



## Memorandum of Understanding between Communications Security Establishment (CSE) and Natural Resources Canada (NRCan)

### PART I – BACKGROUND

This document will cover the agreement between the Communications Security Establishment (CSE) and Natural Resources Canada (referred to as the “Partner Department”), for cyber defence services on NRCan controlled assets.

The Partner Department has requested in writing that CSE conduct cyber defence activities to help protect the Partner Department computer systems;

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 Partner Department is authorized under the *Financial Administration Act* to take reasonable measures to manage or protect the computer systems and networks under its control and supervision, and has the authority under the *Privacy Act* to disclose to CSE personal information for the purposes mentioned in this MoU;

A Ministerial Authorization issued pursuant to the *National Defence Act* (NDA) authorizes CSE to conduct cyber defence operations 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 OPERATIONS TERMS AND CONDITIONS

CSE and the Partner Department 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 operations. CSE’s cyber defence activities augment the Partner Department’s baseline security requirements and responsibilities.



## 2. Fees and Expenses

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

## 3. 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; CSE and the Partner Department will cooperate fully with any such requests.

## 4. Control of Cyber Defence Data (Data)<sup>1</sup>

Data obtained by CSE from the Partner Department 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), 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). Any data not deemed relevant or essential will be deleted in accordance with CSE 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. At all times, CSE will maintain the anonymity of the Partner department.

## 5. Data and Information Handling

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

(2) CSE's Classified or Protected Information

---

<sup>1</sup> Cyber Defence Data (Data) consists of systems activity such as files, processes and network connections.



- a. CSE will ensure that any classified or protected information disclosed to the Partner Department pursuant to this MoU is clearly and appropriately marked as such. The Partner Department will handle such information in accordance with departmental security standards and handling instructions from CSE.
- b. All cyber defence data obtained from the Partner Department that has not come under the control of CSE will be considered Unclassified, but safeguarded in accordance with CSE policy.

Access to cyber defence data obtained from the Partner Department and other information obtained by CSE from or about the Partner Department during cyber defence operations is limited and controlled according to CSE policies.

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

7. 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 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 the Partner Department of the situation, and will not carry out cyber defence operations that may intercept private communications until such time as a new MA is in place.

8. 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 Partner Department's computer systems, the incident and the data will be brought to the attention of the Partner Department management. If the Partner Department attempts to locate this data on their networks



and systems, and is unable to find it, CSE can provide the data to the Partner Department if it is available. The Partner Department shall have responsibility with respect to follow-on action and notification of the appropriate authorities.

9. 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 MoU.

This MoU may be modified in writing at any time with the written consent of both Parties, represented by persons holding positions noted below.

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 confirmation in writing that all data in the Partner Department repository has been destroyed in accordance with CSE policy.

Such notice may be delivered by hand, by regular mail, 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<sup>th</sup>) business day after mailing if sent by regular mail, and on the date of delivery if sent by courier.

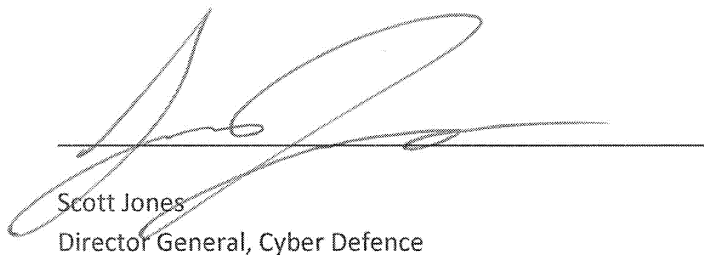
Notices shall be addressed to persons holding the following positions:

Director,  
Cyber Defence Operations  
Communications Security Establishment  
P.O. Box 9703 Terminal  
Ottawa, Ontario  
K1G 3Z4

Director, Security & Emergency  
Management and Intelligence Division,  
Departmental Security Officer,  
Natural Resources Canada  
580 Booth Street  
Ottawa, ON  
K1A 0E4



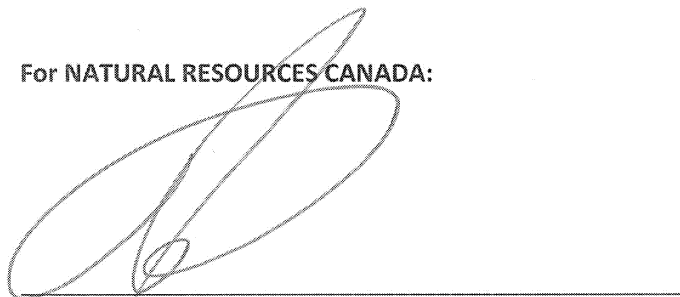
For the COMMUNICATIONS SECURITY ESTABLISHMENT:



Scott Jones  
Director General, Cyber Defence

July 11, 2014  
Date

For NATURAL RESOURCES CANADA:



Pierre Ferland  
Chief Information Officer / Director General  
Chief Information Office and Security Branch  
Natural Resources Canada

11/07/2014  
Date