

CONFIDENTIAL

**Memorandum of Understanding
between Communications Security Establishment (CSE) and Department of Foreign Affairs and
International Trade (DFAIT)¹**

PART I – BACKGROUND

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

CSE 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's Mandate);

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

DFAIT has, pursuant to paragraph 8(2) (b) of the *Privacy Act*, the authority to disclose to CSE personal information and hereby authorizes CSE 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 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's cyber defence operations will be conducted. Subject to operational capacity, the Parties will provide support necessary to carry out cyber defence operations. CSE's cyber defence operations supplement DFAIT'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 clients 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 DFAIT delegates signing authority for concept of operations to any person occupying the position of Deputy Director of the Information Protection Centre at DFAIT.

3. **Roles and Responsibilities**

DFAIT will:

¹ As the Shared Services Canada (SSC) organization evolves and the division of roles and responsibilities of SSC versus the individual Government of Canada departments is finalized, this MoU may be amended to reflect such structure as required.

- 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.
- Provide all the necessary information required by CSE to set up and activate the cyber defence operations, ensuring that CSE staff conducts the service only on computer systems and networks for which DFAIT 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, DFAIT will not take any action on the basis of cyber defence reports, other than following mitigation advice provided in the report.. CSE will provide all caveats and handling instructions related to mitigation advice included in a report or service.

CSE 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'S Directorate of Legal Services (DLS), who will work together with DFAIT'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 activities are subject to review by the CSE 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 from DFAIT during cyber defence operations 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), 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 may share data that has come under CSE 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.

CONFIDENTIAL

8. Data and Information Handling

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

(2) CSE's Classified or Protected Information

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

(b) All cyber defence data obtained from DFAIT that has not come under the control of CSE will be PROTECTED B.

(c) Access to cyber defence data obtained from DFAIT and other information obtained by CSE from or about DFAIT during cyber defence operations is limited and controlled according to CSE policies. DFAIT agrees that access by other persons within CSE may only be authorized by the Director General Cyber Defence at CSE.

9. 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, CSE will have measures in place to protect the privacy of Canadians, as established in CSE policies.

10. Interception of Private Communications

It is understood that for CSE to conduct cyber defence operations which may involve the interception of private communications, CSE requires an MA 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.

CSE may share data that has come under CSE 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 DFAIT repository will vary based on operational need and on technical capacity, as advised by CSE. All cyber defence data in the DFAIT 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.

12. DFAIT Cease Operation Capability

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

13. Destruction of DFAIT's Data

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

Page 3 of 5

CERRID 1045545

14. Information Indicating Criminal Activity

In the unlikely event that any member of CSE encounters indications of a criminal code offence on the computer systems or networks of DFAIT, the incident and the data will be brought to the attention of DFAIT management. If DFAIT attempts to locate this data on their networks and systems, and is unable to find it, CSE can provide the data to DFAIT. DFAIT 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 will not carry out cyber defence operations that may intercept private communications. CSE will inform DFAIT 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:

██████████
Director, Cyber Threat Evaluation Centre

Communications Security Establishment
719 Heron Road
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Fax Number: ██████████

Elizabeth Keighley
Dep Dir Information Protection Centre

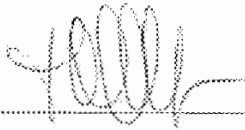
Department of Foreign Affairs and
International Trade
125 Sussex Drive
Ottawa, Ontario
K1A 0G2

Fax Number: (613) 996-1186

- (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.

CONFIDENTIAL

For the COMMUNICATIONS SECURITY ESTABLISHMENT:



Tom Moffa
Deputy Chief
IT Security
Communications Security Establishment

12/12/12

Date

For the DEPARTMENT OF FOREIGN AFFAIRS AND INTERNATIONAL TRADE:



Stéphane Cousineau
Chief Information Officer
Department of Foreign Affairs

Nov 27/12

Date

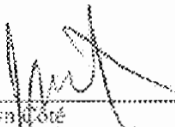


Robin Dubeau
Departmental Security Officer
Department of Foreign Affairs

30 Nov 2012

Date

AND



Jocelyn Jodé
DG International Portfolio
Shared Services Canada

Nov 26/12

Date