Summary authorized, see Annex A.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

TOP SECRET//SI//CEO
CERRID #885257
CCM #12-00146

MAR 30 2012

MEMORANDUM FOR MINISTER OF NATIONAL DEFENCE

Ministerial Authorization Year-End Reporting 2010-11

(For Information)

Summary

- This Memorandum and accompanying report are intended to satisfy reporting obligations under Ministerial Authorization (MA) which require the Communications Security Establishment Canada (CSEC) to report to you on the use and retention of private communications incidentally intercepted in the course of these authorized activities.
- This year, CSEC is reporting to you on six Signals Intelligence (SIGINT) MAs and one Information Technology Security (ITS) MA.

Background

- The seven recently expired CSEC MAs that contain year-end reporting requirements are:
  - [redacted] Interception [redacted]
  - Interception Activities [redacted]
  - Interception Activities Conducted in Support of Canadian Forces Operations in Afghanistan;
  - [redacted]
  - CSE Interception Activities [redacted]
  - [redacted] Interception [redacted] and,
  - Protection of Government of Canada Computer Systems and Networks: Cyber Defence Operations (CDO).
- In accordance with the terms of these MAs, CSEC must report to you on the use and retention of incidentally intercepted private communications related to each of these activity areas, as per the specific requirements for SIGINT and ITS MAs, respectively.

Year-End Report for MAs Expired on 30 November 2011

- As per past practice, CSEC year-end reporting is provided to you in a single consolidated report, which is attached to this Memorandum.
- In addition to the specific requirements for the SIGINT MAs outlined in Part I of the attached report, CSEC is required to report to you when any serious issue arises in the implementation of SIGINT MAs, of which none were encountered during this period.
- In addition to the specific requirements for the ITS MA outlined in Part II of the attached report, the Chief must review, on a twice-yearly basis, the number of private communications used or retained by CSEC to identify, isolate or prevent harm to Government computer systems or networks. My predecessor conducted these reviews at a frequency that surpasses this requirement, and I do not have any issues to report to you in this regard.
- In keeping with past practices, additional information has also been included on the overall results of these CSEC collection programs, to provide context to these activities.
- I can confirm that all activities carried out under each of these MAs were conducted in accordance with the Ministerial Directives *Privacy of Canadians* and *Accountability Framework* issued to CSEC on 19 June 2001, and with CSEC's own relevant operational policies.
- I would be pleased to provide further details on CSEC activities carried out under these MAs at your request.

John Forster
Chief

Attachment

TOP SECRET//SI//CEO
(with attachment)

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

REQUIRED YEAR-END REPORTING

UNDER MINISTERIAL AUTHORIZATION

MARCH 2012

Canada

COMMUNICATIONS SECURTY ESTABLISHMENT CANADA
REQUIRED YEAR-END REPORTING
UNDER MINISTERIAL AUTHORIZATION

PART I:

PART II:

PART I

CSEC REQUIRED YEAR-END REPORTING FOR SIGINT MAs EFFECTIVE 1 DECEMBER 2010 – 30 NOVEMBER 2011

REPORTING REQUIREMENTS FOR ALL SIGINT MAs

In accordance with the terms of CSEC's six SIGINT MAs and following their expiration, CSEC is required to report to the Minister of National Defence on:

i) The number of recognized private communications intercepted pursuant to these MAs that are used or retained on the basis that they are essential to international affairs, defence or security;

ii) The number of recognized solicitor-client communications intercepted pursuant to these MAs that are used or retained on the basis that they are essential to international affairs, defence or security and in conformity with the legal advice received;

iii) The number of intelligence reports produced from the information derived from private communications intercepted pursuant to these MAs; and,

iv) The foreign intelligence value of these reports, as they relate to international affairs, defence or security.

CSEC is also required to report to you when any serious issues arise in the implementation of its SIGINT MAs. During the period of 1 December 2010 to 30 November 2011, there were no serious issues encountered for any of the SIGINT MAs in question.

