



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# 12184774

NOV 18 2014

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

Collection Activities

(For Approval)

ISSUE

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

The Ministerial Directive authorizes the Communications Security Establishment (CSE), within a rigorous assessment and approval framework, to communications on the global information infrastructure (GII). Currently, the main method to acquire these communications is collection. collection may also potentially include activities against as authorized by CSE's foreign intelligence mandate.

You may issue a Ministerial Authorization enabling collection activities 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, it may incidentally intercept private communications when collecting foreign intelligence using collection activities.

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

Canada

TOP SECRET//SI//CEO

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

[REDACTED] applies to all [REDACTED]
[REDACTED] communications data on the GII, including [REDACTED]
[REDACTED]

Rationale for CSE [REDACTED] **Collection Activities:** [REDACTED] communications
may [REDACTED]

[REDACTED]
[REDACTED] These
factors contribute to the need for CSE to collect information using different methods
depending on the manner in which the communications [REDACTED] To collect
[REDACTED]

[REDACTED]
[REDACTED] it has done so under its foreign
intelligence mandate and if the expected foreign intelligence was consistent with GC
intelligence priorities.

Conducting [REDACTED] Collection Activities: CSE [REDACTED] collection activities [REDACTED]

CSE collection activities [REDACTED] may be conducted [REDACTED]

[REDACTED] in order to assess its potential foreign intelligence value. [REDACTED]

Whether [REDACTED] CSE [REDACTED] selected communications data as it is [REDACTED]

CSE Selection Process: [REDACTED]

GII accessible to CSE, and given that this traffic contains [REDACTED]

[REDACTED] it is essential that CSE [REDACTED]

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

[REDACTED] Selection criteria enable CSE to filter out extraneous data and provide greater certainty that the communications that CSE extracts [REDACTED] for interception will be of foreign intelligence value to the GC. Upon selection, these communications are forwarded to a consolidated traffic repository

for further analysis and reporting.¹ Communications data [REDACTED]

[REDACTED] Data may [REDACTED]
depending on [REDACTED]

[REDACTED] activities require the automated analysis [REDACTED] of [REDACTED]
[REDACTED]² This [REDACTED] is essential because most [REDACTED]
[REDACTED] in order to facilitate effective [REDACTED] on the GII.
Packetization also renders a communication [REDACTED] and in this [REDACTED]
communications data [REDACTED] on the GII. Data must be [REDACTED]
[REDACTED] foreign, irrespective of [REDACTED] and [REDACTED] of
potential foreign intelligence interest. This automated analysis [REDACTED] occurs
during the [REDACTED] selection process described above.

CSE also uses its SIGINT [REDACTED] to detect foreign intelligence relating to
[REDACTED] activities, in accordance with GC
intelligence priorities. For instance, CSE [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. CSE reduces the risk of inadvertent interception of private communications through various measures, including network characterization analysis, metadata analysis, [REDACTED] selection criteria validation [REDACTED] and annual re-validation of selection criteria. However, because CSE cannot know in advance if a targeted foreign entity will communicate with persons in Canada, CSE may incidentally intercept a one-end

¹ The traffic repository is qualified as being 'consolidated' [REDACTED]
[REDACTED]

Canadian communication originating or terminating with a foreign entity of intelligence interest.

Despite CSE's best efforts to prevent the interception of communications that both originate and terminate in Canada as described in the above selection process³, two-end Canadian communications may be inadvertently forwarded to the consolidated traffic repository. When subsequently recognized as such by an intelligence analyst, these will be marked for deletion and not used further by CSE. Associated selection criteria will be removed from collection [REDACTED] or refined (augmented) as appropriate, to prevent further collection of two-end Canadian communications.

As a result, CSE requires a Ministerial Authorization to undertake [REDACTED] collection 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 [REDACTED] is an essential source of foreign intelligence produced by CSE [REDACTED]. From December 2013 to May 2014, [REDACTED] collection was the [REDACTED]⁴ Canadian intelligence source for CSE-produced intelligence reports, which covered high intelligence priorities such as

Cabinet Confidence

Cabinet Confidence

In accordance with partnership arrangements, CSE receives requests from its Five Eyes partners to target specific selection criteria [REDACTED]. Once these requests have been validated, and determined to be in-line with GC intelligence priorities, CSE may agree to target Five Eyes selection criteria. More than [REDACTED] percent of the reports generated by CSE's Five Eyes partners that were attributed to Canadian signals intelligence collection were based on CSE [REDACTED] collection.

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.

³ It is not always possible for CSE to know ahead of time that a foreign entity outside Canada has travelled to Canada, and there is a risk that CSE may acquire two-end Canadian communications in that context.

⁴ [REDACTED] program yielded the [REDACTED] share of foreign intelligence produced by CSE for the same period.

In order to demonstrate in advance of conducting [REDACTED] collection 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. 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,⁵ to identify a foreign intelligence priority and to draft a justification to outline the expected value of a collection activity, prior to initiating any selection activities. Selection criteria are subject to validation, [REDACTED] to retrieve communications only when CSE is satisfied that the criteria relate to a foreign target and the external features of a communication.⁶

The use of selection criteria to identify communications for intercept provides CSE with a reasonably reliable means of assessing the foreign nationality, foreign location and intelligence interest of one of the communicants before a communication is retrieved. CSE allows Five Eyes partners to target foreign entities [REDACTED] provided that they abide by the above legal and policy requirements set out in the *NDA* and CSE's policy framework. This means that any selection criteria proposed by a Five Eyes partner for [REDACTED] must be validated by CSE as being directed at foreign entities outside Canada, and in line with GC intelligence priorities.

2. 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. Further, in most cases, information from the GII is the only potential source for the intelligence being sought by the GC, and may only be visible on [REDACTED]

3. The expected value of the interception would justify it

Activities conducted under this Ministerial Authorization provide CSE with unique access to the communications of targeted foreign entities and are an important source

⁵ A foreign assessment must include an assessment of the nationality and location of an entity of foreign intelligence interest.

⁶ Traditionally, external features have referred to information that meets the definition of 'metadata' as outlined in the MD on the Collection and Use of Metadata (2011).

of information about these entities and their activities, intentions and capabilities. CSE's [REDACTED] collection program continues to be a valuable source of foreign intelligence in accordance with GC intelligence priorities. Incidentally acquired private communications from CSE's [REDACTED] collection activities may provide unique foreign intelligence that meets GC priorities and assists Government decision-making.

In addition, CSE's [REDACTED] collection programs also provide CSE with access to foreign intelligence [REDACTED] which would otherwise be unavailable to CSE. This Five Eyes sharing regime is a valuable source of intelligence to the GC. CSE was able to produce approximately [REDACTED] per cent [REDACTED] foreign intelligence reports as a result of intelligence from Five Eyes [REDACTED]
[REDACTED]

After the expiration of the current Ministerial Authorization, 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;
- Accountability Framework Ministerial Directive;
- Privacy of Canadians Ministerial Directive; and,
- Collection and Use of Metadata 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] collection 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