



Canadian Nuclear  
Safety Commission

Commission canadienne  
de sûreté nucléaire

P.O. Box 1046 Station B  
Ottawa, Ontario  
K1P 5S9

C.P. 1046, Succursale B  
Ottawa (Ontario)  
K1P 5S9

Fax: (613) 995-5086

Télécopieur : (613) 995-5086

**Directorate of Security and Safeguards**

①

Your file    Votre référence

Our file    Notre référence

4.11.02

E-DOCS-#3345586

March 10, 2009

Business Relations Advisor  
CSES Communications Security Establishment Canada  
719 Heron Road  
Ottawa, Ontario  
K1G 3Z4

②

As discussed, for  
Toni's signature and  
return to CNSC.

Thanks

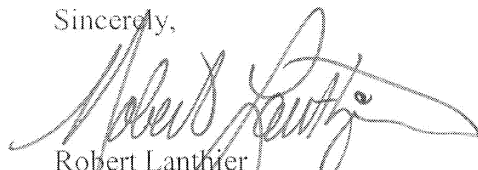
**Subject: Memorandum of Understanding (MOU) between the Communications  
Security Establishment Canada and the Canadian Nuclear Safety  
Commission**

Dear [REDACTED]

Please find enclosed two copies of the duly signed MOU between the Communications Security Establishment Canada and the Canadian Nuclear Safety Commission.

Would you please arrange for Mr. Toni Moffa, Director General of Intelligence Branch to sign the original MOUs and return one signed copy to our office, for our records.

Sincerely,

  
Robert Lanthier  
Director  
Nuclear Security Division

c.c.: D. McKelvey

4523dm

Canada

CONFIDENTIAL



Communications Security Establishment Canada

**Memorandum of Understanding  
between  
The Communications Security Establishment Canada  
and  
The Canadian Nuclear Safety Commission  
concerning  
Handling of SIGINT end-product reports**

February 2, 2009

CONFIDENTIAL

# CONFIDENTIAL

## PURPOSE

1. The Communications Security Establishment Canada (CSEC) and the Canadian Nuclear Safety Commission (CNSC) (together with CSEC, the Participants) recognize the importance of cooperation to ensure that the highest standards of security are applied to signals intelligence (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 CSEC to CNSC.

## AUTHORITIES

2. CSEC'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, CSEC 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. CSEC is also the cryptology and information technology security authority under the Government Security Policy (GSP).

3. The mandate of the CNSC, pursuant to paragraph 9(a) of the *Nuclear Safety and Control Act* (NSC Act), is to regulate the development, production, possession and use of nuclear substances, prescribed equipment and prescribed information in order to prevent unreasonable risk to the health and safety of persons, the environment and national security, and to achieve conformity with Canada's international obligations regarding the peaceful use of nuclear energy. Paragraph 21(1)(a) of the NSC Act also authorizes the CNSC to "enter into arrangements, including an arrangement to provide training, with any person, any department or agency of the Government of Canada or of a province, any regulatory agency or department of a foreign government or any international agency."

## ACCESS

4. CNSC recognizes CSEC's authority to manage the distribution of SIGINT reports as outlined in Appendix "A", Section 4.2, of Treasury Board's *Government Security Policy*.

5. Under this authority, CSEC recognizes the role of CNSC to access SIGINT end-product reporting, as outlined in this MOU, with the exception of restricted reporting.

6. [REDACTED] is the CSEC application that enables Web-based dissemination of SIGINT information to client desktops based on specified client requirements. Appropriately security-cleared CNSC staff located within a SIGINT Secure Area (SSA) may be granted access to [REDACTED] using dedicated terminals. All SIGINT material (excluding restricted reports) provided to CNSC will be delivered via [REDACTED]

7. CNSC users will keep their [REDACTED] information accurate and current.

8. CNSC understands and agrees that all access, 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. CSEC reserves the right to conduct, in cooperation with CNSC, on-site security audits on the handling of SIGINT material.

9. CSEC is committed to providing CNSC the training, policy and operational support required to utilize [REDACTED]. Likewise, CNSC is committed to keeping CSEC abreast of any changes to its internal policies and procedures concerning SIGINT handling.

CONFIDENTIAL

## CONFIDENTIAL

### AUTHORIZED USE and HANDLING

10. CNSC recognizes that "authorized use" of [REDACTED] refers to any use of SIGINT by the CNSC 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, any and all of which must receive prior approval by CSEC's Operational Policy Group. Terms and conditions of SIGINT use are subject to the CSSS, SIGINT Dissemination Procedures and all CSEC Operational Policies, and may be further refined by CSEC in MOU's or letters of agreement.

11. "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. This 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 CSEC Mandrake homepage.)

### MONITORING

12. CNSC understands that [REDACTED] is subject to system and security auditing and monitoring by CSEC. 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, and unauthorized activities are subject to sanctions.

### CONFIDENTIALITY AND SECURITY OF INFORMATION

13. Information provided by CSEC will only be used for the specific purpose for which it is provided. The Participants will ensure that appropriate procedures are in place to protect the information from any further disclosure.

14. The Participants will not disclose any information provided as described in this MOU to a third party without the permission of the originating Participant.

### CONTACTS

15. The primary CSEC client relations contact person is the Client Relations Officer at the Industry Canada site.

16. The primary CNSC contact person is the Security Intelligence Officer – Nuclear Security Division at the CNSC Headquarters site.

### MODIFICATION

17. This MOU may be modified at any time by written consent of the Participants.

### EFFECTIVE DATE

18. This MOU will come into effect when signed by the Participants and shall remain in effect until terminated.

### TERMINATION

19. Either Participant may terminate this MOU at any time upon written notification.

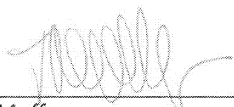
CONFIDENTIAL

2

CONFIDENTIAL

REVIEW

20. 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 6/3/09

Director General,  
Intelligence Branch  
Communications Security Establishment Canada

  
\_\_\_\_\_  
Michael Binder

Date 28/2/09

President,  
Canadian Nuclear Safety Commission

CONFIDENTIAL

3