



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

Your File Votre référence

Our file Notre référence

CERRID# 976801

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

CSE [REDACTED] Collection Activities

(For Approval)

ISSUE

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 *National Defence Act* (NDA), you authorize the Communications Security Establishment (CSE) to intercept private communications in relation to an activity or class of activities for the sole purpose of obtaining foreign intelligence.

You may issue a Ministerial Authorization provided the legislated conditions are met. These 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 global information infrastructure that it requires to obtain foreign intelligence, in accordance with the intelligence priorities of the Government of Canada.

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

CLASS OF ACTIVITIES TO BE AUTHORIZED: [REDACTED] COLLECTION

[REDACTED] applies to all technologies that rely on the [REDACTED] communications data on the global information infrastructure. While the application of [REDACTED] examples include [REDACTED]

It is important that CSE have the capacity to engage in [REDACTED] collection because over [REDACTED] % of the [REDACTED] on the global information infrastructure use a [REDACTED] to access communications networks. In addition, a particular [REDACTED]

Canada

TOP SECRET//SI//CEO

CSE [REDACTED] Collection Activities: CSE's [REDACTED] collection activities target foreign communications data that is [REDACTED]. Because [REDACTED] may be received [REDACTED] collection [REDACTED]

CSE uses various [REDACTED] collection technologies to acquire foreign signals for analysis. The choice of [REDACTED] collection technology depends on the nature of the [REDACTED] communications that CSE suspects are [REDACTED] communications data of foreign intelligence value, and where these communications are [REDACTED]. To support this determination, CSE may undertake a [REDACTED] in order to [REDACTED]

CSE [REDACTED] All CSE [REDACTED] collection methods [REDACTED] communications data collected from the global information infrastructure [REDACTED]

This [REDACTED] is essential because most [REDACTED] communications [REDACTED] in order to facilitate efficient [REDACTED] on the global information infrastructure. Given the [REDACTED] of the communications data that is [REDACTED] acquired through CSE [REDACTED] collection activities, it is essential that CSE [REDACTED] collected data [REDACTED] if it meets predetermined selection criteria associated with foreign intelligence targets.

[REDACTED] also renders communications [REDACTED] and in this [REDACTED] communications data [REDACTED] on the global information infrastructure. This makes it [REDACTED] for CSE [REDACTED] in [REDACTED] of collection whether all of the [REDACTED] data it collects will be foreign, irrespective of the [REDACTED] targeted by CSE activities. As a result, communications that are [REDACTED] CSE's [REDACTED] require [REDACTED] and determine if they are of potential foreign intelligence value. This analysis also minimizes the likelihood of inadvertent interception of private communications.

To facilitate this analysis, and under the authority of the 2011 Ministerial Directive on Metadata, CSE extracts metadata from the communications data [REDACTED]. Metadata does not include communications content, but is information used to identify, describe, manage or route communications. CSE requires it to map the global information infrastructure, support ongoing collection, identify new foreign intelligence targets, [REDACTED] to facilitate the targeted collection of communications of foreign entities that are of foreign intelligence value.

Selection criteria such as the telephone numbers, IP addresses, email addresses of targeted entities and other information extracted from [REDACTED] metadata are [REDACTED]

Selection criteria enable CSE to filter out extraneous data and provide CSE with greater certainty that the communications that CSE extracts [REDACTED] for interception will be of foreign intelligence value to the Government of Canada.

Communications data that is collected [REDACTED] but that is not identified by selection criteria for intercept is destroyed [REDACTED]

[REDACTED] This process can take [REDACTED] depending on [REDACTED]

Interception of Private Communications: The selection criteria facilitate the extraction of specific communications [REDACTED] and upon selection, these are forwarded to a consolidated CSE traffic repository for further analysis by CSE analysts. As data [REDACTED] is forwarded into the consolidated repository, it is [REDACTED] communications and can be [REDACTED] by CSE personnel. [REDACTED] communications residing within the consolidated repository have been intercepted by CSE.

CSE minimizes the inadvertent interception of private communications through metadata analysis and application of selection criteria [REDACTED]. However, because CSE cannot know in advance if the foreign entities being targeted will communicate with persons in Canada, CSE may end up intercepting a one-end Canadian communication originating or terminating with the foreign entity. Any communication that originates or terminates in Canada where there is an expectation of privacy constitutes a private communication. As a result, CSE requires a Ministerial Authorization to undertake [REDACTED] collection activities, as without lawful authority it is a criminal offence to intercept private communications.

