Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

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

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

CERRID# 12183490

NOV 18 2014

# MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

## CSE Cyber Defence Activities

(For Approval)

## ISSUE

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

The Communications Security Establishment's (CSE) mandate to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada (GC) authorizes it, within a rigorous assessment and approval framework, to conduct cyber defence activities. These activities include informing and helping protect the GC from sophisticated cyber threats; and providing cryptographic products and services that protect the GC's most sensitive information.

You may issue a Ministerial Authorization enabling cyber defence activities provided the conditions are met under subsection 273.65(4) of the *National Defence Act* (*NDA*). Ministerial Authorizations are essential to the successful implementation of the CSE information protection mandate; without them, the organization would be unable to detect known threats and vulnerabilities; discover unknown threats and vulnerabilities; and protect GC computer systems and networks from them.

Although CSE cannot target Canadians or persons in Canada, the incidental interception of private communications is unavoidable when conducting cyber defence activities. Pursuant to a Ministerial Authorization, CSE conducts cyber defence activities in accordance with the *NDA* and upon request by federal institutions.

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 *NDA*, you authorize 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 GC from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*.

## CLASS OF ACTIVITIES TO BE AUTHORIZED: CYBER DEFENCE ACTIVITIES

**Cyber Defence Activities:** CSE and its closest cryptologic partners in the United States, the United Kingdom, Australia and New Zealand monitor malicious cyber activity and share cyber threat information. This malicious activity is sustained, highly sophisticated and often [redacted] normal or legitimate internet traffic where it is difficult for users and network administrators to detect. Cyber threat vectors are constantly changing [redacted] CSE is able to defend against these cyber threats by having [redacted] to GC systems and networks. CSE tracks and defends against threat vectors of which it is already aware, and works to detect and catalogue the new threat vectors that attack the GC.

**Rationale for 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 GC'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 cyber threat activity, and providing a more comprehensive picture of cyber threats directed at GC computer systems and networks. CSE also collaborates with the foreign (cyber) intelligence collection and cyber defence programs of its allies to exchange information concerning sophisticated threats and threat actors.

**Conducting Cyber Defence Activities:** From 1 December 2013 – 1 July 2014, CSE detected [redacted] compromises on computers systems and networks of significance to the GC. This includes compromises by both state-sponsored and cybercrime actors. Overall, there were [redacted] incidents attributed to state-sponsored actors including [redacted] attempted compromises and [redacted] actual compromises. Of these [redacted] state-sponsored compromises, [redacted] were identified as being involved with the exfiltration of data from GC systems.

[redacted] is assessed to be responsible for [redacted] percent of state-sponsored incidents detected. [redacted] together accounted for [redacted] percent of detected threat incidents. The remaining [redacted] percent of incidents could not be attributed. Overall, [redacted] was the most targeted sector by state-sponsored actors, due to a [redacted] state-sponsored actor that targeted a department within this sector.

The most prevalent known 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.

[redacted] During cyber defence activities conducted under a Ministerial Authorization, a federal institution provides CSE with [redacted] This [redacted] traffic is [redacted] and retained for a maximum period of [redacted], if required. This retention period [redacted]

[redacted]

CSE cyber defence activities may also include selecting data from the [redacted] or from [redacted] for the purpose of identifying, isolating or preventing harm to GC systems and networks, for cyber capability development, and for establishing an activity baseline

(to determine what is normal activity) and to inform [redacted] detection activities.

**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. Regarding cyber defence activities, CSE only retains private communications that are essential to the protection of electronic information and information infrastructures of importance to the GC. Therefore, CSE does not retain all private communications that it intercepts.

CSE cyber defence activities are conducted on GC computer systems and networks, and communications transmitted on those systems and networks between two or more persons are normally private communications for the purposes of the *NDA*. Upon detection by [redacted] communications suspected of being malicious may be extracted from the [redacted] for further analysis by CSE cyber defence personnel. Communications that have been extracted from the [redacted] have been intercepted by CSE. However, CSE only accounts for those private communications that it uses and retains, as not all suspect communications are found to be malicious.

## CONDITIONS TO BE SATISFIED

You may issue a Ministerial Authorization only if you are satisfied that CSE has met the following five conditions set out in subsection 273.65(4) of the *NDA*:

- the interception is necessary to identify, isolate or prevent harm to GC 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 GC 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 of conducing cyber defence 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 is necessary to identify, isolate or prevent harm to GC computer systems or networks***

Malicious activity directed at GC 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 could not be reasonably obtained by other means***

It is impossible to effectively identify and prevent potential cyber threats from harming GC computer systems or networks without acquiring and analyzing a copy of suspicious files, computer processes or network traffic. Email is a common threat vector, and emails containing malicious code are often socially engineered so that it is not obvious to the recipient that it is not a legitimate email. 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***

In response to a department's request for assistance CSE obtains consent to engage in cyber defence activities from the federal institution responsible for the computer systems and networks being protected. It is impossible to obtain in advance the consent of all parties to a private communication that is intercepted as an incident of cyber defence activities. 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 GC 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 handled in accordance with relevant CSE operational policy. The *NDA* and CSE relevant operational policy specify 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 GC 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 [redacted] of the date it was copied. A private communication is considered to be essential when it has the potential to make an indispensable and fundamental contribution to the understanding of malicious cyber activity including [redacted] capabilities or intentions, for the purpose of mitigating that activity.

### *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 GC 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. Systems owners may, at any time, request that all data that CSE has not retained be deleted.

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 the associated operational policies:

- 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.

CSE cyber defence activities differ from those activities authorized under the [redacted] Collection, [redacted] Collection, and [redacted] Ministerial Authorizations. As cyber threat vectors [redacted] when conducting activities under the cyber defence activities Ministerial Authorization, CSE may examine the data surrounding a private communication but rarely examines the actual correspondence contained within the communication. Under Canadian law, the solicitor-client privilege must be protected. Because the meaning of a private communication is rarely reviewed, CSE has not recognized any privileged solicitor-client communications in the course of cyber defence activities; however, in the rare circumstances in which CSE recognizes that a solicitor-client communication has been intercepted, that communication will be treated in the manner set out in the conditions in the Ministerial Authorization.

The use and retention of intercepted private communications that contain information essential to identify, isolate, or prevent harm to GC 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.

## 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 cyber defence activities, which protect the computer systems and networks of the GC. It is recommended that you approve the attached Ministerial Authorization "Communications Security Establishment Cyber Defence Activities," to be effective 1 December 2014 to 30 November 2015.

John Forster
Chief

Attachment

## ANNEX A

**Ongoing Cyber Defence Activities:** Under the current Ministerial Authorization, "Communications Security Establishment Cyber Defence Activities," effective December 1, 2013, 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
4) [redacted]
5)
6) Canadian Nuclear Safety Commission;
7) [redacted]
8)
9) Natural Resources Canada; and,
10) GC 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 2014-2015 Ministerial Authorization.

**New Agreements:** CSE shall inform you of any new cyber defence activities with new clients within the one-year period covered by this Ministerial Authorization

- Within the past year, CSE has informed you of [redacted] CSE's cyber defence services:

[redacted]

- All cyber defence activities carried out on the systems and networks of GC 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.