Additional Information

For context, CSEC is also including in this report the number of private communications destroyed and the number of solicitor-client communications deleted for each of the respective SIGINT MAs in question. All activities carried out under each of these SIGINT MAs were conducted in accordance with the effective versions of their respective operational policies, which include:

- OPS-1: "Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities";
- OPS 1-13: "Procedures for Canadian [redacted] and Joint CSEC-CF Activities"; and,
- OPS 3-1: "Procedures for [redacted] Operations".

[redacted] INTERCEPTION [redacted]

- **Number of recognized private communications intercepted:** [redacted] (out of a total of [redacted] communications intercepted overall)
    - **Number of private communications used or retained:** [redacted]
    - **Number of private communications destroyed:** [redacted]
- **Number of recognized solicitor-client communications intercepted:** [redacted]
    - **Number of solicitor-client communications used or retained:** [redacted]
    - **Number of solicitor-client communications destroyed:** [redacted]
- **Number of intelligence reports produced with information derived from private communications:** [redacted]
- **Foreign intelligence value of reports produced with information derived from private communications:** Of the [redacted] private communications retained, [redacted] were used in [redacted] foreign intelligence reports, including [redacted] intercept retained during the previous MA review period (covered by the 2009-2010 MA). [redacted] of the [redacted] private communications were retained for future use.

Additional Information

CSEC/CFIOG issued [redacted] foreign intelligence reports based on information derived in whole or in part from [redacted] communications intercept. The reports covered a variety of [redacted] issues. [redacted] of the [redacted] reports were based in whole or in part on "private communications" intercepts and all [redacted] were deemed to have satisfied an intelligence requirement for one or more of CSEC's clientele. Furthermore, CSEC's SIGINT allies issued [redacted] foreign intelligence reports derived from Canadian [redacted] intercept.

This reporting was viewed by clients in [redacted] Government of Canada departments and agencies and was of particular interest to the Privy Council Office, the Department of Foreign Affairs and International Trade, the Canadian Security Intelligence Service, Public Safety Canada, the Department of National Defence, and the Canada Border Services Agency.

With respect to working with international partners, the sharing of Canadian SIGINT collection facilitates CSEC's participation in, and access to, intelligence production from similar allied programs.

INTERCEPTION ACTIVITIES CONDUCTED IN SUPPORT OF CANADIAN FORCES OPERATIONS IN AFGHANISTAN

- **Number of recognized private communications intercepted:** [redacted] (out of a total of [redacted] communications intercepted overall)
    - **Number of private communications used or retained:** [redacted]
    - **Number of private communications destroyed:** [redacted]
- **Number of recognized solicitor-client communications intercepted:** [redacted]
    - **Number of solicitor-client communications used or retained:** [redacted]
    - **Number of solicitor-client communications destroyed:** [redacted]
- **Number of intelligence reports produced with information derived from private communications:** [redacted]
- **Foreign intelligence value of reports produced with information derived from private communications**: There were [redacted] reports produced with information from private communications. [redacted] private communications intercepts were retained for future use.

Additional Information

CSEC/CFIOG produced [redacted] foreign intelligence reports, based in whole or in part on information derived from the [redacted] reports) and [redacted] reports) collection [redacted] The reports covered a variety of issues supporting Canadian [redacted] and were shown to CSEC clientele in [redacted] Government of Canada departments and agencies including the Royal Canadian Mounted Police, Public Safety Canada, the Privy Council Office, the Integrated Terrorism Assessment Centre, the Department of National Defence, the Department of Foreign Affairs and International Trade, the Canadian Security and Intelligence Service, the Correctional Service of Canada, the Canadian International Development Agency, and the Canada Border Services Agency. [redacted] of the aforementioned foreign intelligence reports were based on private communications intercept.

