

**Memorandum of Understanding
between Communications Security Establishment (CSE) IT Security and CSE-CIO**

PART I – BACKGROUND

CSE-CIO has requested in writing that CSE-ITS conduct cyber defence operations to help protect CSE-CIO's information, computer systems and networks;

CSE-ITS has the legislative mandate, *inter alia*, 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 pursuant to paragraph 273.64(1)(b) of the *National Defence Act* (NDA) (Part (b) of CSE-ITS's Mandate);

CSE-CIO is authorized by section 161 of the *Financial Administration Act* to take reasonable measures to manage or protect CSE-CIO information, computer systems and networks;

CSE-CIO has, pursuant to paragraph 8(2) (b) of the *Privacy Act*, the authority to disclose to CSE-ITS personal information and hereby authorizes CSE-ITS to collect such information solely for the purposes mentioned in and under the conditions provided in this MoU; and

The Cyber Defence Operations Ministerial Authorization (MA) has been issued to CSE-ITS per subsection 273.65(3) of the *National Defence Act*.

PART II – CYBER DEFENCE OPERATIONS TERMS AND CONDITIONS

Therefore, the Parties agree as follows:

1. **Purpose**

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

2. **Cyber defence operations conducted under Ministerial Authorization (MA)**

Cyber defence operations are conducted under an MA for the sole purpose of protecting information, computer systems and networks, and providing advice, guidance and services to CSE-CIOs in order to prevent, predict and respond to cyber threats.

A description of the cyber defence operations will be provided in a separate concept of operations document.

The authority signing this MoU on behalf of CSE-CIO delegates signing authority for concept of operations to any person occupying the position of Director Information Security at CSE-CIO.

3. **Roles and Responsibilities**

CSE-CIO will:

- Provide management personnel to assist in fulfilling the terms and conditions of this MoU.
- Provide technical personnel to respond to queries and to action mitigation recommendations from CSE-ITS.

CONFIDENTIAL

- Provide all the necessary information required by CSE-ITS to set up and activate the cyber defence operations, ensuring that CSE-ITS staff conducts the service only on computer systems and networks for which CSE-CIO is the owner or authorized user.
- Ensure that any required authorities or permissions are obtained prior to the commencement of cyber defence operations.

In order to protect classified sources, methods or techniques, CSE-CIO will not take any action on the basis of cyber defence reports, other than following mitigation advice provided in the report. CSE-ITS will provide all caveats and handling instructions related to mitigation advice included in a report or service.

CSE-ITS will:

- Perform computer and network monitoring and related analysis, and will provide mitigation services.
- Be responsible for deploying cyber defence systems and ensuring those systems function as intended.
- Maintain and monitor the system and adapts its architecture during operations based on networks changes or cyber defence capabilities.
- Consult with CSE-ITS's Directorate of Legal Services (DLS), who will work together with CSE-CIO's legal department to resolve any legal matters.

5. Fees and Expenses

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

6. External Review

CSE-ITS activities are subject to review by the CSE-ITS Commissioner, the Information Commissioner, the Privacy Commissioner, and the Auditor General. Interviews or documentation may be requested as part of a review; the Parties will cooperate fully.

7. Control of Data

Cyber defence data obtained by CSE-ITS from CSE-CIO during cyber defence operations will be considered to be under the control of CSE-ITS only if it is identified as being relevant to CSE-ITS's mandate as stated in the NDA paragraph 273.64(1) (b), and in the case of private communications, 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).

CSE-ITS may share data that has come under CSE-ITS control (as described above) with other federal departments and agencies, as well as with counterpart organizations in the United States, United Kingdom, Australia and New Zealand.

8. Data and Information Handling

- (1) CSE-CIO will ensure that any **classified or protected information** provided to CSE-ITS in order to support cyber defence operations (for example network diagrams) are clearly marked as such.

Page 2 of 5

CERRID 1042571

CONFIDENTIAL

(2) CSE-ITS's Classified or Protected Information

- (a) CSE-ITS will ensure that any classified or protected information disclosed to CSE-CIO pursuant to this MoU is clearly and appropriately marked as such. CSE-CIO will handle such information in accordance with departmental security standards and handling instructions from CSE-ITS.
- (b) All cyber defence data obtained from CSE-CIO that has not come under the control of CSE-ITS will be PROTECTED B.
- (c) Access to cyber defence data obtained from CSE-CIO and other information obtained by CSE-ITS from or about CSE-CIO during cyber defence operations is limited and controlled according to CSE-ITS policies. CSE-CIO agrees that access by other persons within CSE-ITS may only be authorized by the Director General Cyber Defence at CSE-ITS.

