



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

SECRET//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

NOV 26 2013

CERRID# 1328092

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

CSE Cyber Defence 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(3) 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 protecting the computer systems and networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*.

You may issue a Ministerial Authorization provided the legislated conditions are met. Ministerial Authorizations are essential to the successful implementation of CSE's information protection mandate; without them, the organization would be unable to detect known threats and vulnerabilities; discover unknown threats and vulnerabilities; and protect Government of Canada computer systems and networks from them.

The purpose of this Memorandum is to request a Ministerial Authorization for CSE's cyber defence activities on Government of Canada computer systems and networks that risk interception of private communications.

Prior to commencing cyber defence activities pursuant to a Ministerial Authorization, CSE obtains the consent of the federal institution to be present on their networks.

CLASS OF ACTIVITIES TO BE AUTHORIZED: CYBER DEFENCE ACTIVITIES

The Cyber Threat Environment: CSE and its closest cryptologic partners in the United States, the United Kingdom, Australia and New Zealand monitor malicious cyber activity. This malicious activity is sustained, highly sophisticated and often hidden in normal or legitimate internet traffic where it is difficult for users and network administrators to detect.

Canada

SECRET//CEO

In 2012, CSE detected [REDACTED] cyber threat incidents on computers systems and networks of significance to the Government of Canada. International Affairs, Trade and Development was the most heavily targeted sector which accounted for [REDACTED] percent of incidents detected. This includes [REDACTED] instances of attempted compromises of Government of Canada systems. There were [REDACTED] compromises, and [REDACTED] instances where threat actors successfully exfiltrated information. [REDACTED] is assessed to be responsible for [REDACTED] percent of all incidents detected. In comparison, [REDACTED] together accounted for [REDACTED] percent of detected threat incidents. The remaining [REDACTED] percent of incidents could not be attributed; however, based on the type of information targeted in the incidents, [REDACTED] is likely the responsible actor.

The most prevalent technique employed by cyber threat actors over the past year was spear-phishing [REDACTED]. In these cases, threat actors used legitimate-looking emails that were crafted to appear relevant to the recipient. These tailored emails contained malicious attachments, or seemingly legitimate links to malicious web sites.

CSE Cyber Defence Activities: While federal institutions have commercially-available means to detect malicious activities directed against their networks, these capabilities are insufficient to counter the growing threats to the Government of Canada's cyber security. By collaborating with CSE's foreign intelligence collection program, CSE's cyber defence program is able to better defend against these threats. This collaboration allows for the sharing of cyber defence-related expertise, tools and data from foreign cyber threat activity, providing a comprehensive picture of foreign cyber threats directed at Government of Canada computer systems and networks. CSE also draws upon the [REDACTED] cyber defence programs [REDACTED] to provide information concerning sophisticated foreign threats and threat actors.

Network Detection

During cyber defence activities conducted under a Ministerial Authorization, a federal institution provides CSE with [REDACTED]. Data from each federal institution is [REDACTED] and retained for a period of up to [REDACTED] (a current list of existing and newly-established federal clients is provided at Annex A). This retention period [REDACTED]

[REDACTED]

Interception of Private Communications: CSE cyber defence activities are conducted on Government of Canada computer systems and networks, and all communications transmitted on those systems and networks between two or more persons are private communications for the purposes of the NDA. Upon detection by [REDACTED] suspect communications may be extracted from the [REDACTED] data for further analysis by CSE cyber defence personnel. Communications that have been extracted from the [REDACTED] by CSE have been intercepted by CSE. Should [REDACTED]

CONDITIONS TO BE SATISFIED

You may issue a Ministerial Authorization only if you are satisfied that CSE has met the five conditions set out in subsection 273.65(4) of the NDA and is appropriately managing the risk of intercepting private communications.

- the interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks;
- the information to be obtained could not reasonably be obtained by other means;
- the consent of persons whose private communications may be intercepted cannot reasonably be obtained;
- 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,
- satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.

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 is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks*

Malicious activity directed against Government of Canada computer systems and networks is often disguised as normal or legitimate files, computer processes or network traffic. In order to identify, isolate and mitigate cyber threats, it is likely that CSE will intercept private communications in the course of monitoring, acquiring and analyzing traffic on computer systems or networks of federal institutions.