CSEC's SIGINT allies (DSD, GCHQ, and NSA) issued [redacted] foreign intelligence reports derived in whole or in part from [redacted] reports), [redacted] reports), or [redacted] reports) collection, or, as in one case, a combination thereof. The reports covered a variety of [redacted] security issues. In addition, CSEC/CFIOG used [redacted] reports) and [redacted] report) collection to produce [redacted] SIGINT reports that were provided directly to the Canadian Forces [redacted] to support their ongoing operations. [redacted]

[redacted] INTERCEPTION [redacted]

- **Number of recognized private communications intercepted:** [redacted] (out of a total of [redacted] communications intercepted overall)
    - **Number of private communications used or retained:** [redacted]
    - **Number of private communications destroyed:** [redacted]
- **Number of recognized solicitor-client communications intercepted:** [redacted]
    - **Number of solicitor-client communications used or retained:** [redacted]
    - **Number of solicitor-client communications destroyed:** [redacted]
- **Number of intelligence reports produced with information derived from private communications:** [redacted]
- **Foreign intelligence value of reports produced with information derived from private communications**: There were [redacted] reports produced with information from private communications.

Additional Information

CSEC/CFIOG [redacted] foreign intelligence reports based on information derived from Canadian [redacted] collection. During the same timeframe, however, NSA and GCHQ issued [redacted] foreign intelligence reports based in whole or in part on Canadian [redacted] collection. The reports dealt with [redacted]

[redacted] collection also continued to provide information on global networks used to support other CSEC collection programs and improve understanding of targets and their communications patterns.

INTERCEPTION ACTIVITIES [redacted]

- **Number of recognized private communications intercepted:** [redacted] (out of a total of [redacted] communications intercepted overall)
    - **Number of private communications used or retained:** [redacted]
    - **Number of private communications destroyed:** [redacted]
- **Number of recognized solicitor-client communications intercepted:** [redacted]
    - **Number of solicitor-client communications used or retained:** [redacted]
    - **Number of solicitor-client communications destroyed:** [redacted]
- **Number of intelligence reports produced with information derived from private communications:** [redacted]
- **Foreign intelligence value of reports produced with information derived from private communications**: There were [redacted] reports produced with information from private communications.

Additional Information

CSEC issued [redacted] foreign intelligence reports based in whole or in part from [redacted] These reports covered [redacted] issues and were viewed by CSEC clients in [redacted] government departments or agencies.

CSEC's SIGINT allies (NSA and GCHQ) issued [redacted] foreign intelligence reports derived in whole or in part from [redacted] reports), [redacted] reports), [redacted] report) collection. [redacted] reporting generally related to [redacted]

This reporting was viewed by clients in [redacted] Government of Canada departments and agencies and was of particular interest to the Privy Council Office, the Department of Foreign Affairs and International Trade, the Canadian Security Intelligence Service, the Canada Border Services Agency and the Department of National Defence.

During the review period, a new [redacted] was introduced. A total of [redacted] communications were intercepted through this new [redacted] foreign intelligence [redacted] produced.

During the previous MA cycle [redacted] intercepted [redacted] communications. A [redacted]

[redacted]

The majority of the [redacted] were [redacted] private communications or solicitor-client communications were recognized; accordingly, [redacted] reports were based on such information.

Additional Information

CSEC/CFIOG issued [redacted] foreign intelligence reports (including [redacted] report) based in whole or in part on information derived from [redacted] collection. [redacted] percent of the reports were derived from a [redacted] operation directed against [redacted] covered a wealth of [redacted] issues, while [redacted] percent of the reports similarly concerned [redacted] for an additional [redacted] percent of the total; [redacted] percent; and [redacted] percent. [redacted] accounted for six percent of the reports. The remaining [redacted] percent covered [redacted]

CSEC's SIGINT allies (NSA, GCHQ, and DSD) issued [redacted] foreign intelligence reports derived in whole or in part from Canadian [redacted] collection. These reports covered a wide range of issues related to [redacted]

This reporting was viewed by clients in [redacted] Government of Canada departments and agencies and was of particular interest to the Privy Council Office, the Department of Foreign Affairs and International Trade, the Canadian Security Intelligence Service, the Department of National Defence and the Canada Border Services Agency.

As noted, this year's [redacted] collection volumes rose in comparison to the previous year. The [redacted] and program adjustments, building on developments undertaken in 2009-2010. These include a streamlined approach to requirements and approval processes, as well as the implementation of automated [redacted] Intelligence reporting trends have also evolved during the period, with more emphasis being placed on [redacted] and are always guided by CSEC's Ministerial Directive on Intelligence Priorities.

