

CONFIDENTIAL



Communications Security Establishment

**Memorandum of Understanding
between
The Communications Security Establishment
and
Health Canada**

February 12, 2008

CONFIDENTIAL

CONFIDENTIAL

PURPOSE

1. The Communications Security Establishment (CSE), Health Canada the Public Health Agency of Canada (together with CSE, the Parties) recognize the importance of cooperation to ensure that the highest standards of security are applied to SIGINT report handling. This Memorandum of Understanding (MOU) is intended to clarify roles, responsibilities and standards governing the dissemination and usage of classified information supplied by CSE to Health Canada (HC) and the Public Health Agency of Canada (PHAC).

AUTHORITIES

2. CSE's mandate powers and authorities are defined in Part V.1 of the National Defence Act, as amended by the Anti-Terrorism Act of December 2001. In broad terms, CSE provides: foreign signals intelligence in accordance with Government of Canada (GoC) intelligence priorities; advice, guidance and services to help protect electronic information and information infrastructures of importance to the GoC, and technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. CSE is also the cryptology and information technology security authority under the Government Security Policy (GSP).

3. Health Canada is the Federal department responsible for helping Canadians maintain and improve their health. A few of Health Canada's functions are regulation of a large variety of products, medicines and medical devices, pesticides, chemical, nuclear and radiological safety, illicit drugs and food. A key focus of HC is to maintain a pandemic preparedness plan and to contribute to the security of Canadians by coordinating the actions of 20 federal departments and agencies in response to nuclear accidents and development capabilities to rapidly detect and respond to terrorist events.

4. *The Public Health Agency of Canada Act* provides the statutory basis for PHAC's powers and authority. The legislation establishes the Agency as a separate entity within the Health portfolio mandated to promote and protect the health of Canadians through leadership, partnership, innovation and action in public health. A key focus for the Agency is to anticipate and respond effectively to public health threats.

DISSEMINATION

5. HC and PHAC recognizes CSE's authority to manage the distribution of SIGINT reports as outlined in Appendix "A", Section 4.2, of Treasury Board's *Government Security Policy*.

6. Under this authority, CSE recognizes the role of the Health Canada's Departmental Security Officer to disseminate SIGINT end-product reporting, as outlined in this MOU, within PHAC and Health Canada, with the exception of restricted reporting.

7. CSE also recognizes the procedures and processes underpinning PHAC's internal dissemination program outlined in Health Canada's *CRO Protocol* document, which was approved by CSE.

8. [REDACTED] is the CSE application that enables web-based dissemination of SIGINT information to client desktops based on specified client requirements. Appropriately security-cleared HC and PHAC staff located within a SIGINT Secure Area (SSA) may be granted access to [REDACTED] using dedicated terminals.

9. CSE will support internal dissemination by granting, to selected, appropriately security-cleared HC and PHAC employees, access to the [REDACTED] Client Service Interface. This will permit selected users to enter client profiles, feedback and requirements, allowing CSE in return, to track and measure SIGINT end-product usage of clients.

CONFIDENTIAL

CONFIDENTIAL

10. It is understood that all SIGINT material (excluding restricted reports) provided to HC and PHAC will be delivered via the [REDACTED] system meaning that:

- HC and PHAC clients who have access to a MANDRAKE terminal may request [REDACTED] accounts;
- designated HC and PHAC employees will perform internal dissemination of regular end-reports within PHAC and Health Canada.

11. HC and PHAC will keep their [REDACTED] information accurate and current. A CSE Client Account Representative will assist PHAC with [REDACTED] best practices.

12. HC and PHAC understand and agree that all handling, distribution, retention and destruction of SIGINT material will be executed in accordance with the *Canadian SIGINT Security Standards (CSSS)* and other applicable policies and procedures. Unless otherwise approved by CSE, these activities will only be performed for PHAC and Health Canada internal SIGINT clients according to each individual client's security clearance and need to know requirements. CSE reserves the right to conduct, in cooperation with HC and PHAC, on-site security audits on the handling of COMINT material.

13. CSE is committed to providing HC and PHAC the training, policy and operational support required to fulfill its internal dissemination mandate. Likewise, HC and PHAC are committed to keeping CSE abreast of any changes to its dissemination policies and procedures.

AUTHORIZED USE

14. HC and PHAC recognizes that "authorized use" of [REDACTED] refers to any use of SIGINT by the department that can be clearly shown to be in support of its mandate, which may include "need-to-know"-based searches of [REDACTED] internal dissemination, inclusion of SIGINT in briefings and assessments, and actions taken based on SIGINT, which must be receive prior approval by CSE's Operational Policy Group. Terms and conditions of SIGINT use are subject to the CSSS, SIGINT dissemination procedures and all CSE Operational Policies, and may be further refined by CSE in memoranda of understanding or letters of agreement.

15. "Need-to-know" is a determination made by an authorized holder of information to assess whether a recipient requires access to that information in order to perform an authorized government function. It is a fundamental aspect of SIGINT handling and reflects the principle that not everyone who is cleared to see SIGINT necessarily needs to see all of it. (For further details, see OPS-5-15, Need-to-Know Guidelines, available on the CSE Mandrake homepage.)

MONITORING

16. HC and PHAC understand that [REDACTED] is subject to system and security auditing and monitoring by CSE. Any use of [REDACTED] must follow the principles of "authorized use" and "need-to-know". Users understand that their [REDACTED] use is subject to monitoring, as defined herein, and unauthorized activities are subject to sanctions.

CONFIDENTIALITY AND SECURITY OF INFORMATION

17. Information provided by a Party pursuant to this MOU will only be used for the specific purpose for which it is provided. The Parties will ensure that appropriate procedures are in place to protect the information from any further disclosure.

CONTACTS

18. The primary CSE client relations contact person is the Head Client Relations Officer at PCO.

19. The primary Health Canada contact person is the Departmental Security Officer.

CONFIDENTIAL

2

CONFIDENTIAL

MODIFICATION

20. This MOU may be modified at any time by written consent of the Parties.

EFFECTIVE DATE

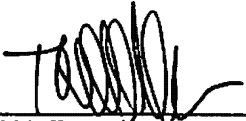
21. This MOU will come into effect when signed by the Parties and remain in effect until terminated.

TERMINATION

22. Either Party, upon written notice, may terminate this MOU at any time.

REVIEW

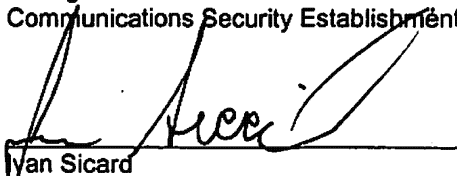
23. This Memorandum of Understanding will be reviewed on an annual basis to ensure it remains current with operational requirements and administrative changes.



Toni Moffa

Date 17 Feb 2008

Director General,
Intelligence Branch
Communications Security Establishment



Ivan Sicard

Date 26 Feb, 2008

Executive Director/DSO/SIO
Health Canada

CONFIDENTIAL

3