Summary authorized, see Annex A.

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

TOP SECRET//SI//CEO
CERRID#1204582
ECT#13-2911

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

MINISTERIAL AUTHORIZATION YEAR END REPORTS

2011-2012

Canada

NOT REVIEWED

00000

COMMUNICATIONS SECURTY ESTABLISHMENT CANADA MINISTERIAL AUTHORIZATION (MA) YEAR END REPORTING

PART I: 2011-12 SIGNALS INTELLIGENCE (SIGINT) MINISTERIAL AUTHORIZATION END REPORTS

SIGINT MA REPORTING REQUIREMENTS 3

1) [redacted] Interception [redacted] 4

2) Interception activities conducted in support of the Government of Canada Mission in Afghanistan 7

3) [redacted] Interception [redacted] 9

4) Interception Activities [redacted] 10

5) [redacted] 12

6) CSE Interception Activities [redacted] 14

PART II: 2011-12 INFORMATION TECHNOLOGY SECURITY (ITS) MINISTERIAL AUTHORIZATION END REPORTS

ITS MA REPORTING REQUIREMENTS 15

1) Protection of Government of Canada Computer Systems and Networks: Cyber Defence Operations (CDO) 16

Annex:

1) The 2011-2012 National SIGINT Priorities List 19

PART I

CSEC SIGNALS INTELLIGENCE MINISTERIAL AUTHORIZATION END REPORTS

(For the period between 1 December 2011 to 30 November 2012)

REPORTING REQUIREMENTS

REQUIRED REPORTING: Following the expiration of the 2011-12 SIGINT MAs, 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.

SIGNIFICANT ISSUE REPORTING: Ministerial Authorizations require that CSEC report serious issues that arise in the implementation of Ministerial Authorizations to the Minister of National Defence. Significant issues include but are not limited to a sustained substantial decrease in the value of a source of foreign intelligence, or any sustained major increase in the number of recognized private communications or solicitor-client communications intercepted pursuant to the Ministerial Authorization in question.

SUPPLEMENTAL INFORMATION: While not required by Ministerial Authorization, CSEC is including the number of private communications destroyed and the number of solicitor-client communications deleted for each of the respective SIGINT MAs in question.

DYNAMIC NATURE OF CSEC DATABASE INFORMATION: CSEC analysts may alter the annotations or markings associated with communications data residing in CSEC databases over time. These changes are normal and unavoidable as CSEC continually reassesses data as new information about it becomes available.

For example, this means communications data recognized as a "private communication" at one time may be reassessed in light of new information obtained, and no longer be deemed a private communication, and vice versa. This can produce minor variations in the number of private communications in CSEC databases from one reporting period to another. The metrics provided in this end report accurately reflects the content of CSEC data repositories at the time the report was written.

1. [redacted] INTERCEPTION [redacted]

CSEC collected [redacted] communications under the [redacted] program during the 2011-12 reporting period.

MA Required Reporting:

i) The number of recognized private communications intercepted that CSEC used or retained: [redacted]

Supplemental:
- [redacted] private communications were intercepted through [redacted] collection activities during the 2011-12 reporting period.
- [redacted] intercepted private communications were destroyed because they were not deemed essential to international affairs, defence or security.
- All recognized private communications intercepted under the [redacted] program are accounted for.

ii) The number of recognized solicitor-client communications intercepted that CSEC used or retained: [redacted]

Supplemental:
- [redacted] solicitor-client communications were intercepted through [redacted] collection activities during the 2011-12 reporting period.
- [redacted] intercepted solicitor-client communications were destroyed since they were not deemed essential to international affairs, defence or security.
- [redacted] recognized solicitor-client communications intercepted under the [redacted] program are accounted for.

iii) The number of intelligence reports CSEC produced from the information derived from private communications intercepted pursuant to this MA: [redacted]

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

Foreign Intelligence Value - All communications collected under this program were derived from selection criteria directed at Foreign Intelligence targets approved in accordance with the National SIGINT Priorities list (NSPL). CSEC NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the Ministerial Directive on Intelligence Priorities for Fiscal Year 2011-12.

[redacted] of the [redacted] intelligence reports issued by CSEC/CFIOG were based in whole or in part on intercepted private communications. [redacted] of the [redacted] reports were deemed "exceptional", and [redacted] more were flagged as having "satisfied an intelligence requirement" for one or more of CSEC's clients.

Of the [redacted] private communications retained, [redacted] were used in [redacted] foreign intelligence reports, all of which addressed NSPL priorities. [redacted] of the [redacted] private communications met criteria for determining essentiality for international affairs, defence or security, and were retained for future use.

Supplemental Reporting:

CSEC/CFIOG issued [redacted] foreign intelligence reports based on information derived in whole or in part from [redacted] collection. The reports covered [redacted] all of which directly supported the Government of Canada's intelligence priorities for 2011-12.

CSEC's SIGINT allies issued an additional [redacted] foreign intelligence reports derived from CSEC [redacted] collection. The sharing of Canadian SIGINT collection facilitates CSEC's participation in, and access to, intelligence production [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, Public Safety Canada, the Department of National Defence, and the Canada Border Services Agency.

