

November 15, 2011

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

Hereinafter referred to as "CSEC"

AND

THE DEPARTMENT OF FOREIGN AFFAIRS AND INTERNATIONAL TRADE (DFAIT)

Hereinafter referred to as "DFAIT"

Concerning the provision of signals intelligence (SIGINT) service at DFAIT.

PURPOSE

RECOGNIZING the importance of DFAIT to CSEC as a SIGINT client and the value to DFAIT of the CSEC SIGINT service.

RECOGNIZING that the powers, duties and functions of the Minister of Foreign Affairs, in accordance with section 10 (1), of the *Department of Foreign Affairs and International Trade Act*; "extend to and include all matters over which Parliament has jurisdiction, not by law assigned to another department, board, or agency of the Government of Canada, relating to the conduct of the external affairs of Canada...".

RECOGNIZING CSEC's mandate, powers and authorities which 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 (GC) intelligence priorities; advice, guidance and services to help protect electronic information and information infrastructures of importance to the GC, 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).

RECOGNIZING the need to establish roles, responsibilities and standards governing the dissemination of SIGINT end-product reports supplied by CSEC to DFAIT and the operation of the DFAIT client relations office.

RECOGNIZING the importance of DFAIT / CSEC cooperation to ensure that the highest standards of security are applied to handling of signals intelligence (SIGINT) end-product reports.

RECOGNIZING CSEC's authority to manage the distribution of SIGINT as outlined in Treasury Board's *Policy on Government Security* (PGS).

NOW THEREFORE DFAIT and CSEC undertake, further to the General Framework MOU between DFAIT and CSEC, to continue to cooperate on the effective and secure distribution of SIGINT material.

DEFINITIONS

In this Memorandum of Understanding, unless otherwise dictated by the context,

"Authorized use" of SIGINT means any use of SIGINT by the department that can be shown to be in support of the department's mandate. This may include "need-to-know"-based searches of [REDACTED] internal DFAIT dissemination, inclusion of SIGINT in briefings and assessments, and any "Action-on" activity taken based on SIGINT.

"Action-on" is defined in CSEC's Ops 5-9 policy as being "Any action taken on the basis of Communications Intelligence (COMINT) which might jeopardize the COMINT source. This usually involves a sanitization." Such "Action-on" activity must receive prior approval by CSEC's Operational Policy Group.

"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 their authorized government function.

[REDACTED] means the CSEC application that enables web-based dissemination of SIGINT reports to users' desktops based on specified client requirements.

PART I: DISSEMINATION

1. CSEC will provide seconded staff to a Client Relations Unit within DFAIT's Threat Assessment and Intelligence Service Division with the purpose of meeting the intelligence requirements of the Department. CSEC Client Relations Officers (CROs) will form a part of an integrated team providing service to selected, security-cleared DFAIT clients. The objectives of the office will be agreed upon through an annual service plan, consistent with Cabinet direction on intelligence priorities, in partnership between DFAIT DG Security and Intelligence and CSEC DG Intelligence.

2. The Client Relations Office at DFAIT will be staffed by DFAIT personnel, including the Head, and seconded personnel, including from CSEC. Non-CSEC personnel would be required to complete a standard training program on the SIGINT process and policies as determined by CSEC. The CSEC staffing component is currently set at [REDACTED] CSEC will consider changes to this upon request from DFAIT. The operational priorities and direction of the unit will be managed by DFAIT's Head, Client Relations, under the management of the Director, Threat Assessment and Intelligence Services Division. CSEC personnel will remain administratively accountable to the SIGINT [REDACTED] in the CSEC Intelligence Branch.

3. CROs within an integrated Client Relations Unit will provide DFAIT clients with all types and sources of intelligence, including but not limited to SIGINT, HUMINT and assessments based on client requirements. By mutual agreement, all members of the Client Relations Unit will support CSEC's SIGINT objectives through the provision of client requirements, priorities and feedback, and will educate clients concerning SIGINT capabilities.

4. [REDACTED] will only be accessed via terminals within a CSEC-approved Secure SIGINT Area (SSA).

PART II: MONITORING AND COMPLIANCE

5. DFAIT understands that [REDACTED] is subject to system and security auditing and monitoring. Any use of [REDACTED] must follow the principles of "authorized use" and "need-to-know". Users understand that they must not expect privacy and unauthorized activities are subject to sanctions.

6. DFAIT will handle SIGINT material in accordance with the *Canadian SIGINT Security Standards (CSSS)*, CSEC Operational Policies, and other applicable policies and procedures.

7. DFAIT understands that their compliance with the above documents is subject to security auditing and monitoring.

8. DFAIT will ensure that all DFAIT products that contain information from SIGINT are appropriately classified and referenced.

9. Certain restricted SIGINT products (e.g., those with named distribution lists or those requiring a special indoctrination) must be disseminated in accordance with the "need-to-know" principle as determined by CSEC. In the rare event that a distribution list for such a report does not include DFAIT's Director General, Security and Intelligence, and DFAIT's Director, Threat Assessment and Intelligence Services, CSEC will inform them of the fact that a report is being distributed.

10. CSEC will inform DFAIT of any non-compliance issues so that they can cooperate on measures to address such matters.

11. DFAIT must report compromises or suspected compromises of SIGINT to the Departmental Security Officer (DSO) who, in turn, must immediately inform CSEC.

PART III: CONFIDENTIALITY AND SECURITY OF INFORMATION

12. Information provided by CSEC and DFAIT pursuant to this MOU will only be used for the specific purpose for which it is provided. CSEC and DFAIT will ensure that appropriate procedures are in place to protect the information from any further disclosure.

13. CSEC and DFAIT will not disclose any information provided pursuant to this MOU to a third party without the permission of the originating party.

PART IV: CONTACTS


14. The primary CSEC contact person is the SIGINT [REDACTED] in DGI.

15. The primary DFAIT contact person is the Director, Foreign Intelligence Division.

PART V: EFFECTIVE DATE, MODIFICATIONS

16. This MOU:

- (a) will come into effect when signed by CSEC and DFAIT and will remain in effect until terminated,
- (b) may be modified at any time by written consent of both CSEC and DFAIT,
- (c) may be terminated at any time upon one month's written notice,
- (d) be added to Annex A of the General Framework Agreement between CSEC and DFAIT, and
- (e) will be reviewed as required to ensure it remains current with operational requirements and administrative changes.



Peter Cork

Date 24 Nov 11

Director General, Intelligence
Communications Security Establishment Canada



Artur Wilczynski

Date Dec. 2 / 11

Director General, Security and Intelligence Bureau
Department of Foreign Affairs and International Trade Canada