Memorandum of Understanding between Communications Security Establishment (CSE) and Shared Services Canada (SSC)

PART I – BACKGROUND

SSC has requested in writing that CSE conduct cyber defence activities to help protect computer systems and networks under the control and supervision of SSC;

CSE has the legislative 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;

The *Financial Administration Act* authorizes SSC to take reasonable measures to manage or protect the computer systems and networks under its control and supervision;

A Ministerial Authorization issued pursuant to the *National Defence Act* (NDA) authorizes CSE to conduct cyber defence activities that may involve the interception of private communications, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference.

PART II – CYBER DEFENCE ACTIVITIES TERMS AND CONDITIONS

CSE and SSC agree as follows:

1. Purpose

   The purpose of this MoU is to set out the terms and conditions under which CSE's cyber defence activities will be conducted. Subject to operational capacity, the Parties will provide the support necessary to carry out cyber defence activities. CSE's cyber defence activities supplement SSC's user baseline security requirements and responsibilities.

2. Roles and Responsibilities

   SSC will:

   - Provide management personnel to assist in fulfilling the terms and conditions of this MoU.

CERRID #9928631

- Provide technical personnel both to respond to queries and action mitigation recommendations from CSE.

- Provide the necessary information required by CSE to set up and activate cyber defence activities, to ensure that CSE conducts services only on computer systems and networks under the control and supervision of SSC.

- Ensure that CSE is kept apprised of the nature and extent of SSC authorities and any changes that are made to those authorities, as they happen.

- Notify CSE of any changes to any system or network under the control and supervision of SSC that may impact upon CSE's cyber defence activities, such as providing timely notification of changes to Internet Protocol (IP) allocations.

- Ensure that SSC clients have been informed that CSE may acquire their data, including personal information and/or private communications, while conducting cyber defence activities for SSC.

- Facilitate CSE's interactions with SSC's vendors or suppliers as necessary.

CSE will:

- Perform cyber defence activities to protect SSC's computer systems and networks from mischief, unauthorized use or interference.

- Test tools prior to deploying them on SSC computer systems and networks.

- Provide details prior to initial tool or service deployment on any of SSC's computer systems or networks. Details will include

    - operational engagement processes and procedures,

    - possible risks of deploying a tool or service, and

    - technical information and parameters of tools or services (to allow SSC to assess potential impacts).

- Inform SSC of any significant changes to deployed tools or services that may affect the level of risk.

- Investigate possible undue effects of cyber defence tools that are reported by SSC.

- Keep SSC informed when engaging with SSC clients on deployment of cyber defence tools on assets under client authority, if these assets connect or may connect to SSC owned systems or networks.

3. Risk Acceptance

CSE and SSC recognize that while cyber defence activities enhance and contribute to the defence of SSC systems, certain inherent risks accompany any level of activity. Any potential risks associated with tools or services will be brought to the attention of SSC prior to deployment.

4. Fees and Expenses

Each Party will be responsible for its own fees and expenses during the conduct of cyber defence activities.

5. External Review

CSE activities are subject to review by the CSE Commissioner, the Information Commissioner, the Privacy Commissioner, the Auditor General and any other body established by Parliament for review purposes. Interviews or documentation may be requested as part of a review; CSE and SSC will cooperate fully with any such requests.

6. Control of Data

Cyber defence data obtained by CSE from SSC during cyber defence activities will be considered to be under the control of CSE only if it is identified as being relevant to CSE's mandate as stated in the NDA paragraph 273.64(1) (b). Further, data from SSC which contains private communications will be deemed under the control of CSE where it is found to be essential to use and retain for the purpose of identifying, isolating or preventing harm to GC computer systems or networks (as required by paragraph 273.65(4) (d) of the NDA). Any data not deemed to be relevant or essential will be deleted in accordance with CSE's policy.

CSE may share data that has come under its control (as described above) with domestic and international partners involved in cyber security (both public and private sectors), for the purpose of understanding and mitigating threats.

7. Data and Information Handling

(1) SSC will ensure that any **classified or protected information** provided to CSE in order to support cyber defence activities (for example, network diagrams) is clearly and appropriately marked.

(2) SSC will inform CSE of clients that may have an increased level of sensitivity regarding their data. CSE will handle such data accordingly.

(3) CSE's Classified or Protected Information

a. CSE will ensure that any classified or protected information disclosed to SSC pursuant to this MoU is clearly and appropriately marked as such. SSC will handle such information in accordance with departmental security standards and handling instructions from CSE.

b. All cyber defence data obtained from SSC that has not come under the control of CSE will be considered PROTECTED B, unless marked otherwise.

Application of CSE's policies will limit and control access to cyber defence data obtained from SSC and to other information obtained by CSE from, or about, SSC during cyber defence activities. Cyber defence data will be stored for up to a maximum of [redacted] from the date it is copied; this does not include data that has come under the control of CSE.

8. Personal Information and Privacy of Canadians

CSE will handle personal information under its control in accordance with the Privacy Act. As required by paragraph 273.64(2)(b) of the NDA and established in CSE policies, CSE will have measures in place to protect the privacy of Canadians.

9. Interception of Private Communications

It is understood that for CSE to conduct cyber defence activities which may involve the interception of private communications, CSE requires a Ministerial Authorization from the Minister of National Defence, pursuant to subsection 273.65 (3) of the NDA. CSE will only intercept private communications for the sole purpose of protecting the Government of Canada's computer systems or networks from mischief, unauthorized use or interference.

If at any point during the term of this MoU no applicable MA is in force, CSE will inform SSC of the fact, and will cease cyber defence activities that may intercept private communications until such time as a new MA is in place.

SSC can at any time suspend cyber defence activities by contacting CSE, or by terminating the flow of copied network traffic on the communications link between SSC and CSE.

10. Information Indicating Criminal Activity

In the unlikely event that any member of CSE encounters indications of a *Criminal Code* offence (unrelated to a cyber threat) on the computer systems or networks of SSC, the incident and the data will be brought to the attention of SSC management. If SSC attempts to locate this data on their networks and systems, and is unable to find it, CSE can provide it to SSC if the data is available. SSC shall have responsibility with respect to follow-on action and notification of the appropriate authorities.

11. Term of this MoU

This MoU comes into effect on the day it is signed by the Parties and will remain in effect until either Party rescinds this agreement in writing.

This MoU may be modified at any time with the written consent of both Parties (those signing this MoU, their successors, or equivalents).

Either Party may terminate or suspend services at any time, upon providing signed, written notice.

Within [redacted] of the termination of this MoU, CSE will provide notice in writing that all data in the SSC repository has been destroyed in accordance with CSE policy.

Such notice may be delivered by hand, by regular mail, by email, or by courier. A notice shall be deemed to have been received on the day of its delivery if delivered by hand, on the fifth (5^{th}) business day after mailing if sent by regular mail, and on the date of delivery if sent by courier or email.

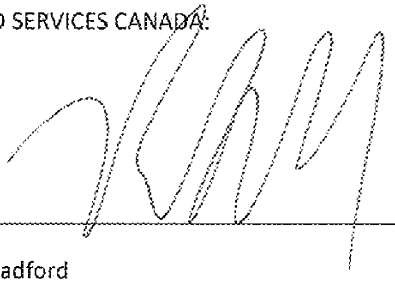
For the COMMUNICATIONS SECURITY ESTABLISHMENT:

24 March 2014

Toni Moffa
Deputy Chief
IT Security
Communications Security Establishment

Date

For SHARED SERVICES CANADA:



MAR 2 7 2014

Kevin Radford
Senior Assistant Deputy Minister
Operations
Shared Services Canada

Date

CERRID #9928631