CONDITIONS TO BE SATISFIED

You may issue a Ministerial Authorization only if you are satisfied that CSE has met the four conditions set out in Subsection 273.65(2) of the NDA and is appropriately managing the risk of intercepting private communications.

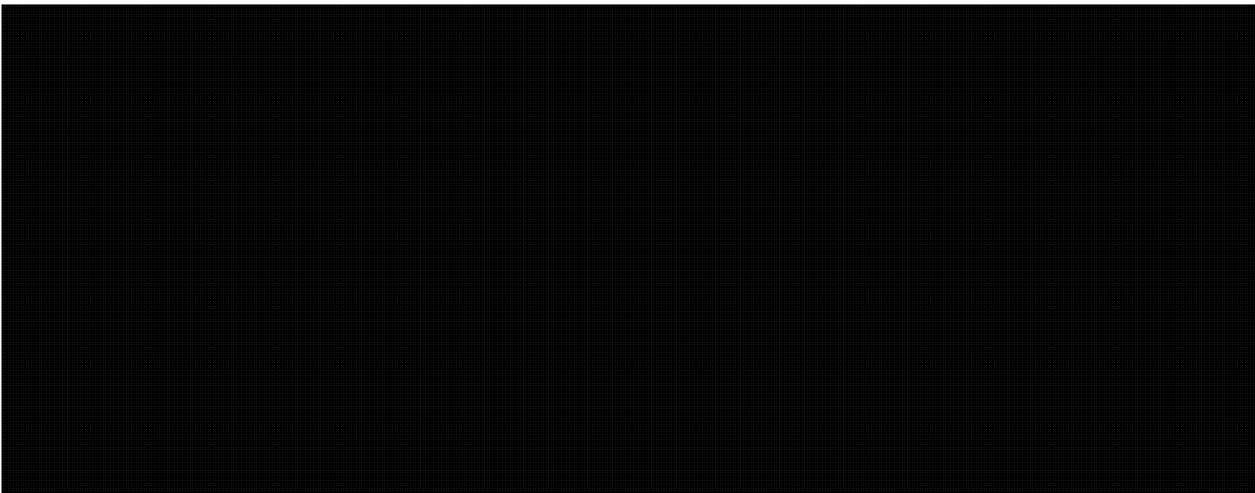
- The interception will be directed at foreign entities located outside Canada;
- The information to be obtained could not be reasonably obtained by other means;
- The expected foreign intelligence value of the information that would be derived from the interception justifies it; and
- Satisfactory measures 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 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 strict procedures that provide a reasonable assurance that interception activities are directed at foreign entities located outside of Canada. This includes maintaining an automated directory of selection criteria to identify the communications of a target of interest for intercept. Selection criteria can only be used to identify communications for intercept if CSE is satisfied that they relate to a foreign target and the external component of a communication. The use of selection criteria to identify foreign communications for collection provides CSE with a reasonably reliable means of identifying who one of the communicants is likely to be and whether he or she is located outside Canada before a communication is intercepted. Further, the content of a communication is [REDACTED] CSE has a reasonable assurance that the communication has at least one end located outside Canada.



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

The nature of CSE's signals intelligence activities is such that the intercepted information, including any private communications, would not be shared voluntarily by the targeted foreign entity. Further, in most cases, intercepted communications are the only potential source for the information being sought.

3. The expected foreign intelligence value of the information that would be derived from the interception justifies it

Activities conducted under this Ministerial Authorization provide CSE with unique access to the communications of targeted foreign entities and are an important source of information about these entities and their activities. CSE's [REDACTED] collection activities enhance its capacity to understand and locate targets of interest and provide CSE and its Allies with foreign intelligence in accordance with Government of Canada intelligence priorities.

CSE also derives technical information about global information networks from its [REDACTED] collection activities. This supports other collection activities and improves CSE's understanding of its targets and their communication patterns. For example, CSE's [REDACTED] collection activities are a rich source of information related to [REDACTED] and this research ultimately benefits CSE's own collection activities.

After the expiration of the current Ministerial Authorizations, CSE will report to you on the full period of the authorization for each activity, in accordance with the associated reporting requirements outlined in the Ministerial Authorization. Detailed information on each of the programs that CSE operates under the [REDACTED] Class of Activities Ministerial Authorization is provided in Annex A.