9. Personal Information and Privacy of Canadians

CSE-ITS will handle personal information under its control in accordance with the Privacy Act.

As required by paragraph 273.64(2)(b) of the NDA, CSE-ITS will have measures in place to protect the privacy of Canadians, as established in CSE-ITS policies.

10. Interception of Private Communications

It is understood that for CSE-ITS to conduct cyber defence operations which may involve the interception of private communications, CSE-ITS requires an MA from the Minister of National Defence, pursuant to subsection 273.65 (3) of the NDA. CSE-ITS 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.

CSE-ITS may share data that has come under CSE-ITS control (as described above) with other federal departments and agencies, as well as with counterpart organizations in the United States, United Kingdom, Australia and New Zealand..

11. Data Retention

Retention duration of cyber defence data in the CSE-CIO repository will vary based on operational need and on technical capacity, as advised by CSE-ITS. All cyber defence data in the CSE-CIO repository will be stored for up to a maximum of [REDACTED] from the date it is copied (provided a Ministerial Authorization is in place, and this MoU remains in effect). This does not include data that is under the control of CSE-ITS.

12. CSE-CIO Cease Operation Capability

CSE-CIO can at any time suspend cyber defence operations by contacting CSE-ITS's Cyber Threat Evaluation Centre, or by terminating the flow of copied network traffic on the communications link between CSE-CIO and CSE-ITS.

13. Destruction of CSE-CIO's Data

Within [REDACTED] of the termination of this MoU (at the request of CSE-CIO (see paragraph 12), or at CSE-ITS's request), CSE-ITS will provide confirmation in writing that all data in the CSE-CIO repository has been destroyed in accordance with CSE-ITS policy.

14. Information Indicating Criminal Activity

In the unlikely event that any member of CSE-ITS encounters indications of a criminal code offence on the computer systems or networks of CSE-CIO, the incident and the data will be brought to the attention of

Page 3 of 5

CERRID 1042571

CONFIDENTIAL

CSE-CIO management. If CSE-CIO attempts to locate this data on their networks and systems, and is unable to find it, CSE-ITS can provide the data to CSE-CIO. CSE-CIO shall have sole responsibility with respect to follow-on action and notification of the appropriate authorities.

15. Term of this MoU

- (1) This MoU comes into effect on the day it is signed by the Parties and will remain in effect until either party rescinds this MoU.
- (2) The Parties to this MoU acknowledge that if at any point during the term of this MoU there is a period of time where no applicable MA is in force, during that period CSE-ITS will not carry out cyber defence operations that may intercept private communications. CSE-ITS will inform CSE-CIO if this situation occurs.
- (3) This MoU may be modified in writing at any time with the written consent of both Parties.
- (4) Either Party may terminate or suspend the services at any time upon providing appropriate notice.
- (5) Any notice to either Party hereunder must be in writing and signed by the Party giving it. Notices shall be addressed as follows:

[REDACTED]
Director, Cyber Threat Evaluation Centre

Communications Security Establishment
IT Security
1500 Bronson Avenue
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Fax Number: [REDACTED]

[REDACTED]
Director, Information Security

Communications Security Establishment
Chief Information Office
1929 Ogilvie Road
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Fax Number: (613) xxx-xxxx

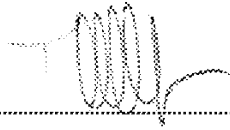
- (6) Such notice may be delivered by hand, by regular mail, by courier or by facsimile. A notice shall be deemed to have been received on the day of its delivery if delivered by hand, on the fifth (5th) business day after mailing if sent by regular mail, on the date of delivery if sent by courier and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

Page 4 of 5

CERRID 1042571

CONFIDENTIAL

For the COMMUNICATIONS SECURITY ESTABLISHMENT:

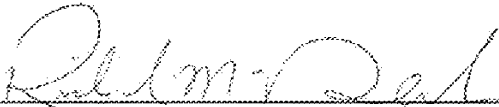


Toni Muffa
Deputy Chief
CSE-IT Security
Communications Security Establishment

14/9/12

Date

For the CSE-CIO



Richard McDonald
Chief Information Officer
CSE-CIO
Communications Security Establishment

Sept 14, 2012

Date