



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

TOP SECRET//SI
Canadian Eyes Only

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

OCT 26 2011

CERRID# 781935

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

Interception Activities [REDACTED]

(For Approval)

PROPOSED MINISTERIAL AUTHORIZATION

The Communications Security Establishment (CSE) requests a Ministerial Authorization pursuant to subsection 273.65(1) of the *National Defence Act*.

ACTIVITY OR CLASS OF ACTIVITIES TO BE AUTHORIZED

For the sole purpose of obtaining foreign intelligence and subject to the conditions listed below, subsection 273.65(1) of the *National Defence Act* allows you to authorize CSE, in writing, to intercept private communications in relation to an activity or class of activities specified in the Ministerial Authorization.

Under this authority, CSE hereby requests a Ministerial Authorization to intercept private communications when conducting a class of collection activities [REDACTED]

[REDACTED] This class of collection activities uses a selection of information-gathering methods, each of which targets a particular kind of communication technology. This class of collection activities is referred to in Canada under the covername [REDACTED]

All CSE foreign intelligence collection activities are conducted under paragraph 273.64(1)(a) of the *National Defence Act*. These activities are in accordance with Government of Canada Intelligence Priorities. The Intelligence Priorities are issued to CSE annually through Ministerial Directive and are the foundation of CSE's National SIGINT Priorities List (NSPL). For 2011-2012, the NSPL sets-out the following categories: **Cabinet Confidence**

Cabinet Confidence


Cabinet Confidence

The NSPL categories are necessarily flexible to accommodate unforeseen developments, but always remain consistent with the Government of Canada intelligence priorities.

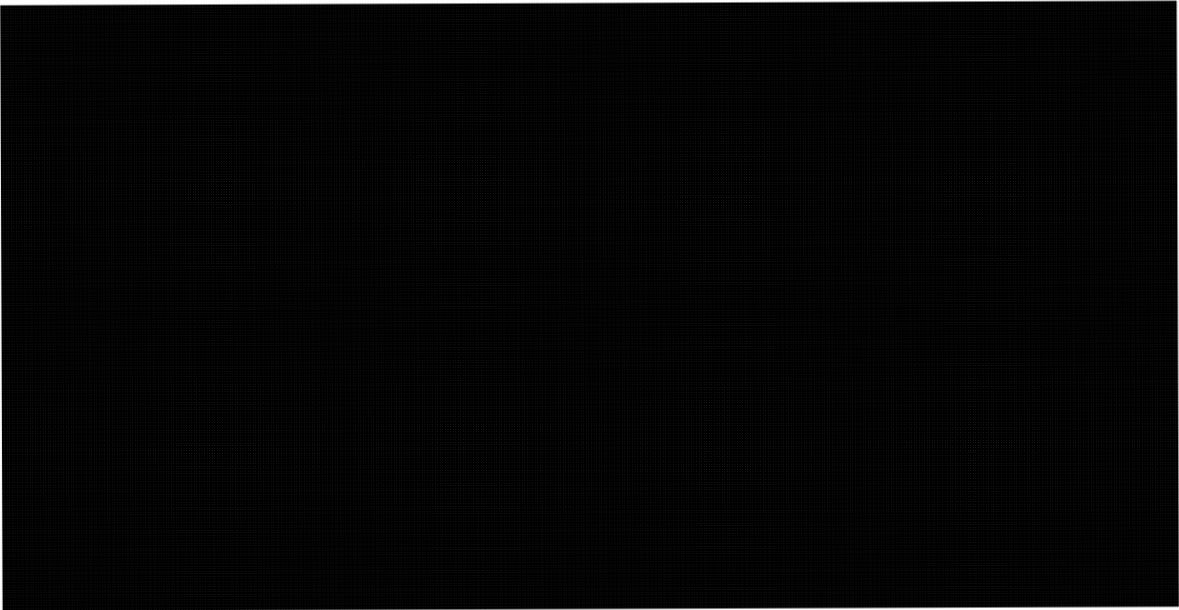
Canada

TOP SECRET//SI
Canadian Eyes Only

Among the foreign intelligence collection activities authorized under paragraph 273.64(1)(a) of the *National Defence Act* are collection activities called [REDACTED]



CSE is also working to modernize and enhance its [REDACTED] thereby positioning the organization to respond more rapidly to emergency situations abroad, such as kidnappings.



Determining the possible foreign intelligence value of information acquired through [REDACTED] activities and identifying cyber threats takes place following the application of such technical methods as are required to render the communications amenable to selection and analysis.

CSE's [REDACTED] activities may result in the interception of communications that either terminate or originate in Canada and in which the originator has a reasonable expectation of privacy, which constitute private communications pursuant to the *National Defence Act*. A Ministerial Authorization is therefore necessary to allow CSE to intercept private communications in the conduct of its [REDACTED] activities.

For your information, CSE also acquires telecommunication-related information used to identify, describe, manage or route all or part of the telecommunication, information referred to as "metadata", to gain a better understanding of the global information infrastructure and identify new targets. This activity, also authorized under paragraph 273.64(1)(a) of the *National Defence Act*, does not require a Ministerial Authorization and is conducted in accordance with the 2005 Ministerial Directive on the "Collection and Use of Metadata".

CONDITIONS TO BE SATISFIED

Under subsection 273.65(2) of the *National Defence Act*, you must be satisfied that:

- 1) the interception will be directed at foreign entities located outside Canada;
- 2) the information to be obtained could not reasonably be 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.