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

It is impossible to effectively identify and prevent potential cyber threats from harming Government of Canada computer systems or networks without acquiring and analyzing a copy of suspicious files, computer processes or network traffic. Some of the traffic that will be acquired and copied will consist of private communications, and therefore the necessary information could not reasonably be obtained by means that do not risk the interception of private communications.

3. *The consent of the persons whose private communications may be intercepted cannot reasonably be obtained*

While CSE has obtained the consent of the requesting federal institution, it is impossible to obtain the consent of all persons outside the federal institution network who may legitimately communicate with internal users. Furthermore, obtaining this advance consent may alert malicious actors to CSE's presence on a particular network, thereby enabling them to evade detection.

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*

All information obtained by CSE from a federal institution's network or system during cyber defence activities is used or retained in accordance with OPS-1-14, "Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization," and related documentation. The NDA and OPS-1-14 require the application of an essentiality test to determine whether information from a private communication that is intercepted in the conduct of authorized cyber defence activities is essential to identify, isolate, or prevent harm to Government of Canada computer systems or networks. Only information that is deemed essential may be used or retained by CSE; otherwise it is automatically deleted on or before the 12 month anniversary of the date it was copied.

5. Satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information

CSE may use or retain information for the purpose of furthering its investigation into cyber threat activities on Government of Canada systems or networks. This use or retention includes sharing it within CSE or with domestic and international partners.

Any information sharing will be done in strict accordance with CSE-approved operational policy. The sharing of information from private communications will only be undertaken if it is essential to protect Government of Canada computer systems or networks. Data in the [REDACTED] remains under the control of the federal institution from which it originated. Communications that have been intercepted and used or retained by CSE are no longer under the control of the federal institution [REDACTED]
[REDACTED]

CSE's policies relating to accountability, the privacy of Canadians and the conduct of cyber defence activities are outlined in the following Ministerial Directives and operational policies:

- Accountability Framework Ministerial Directive;
- Privacy of Canadians Ministerial Directive;
- OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities; and
- OPS-1-14: Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization.


CSE employees must conduct activities in accordance with the most current version of these Ministerial Directives and operational policies. CSE 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 privacy of Canadians and all other operational policies must comply with it. A copy of OPS-1 is attached for your reference at Annex B.

The use and retention of intercepted private communications that contain information essential to identify, isolate or prevent harm to Government of Canada computer systems and networks 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 policy instruments that enable CSE to fulfill its mandate without risk of criminal liability for the incidental interception of private communications. This Ministerial Authorization will enable CSE to continue its cyber defence activities, which protect the computer systems and networks of the Government of Canada. It is recommended that you approve the attached Ministerial Authorization "Protection of Government of Canada Computer Systems and Networks: Communications Security Establishment Cyber Defence Activities," to be effective 1 December 2013 to 30 November 2014.




John Forster
Chief

Attachment

ANNEX A

- **Ongoing Cyber Defence Activities:** Under the current Ministerial Authorization, "Communications Security Establishment Cyber Defence Activities," effective December 1, 2012, CSE is engaged in ongoing cyber defence activities (that intercept private communications) in support of the computer systems and networks of the following federal institutions:
 - 1) Communications Security Establishment;
 - 2) Department of National Defence;
 - 3) Department of Foreign Affairs, Trade and Development; and
 - 4) Government of Canada Departments and Agencies using the Secure Channel Network (SC Net) that is administered by Shared Services Canada
- CSE intends to continue these cyber defence activities with these federal institutions under the 2013-2014 Ministerial Authorization.
- **New Agreements:** Prior to CSE engaging in any new cyber defence activities with new clients within the one-year period covered by this Ministerial Authorization, CSE shall inform you and provide an updated copy of this Annex.

- 
- On 14 November, 2013, CSE received a letter of request from Shared Services Canada on which it intends to act.

- All cyber defence activities carried out on the systems and networks of Government of Canada departments are conducted under the strict supervision of CSE personnel in cooperation with the requesting federal institution's staff, and in accordance with established policies and procedures.