

CONFIDENTIAL



Communications Security Establishment Canada

**Memorandum of Understanding
between
The Communications Security Establishment Canada
and
Public Works and Government Services Canada
concerning
Handling of SIGINT end-product reports**

December 30, 2010

CONFIDENTIAL

CONFIDENTIAL

PURPOSE

1. The Communications Security Establishment Canada (CSEC) and Public Works and Government Services Canada (PWGSC) (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 PWGSC.

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 Policy on Government Security (PGS).

3. The Policy on Government Security identifies PWGSC as a Lead Security Agency with a number of responsibilities, including the delivery of services related to IT security, physical security, and the Industrial Security Program. In addition, pursuant to the *Defence Production Act* as well the Controlled Goods Regulations, PWGSC administers the Controlled Goods Program to safeguard controlled goods and/or controlled technology within Canada and prevent access by unauthorized persons. To support the preceding, the mandate of the [REDACTED] of PWGSC, pursuant to Departmental Policy 051 (DP 051), is to:

- a) Obtain, collate and analyze information concerning the security of PWGSC personnel, services, information, critical infrastructure and other assets;
- b) Provide PWGSC's senior managers with threat assessments, trend analysis, advice and other information drawn from security intelligence in advance of potentially harmful events;
- c) Coordinate information analysis in support of PWGSC's response to changes in security readiness levels as defined by the "Operational Security Standard – Readiness Levels for Federal Government Facilities".

ACCESS

4. PWGSC recognizes CSEC's authority to manage the distribution of SIGINT reports as outlined in Treasury Board's *Policy on Government Security*.

5. Under this authority, CSEC recognizes the role of PWGSC 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 PWGSC 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 PWGSC will be delivered via [REDACTED]

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

8. PWGSC 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)*

CONFIDENTIAL

CONFIDENTIAL

and other applicable policies and procedures. CSEC reserves the right to conduct, in cooperation with PWGSC, on-site security audits on the handling of SIGINT material.

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

AUTHORIZED USE AND HANDLING

10. PWGSC recognizes that "authorized use" of [REDACTED] refers to any use of SIGINT by the PWGSC 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 PWGSC 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. PWGSC 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 COMCO or D/COMCO must report compromises or suspected compromises of SIGINT to the Departmental Security Officer (DSO) who, in turn, must immediately inform CSEC.

15. The Participants will not disclose any information provided pursuant to this MOU to a third party without the permission of the originating Participant.

CONTACTS

16. The primary CSEC client relations contact person is the Director, [REDACTED] in the Intelligence Branch.

17. The primary PWGSC contact person is the Manager in the [REDACTED]

MODIFICATION

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

CONFIDENTIAL

2

CONFIDENTIAL

EFFECTIVE DATE

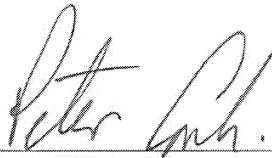
19. This MOU will come into effect when signed by the Participants and shall remain in effect until terminated.

TERMINATION

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

REVIEW

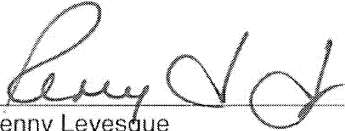
21. This Memorandum of Understanding will be reviewed on an annual basis to ensure it remains current with operational requirements and administrative changes.



Peter Cork

Director General,
Intelligence Branch
Communications Security Establishment Canada

Date 6 JAN 2011



Penny Levesque

Director General, Corporate Services
and Departmental Security Officer
Public Works and Government Services Canada

Date 11 Jan 2011

CONFIDENTIAL