACTED] activities that risk interception of private communications and provide valuable foreign intelligence to the GC, as well as CSE's domestic and international partners. It is recommended that you approve the attached Ministerial Authorization "Communications Security Establishment [REDACTED] Collection Activities" to be effective 1 December 2014 to 30 November 2015.



John Forster  
Chief

Attachment