The standard used by CSE for each of the conditions listed in 273.65(2) is a reasonableness standard that takes into account the specific and particular context of signals intelligence activities. These requirements are met respectively as follows:

- 1) CSE follows a very strict set of procedures to reasonably assure itself that collection activities that risk the interception of private communications are directed at foreign entities located outside Canada. CSE has established and maintains an automated directory of selectors (such as telephone numbers, internet protocol addresses or e-mail addresses) used for intercepting the communications of targets of interest.


These selectors represent the identifying and routing metadata [REDACTED]


This metadata provides CSE with a reasonably reliable way to identify who one of the communicants is likely to be, and whether he or she is located outside Canada.

These selectors are obtained from a number of sources, including but not limited to: open source information, analysis of previously acquired signals intelligence and information provided by various departments and agencies of the Government of Canada, as well as allied agencies.

In accordance with procedures in place, prior to any targeting and before collection systems are tasked to collect communications, CSE personnel must be satisfied, based on all the information that CSE has available to it at the time, that the proposed selectors are associated with a foreign entity located outside Canada and relate to a Government of Canada intelligence priority (as most recently outlined in **Cabinet Confidence** and the associated Ministerial Directive). In addition, selectors must meet the definition of the term 'metadata' in the Ministerial Directive entitled "Collection and Use of Metadata".

Consequently, a selector can only be used to intercept communications where CSE is satisfied that it is foreign and relates to the external component of communications. The content of communications is not scanned until CSE has reasonable assurance that such communications have at least one end located outside Canada. The use of selectors allows CSE to elevate the level of certainty that communications having no foreign intelligence value will not be intercepted. In the unlikely event that communications having both ends in Canada are intercepted, CSE will, upon recognition, take necessary steps to delete them from its databases.

Regarding CSE's cyber threat detection activities, CSE proposes, because of the very specific nature of hostile cyber activities, 



- 2) The information CSE is seeking to obtain could not reasonably be obtained by means other than interception because:
- information derived from the communications acquired by CSE, including information from any private communications that are intercepted, would not be shared voluntarily by the targeted foreign entities; and
 - the communications acquired by CSE, including those private communications that are intercepted, will in most cases be the only potential source for the information.
- 3) In its totality, the expected foreign intelligence value of the information to be derived from the interception justifies it. The foreign intelligence value of these interceptions can be accurately judged in the context of the foreign intelligence derived from the [REDACTED] program, in its entirety.

Overall, interception activities conducted under this program [REDACTED]

[REDACTED] enhancing CSE's capacity to understand and locate targets of interest and providing foreign intelligence in accordance with Government of Canada intelligence priorities. Between the commencement of the current Ministerial Authorization on December 1, 2010 and May 31, 2011 CSE [REDACTED] issue any intelligence reports based on [REDACTED] collection. [REDACTED] CSE's allies from the US National Security Agency and UK Government Communications Headquarters produced [REDACTED] reports, shared with Canada, with information derived from collection [REDACTED]

For your information, between the commencement of the current Ministerial Authorization on December 1, 2010 and May 31, 2011, [REDACTED] communications were intercepted under the [REDACTED] program, [REDACTED] of which were recognized as a "private communication." [REDACTED] solicitor-client communications were recognized.

After the expiration of the current Ministerial Authorization, CSE will report to you on the full period of that authorization in accordance with the reporting requirements listed therein.

- 4) Measures developed by CSE, in the form of operational policies and procedures, are in place and provide direction to CSE in protecting the privacy of Canadians and ensuring that private communications will only be used or retained if they are essential to international affairs, defence or security. Essentiality is defined as containing information that is clearly related to the intelligence priorities of the Government of Canada.

CSE policies relating to accountability, the privacy of Canadians and the operation of this program are currently found in the following CSE documents:

- the Ministerial Directives entitled "Accountability Framework" (2001), "Privacy of Canadians" (2001) and "Collection and Use of Metadata" (2005); and
- the operational procedures entitled OPS-1: "Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities" and OPS-1-13: "Procedures for Canadian [REDACTED] and Joint CSEC-CF Activities".

CSE employees will only conduct these activities according to the operational policies and procedures in effect. Should revisions to operational policies and procedures result in an increased risk to the privacy of Canadians, or a reduction of measures to protect the privacy of Canadians, CSE will advise you. For your ease of reference, we have attached to this package the foundational policy (OPS-1) that establishes baseline measures to protect the privacy of Canadians and to ensure the legal compliance of CSE operational activities. All other operational policies and procedures must comply with this policy.


CSE employees involved in collection activities [REDACTED] and the processing and analysis of information obtained as a result of these activities, are trained in these measures and are fully aware of their responsibilities in implementing them. The application of these measures is monitored by CSE management and reviewed by the CSE Commissioner.

In accordance with the *National Defence Act*, you must be satisfied that the conditions set forth in subsection 273.65(2) have been met prior to issuing the attached Ministerial Authorization.

Solicitor-Client Privilege

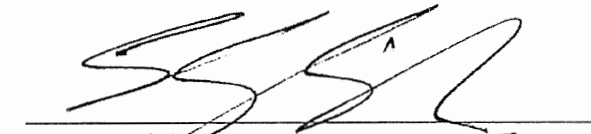
RECOMMENDATION

It is recommended that you approve the attached Ministerial Authorization "Interception Activities [REDACTED] to be effective December 1, 2011 to November 30, 2012.


John Adams
Chief

Attachment

I concur with the recommendation:


Stephen Rigby
National Security Advisor to the Prime Minister
Privy Council Office

cc: Robert Fonberg, Deputy Minister, National Defence