

CONFIDENTIAL



Communications Security Establishment Canada

**Memorandum of Understanding  
between  
The Communications Security Establishment Canada  
and  
Canada Revenue Agency  
concerning  
Handling of SIGINT end-product reports**

October 27, 2008

CONFIDENTIAL

# CONFIDENTIAL

## PURPOSE

1. The Communications Security Establishment Canada (CSEC) and the Canada Revenue Agency (CRA) (together with CSEC, the Parties) 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 the CRA.

## 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 Review and Analysis Division (RAD) of the CRA is to manage the risk of terrorist involvement in the registration system for charities and to implement Part 6 of the *Anti-Terrorism Act*, the *Charities Registration (Security Information) Act*<sup>1</sup>. RAD fulfills its mandate by:

- Preventing organizations with ties to terrorism from obtaining registration;
- Detecting and revoking registered organizations with ties to terrorism; and
- Ensuring that the CRA contributes fully to the GoC's overall efforts to combat terrorist financing, through appropriate sharing of information.

## ACCESS

4. CRA 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 CRA 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 CRA 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 CRA will be delivered via [REDACTED]

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

8. CRA 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 CRA, on-site security audits on the handling of SIGINT material.

---

<sup>1</sup> An Act respecting the registration of charities having regard to security and criminal intelligence information. For the purpose of the Act, "information" means security or criminal intelligence information and information that is obtained in confidence from a source in Canada, from the government of a foreign state, from an international organization of states or from an institution of such a government or organization.

CONFIDENTIAL

## CONFIDENTIAL

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

### AUTHORIZED USE

10. CRA recognizes that "authorized use" of [REDACTED] refers to any use of SIGINT by the agency 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. CRA 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 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.

14. The Parties will not disclose any information provided pursuant to this MOU to a third party without the permission of the originating Party.

15. CRA shall consult with CSEC prior to any actions or proceedings being undertaken under either the *Income Tax Act* or the *Charities Registration (Security Information) Act* which may utilize information provided pursuant to this MOU.

16. CRA shall fully support any decision or assist in any course of action that CSEC may take to protect its information, including objecting or making an appropriate notification under section 38 of the *Canada Evidence Act* whenever required and permitted.

### CONTACTS

17. The primary CSEC client relations contact person is the Director, [REDACTED]

18. The primary CRA contact person is the Manager, Strategic Intelligence and Liaison.

### MODIFICATION

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

CONFIDENTIAL

2

## CONFIDENTIAL

### EFFECTIVE DATE

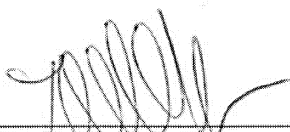
20. This MOU will come into effect when signed by the Parties and remain in effect until terminated.

### TERMINATION

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

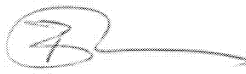
### REVIEW

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

  
\_\_\_\_\_  
Toni Moffa

Director General,  
Intelligence Branch  
Communications Security Establishment Canada

Date 11/24/08

  
\_\_\_\_\_  
Terry De March

Director General,  
Charities Directorate  
Canada Revenue Agency

Date 17/11/08

CONFIDENTIAL

3