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

- Accountability Framework Ministerial Directive;
- Privacy of Canadians Ministerial Directive;
- Collection and Use of Metadata Ministerial Directive;
- OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities; and
- OPS-1-13: Operational Procedures Related to Canadian [REDACTED] Collection Activities

CSE employees must conduct activities in accordance with the most current version of these Ministerial Directives and operational policies. The organization will advise you of any 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. Copies of OPS-1 and OPS-1-13 are attached for your reference at Annex B.

Where CSE incidentally intercepts a private communication, a communication of a Canadian outside Canada, or a solicitor-client communication, the intercept can only be used or retained if it is deemed essential to international affairs, defence or security. This means that:


- communications that both originate and terminate in Canada, will, upon recognition, be marked accordingly and not be used further by CSE. These communications are either deleted from CSE's databases or over a short duration overwritten from CSE's [REDACTED]
- 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.

Solicitor-Client Privilege

RECOMMENDATION

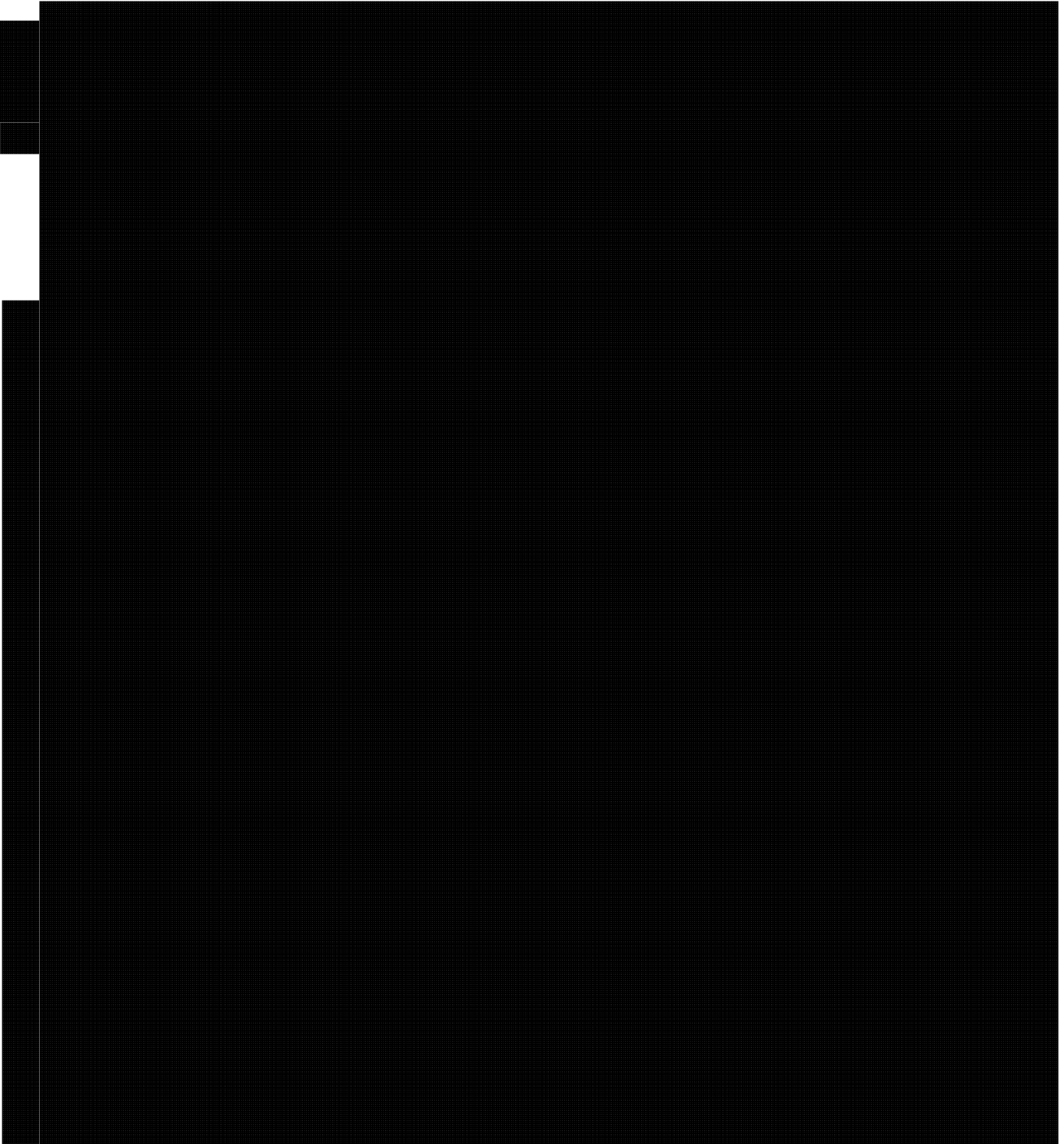
Ministerial Authorizations are vital legal instruments that enable CSE to fulfill its mandate without risk of criminal liability for the incidental interception of private communications. This Ministerial Authorization will permit CSE to continue its collection activities that target foreign [REDACTED] and provide valuable foreign intelligence to the Government of Canada, as well as CSE's domestic and international partners. It is recommended that you approve the attached Ministerial Authorization "CSE [REDACTED] Collection Activities," to be effective December 1, 2012 to November 30, 2013.