CSEC'S INTERCEPTION ACTIVITIES [redacted]

[redacted] has not yet commenced at the [redacted]

- **Number of recognized private communications intercepted:** [redacted]
    - **Number of private communications used or retained:** [redacted]
    - **Number of private communications destroyed:** [redacted]
- **Number of recognized solicitor-client communications intercepted:** [redacted]
    - **Number of solicitor-client communications used or retained:** [redacted]
    - **Number of solicitor-client communications destroyed:** [redacted]
- **Number of intelligence reports produced with information derived from private communications:** [redacted]

Foreign intelligence value of reports produced with information derived from private communications: [redacted]

Additional Information

[redacted] CSEC sought an MA for this particular operation because the planned [redacted] and potential [redacted] activity could result in the incidental interception of private communications.

The [redacted] was undertaken last year. Analysis of the [redacted] private communications were noted [redacted]

This report outlines the operational status of CSEC's Interception Activities [redacted] conducted for the period from 22 July to 30 November 2011. Please note that [redacted] end product reports were issued during the review period.

PART II

CSEC REQUIRED YEAR-END REPORTING FOR ITS MA EFFECTIVE 1 DECEMBER 2010 – 30 NOVEMBER 2011

REPORTING REQUIREMENTS FOR ITS MA

In accordance with the terms of CSEC's ITS MA pertaining to the protection of Government computer systems and networks, CSEC is required to report to the Minister of National Defence after its expiration, on a per federal institution basis, to specify:

> i) The number of private communications used or retained, pursuant to this Ministerial Authorization, on the basis that the information extracted from those private communications was essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. Such reporting will also specify the total number of these used or retained private communications shared with the CSEC SIGINT program..

Also pursuant to this MA, the Chief, CSEC must review on a twice yearly basis the number of private communications used or retained by CSEC to identify, isolate or prevent harm to Government of Canada computer systems or networks. In regards to the MA period in question, reviews by the Chief, CSEC have been conducted at a frequency that surpasses this requirement, and no serious issues were identified in this regard.

In addition, all activities carried out under this MA were conducted in accordance with the effective versions of its associated operational policies, which include:

- OPS-1: "Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities"; and,
- OPS-1-14: "Operational Procedures for Cyber Defence Operations Conducted under Ministerial Authorization".

PROTECTION OF GOVERNMENT OF CANADA COMPUTER SYSTEMS AND NETWORKS: CYBER DEFENCE OPERATIONS (CDO)

- **Number of private communications used or retained:** [redacted]
    - **During protection activities carried out at** [redacted]
    - **During protection activities carried out at the** [redacted]
    - **During protection activities carried out at the** [redacted]
    - **During protection activities carried out at** [redacted]
- **Number of used or retained private communications shared with the CSEC SIGINT program:** [redacted]
    - **During protection activities carried out at** [redacted]
    - **During protection activities carried out at the** [redacted]
    - **During protection activities carried out at the** [redacted]
    - **During protection activities carried out at** [redacted]

Additional Information

CSEC produced a total of [redacted] reports based on [redacted] incidents (note that one report can include several incidents) from Cyber Defence Operations under this MA, describing and responding to cyber events targeting federal systems and networks. A subset of these reports was also shared with Five Eyes cryptologic partner agencies. Information included in these reports is based on current knowledge and available data obtained under this MA.

As malicious cyber activity directed against an expanding range of Government computer systems is often embedded in normal or legitimate network traffic, the uniqueness of this MA program is that the acquisition of private communications is sometimes necessary for the effective identification and prevention of potential cyber threats. In light of this, CSEC notes that the number of used or retained private communications referenced above constitutes a minute fraction of the vast volume of data monitored by CSEC under this MA in the course of protecting Government systems and networks.

In related cyber defence efforts and in support of Canada's Cyber Security Strategy, CSEC established the Cyber Threat Evaluation Center (CTEC) in late 2009. Over the course of 2011, this new area, combined with existing cyber defence capabilities, continued delivery of its products and services to build cyber threat awareness and strengthen defensive postures within the federal Government. A full-year reporting period and increased protection activities at [redacted] reflect an increase in CSEC's ITS reporting levels while still remaining in line with previous years' reporting.