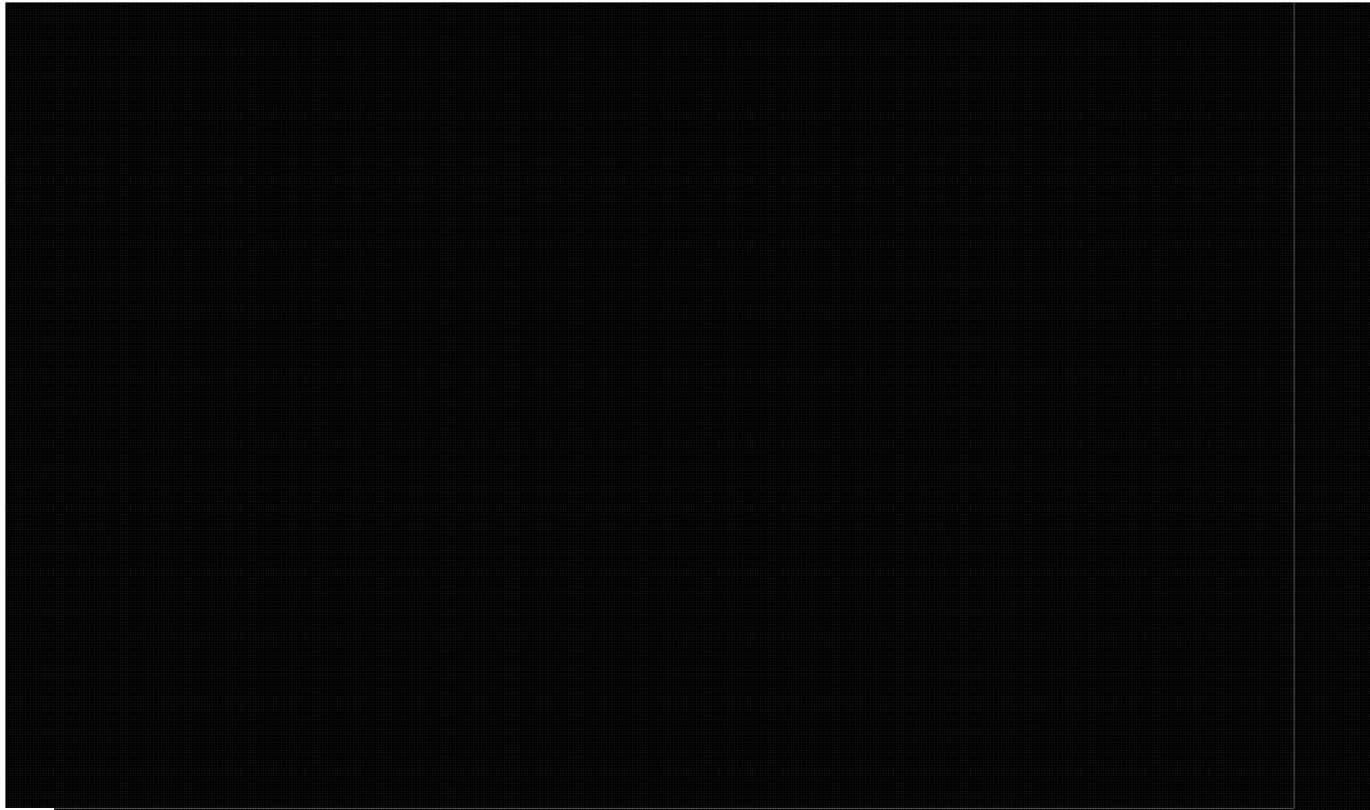
John Forster
Chief

Attachment

ANNEX A



TOP SECRET//SI//CEO



TOP SECRET//SI//CEO