SIGNIFICANT ISSUE: [redacted] COLLECTION TRENDS

The [redacted] communications collected under the CSEC [redacted] collection program during 2011-12 represent an increase of [redacted] over the [redacted] communications collected during the previous 2010-11 reporting period. At the same time, the number of private communications intercepted through CSEC [redacted] collection activities fell from [redacted] in 2010-11 to [redacted] in 2011-12, representing a [redacted] decrease in private communications intercepted under this program over the past year.

Collectively, these changes reflect significant success in CSEC efforts to increase the quantity and relevance of foreign intelligence communications acquired through [redacted] collection activities while simultaneously reducing incidental collection of private communications that are not relevant to CSEC's foreign intelligence mandate.

This success was achieved through the establishment of a new CSEC [redacted] collection program called [redacted] which became operational in May of 2012. [redacted] was launched in support of CSEC's Strategy 2015, whose goals include the expansion of [redacted] collection to include [redacted] has advanced this 2015 goal.

When the program was activated, CSEC initially encountered a larger number and a wider range of complex communications data than originally expected. This led to a temporary spike in collection of incidental communications data (communications data that does not have foreign intelligence value) under the program, and this spike included private communications.

Upon recognition of this issue, CSEC temporarily suspended [redacted] collection first in [redacted] and again in [redacted] in order to develop and test solutions to reduce incidental collection. This testing continued throughout [redacted] and a technical solution that addressed the problem was deployed to all [redacted] by the end of that month. All CSEC [redacted] collection activities recommenced on [redacted] 2012.

More detailed information on this incident and the CSEC response is available upon request.

2. INTERCEPTION ACTIVITIES CONDUCTED IN SUPPORT OF THE GOVERNMENT OF CANADA MISSION IN AFGHANISTAN

CSEC collected [redacted] communications in Support of the Government of Canada Mission in Afghanistan during the 2011-12 reporting period. [redacted]

MA Required Reporting:

i) The number of recognized private communications intercepted that CSEC used or retained: [redacted]

ii) The number of recognized solicitor-client communications intercepted that CSEC used or retained: **0**

iii) The number of intelligence reports CSEC produced from the information derived from private communications intercepted pursuant to these MAs: [redacted]

iv) The foreign intelligence value of these reports, as they relate to international affairs, defence or security: [redacted]

Foreign Intelligence Value – All communications collected under this Ministerial Authorization were derived from selection criteria directed at Foreign Intelligence targets approved in accordance with the National SIGINT Priorities list (NSPL – see Annex). CSEC NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the 2011-12 Ministerial Directive on Intelligence Priorities.

Supplemental Reporting:

CSEC/CFIOG produced [redacted] foreign intelligence reports, based in whole or in part on information derived from the [redacted] reports) and [redacted] report) collection sites. The reports covered a variety of issues supporting Canadian [redacted] and were shown to CSEC clients in [redacted] Government of Canada departments and agencies including the Privy Council Office, the Department of National Defence, the Department of Foreign Affairs and International Trade, the Canadian Security and Intelligence Service, the Canada Border Services Agency, and the Intelligence Assessment Secretariat. [redacted] of the aforementioned foreign intelligence reports were based on intercepted private communications .

During the review period, a total of [redacted] communications were collected under the [redacted] program and [redacted] were collected under [redacted] for a total of [redacted] communications. [redacted] of these communications were recognized as "private communications".

During the same timeframe, CSEC's SIGINT allies (Australia's Defence Signals Directorate (DSD), the U.K's Government Communications Headquarters (GCHQ) and the U.S. National

Security Agency (NSA)) issued [redacted] FI reports derived in whole or in part from communications collected [redacted]

[redacted] and [redacted] were both in operation during the review period. However, operational responsibility for [redacted] and only [redacted] remained in operation under this MA until the conclusion of the review period.

3. [redacted] INTERCEPTION [redacted]

CSEC collected [redacted] communications under the [redacted] program during the 2011-12 reporting period. [redacted]

MA Required Reporting:

i) The number of recognized private communications intercepted that CSEC used or retained: [redacted]

ii) The number of recognized solicitor-client communications intercepted that CSEC used or retained: [redacted]

iii) The number of intelligence reports CSEC produced from the information derived from private communications intercepted pursuant to these MAs: [redacted]

iv) The foreign intelligence value of these reports, as they relate to international affairs, defence or security: [redacted]

Foreign Intelligence Value – All communications collected under this Ministerial Authorization were derived from selection criteria directed at foreign intelligence targets approved in accordance with the National SIGINT Priorities list (NSPL – see Annex). CSEC NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the 2011-12 Ministerial Directive on Intelligence Priorities.

Supplemental Reporting:

CSEC/CFIOG [redacted] foreign intelligence (FI) reports based on information derived from Canadian [redacted] collection during the review period. Among CSEC's SIGINT allies, GCHQ and the NSA issued [redacted] reports based in whole or in part on Canadian [redacted] collection. [redacted]

4. INTERCEPTION ACTIVITIES [redacted]

CSEC collected [redacted] communications under the [redacted] program during the 2011-12 reporting period. [redacted]

MA Required Reporting:

i) The number of recognized private communications intercepted that CSEC used or retained: [redacted]

ii) The number of recognized solicitor-client communications intercepted that CSEC used or retained: [redacted]

iii) The number of intelligence reports CSEC produced from the information derived from private communications intercepted pursuant to these MAs: [redacted]

iv) The foreign intelligence value of these reports, as they relate to international affairs, defence or security: [redacted]

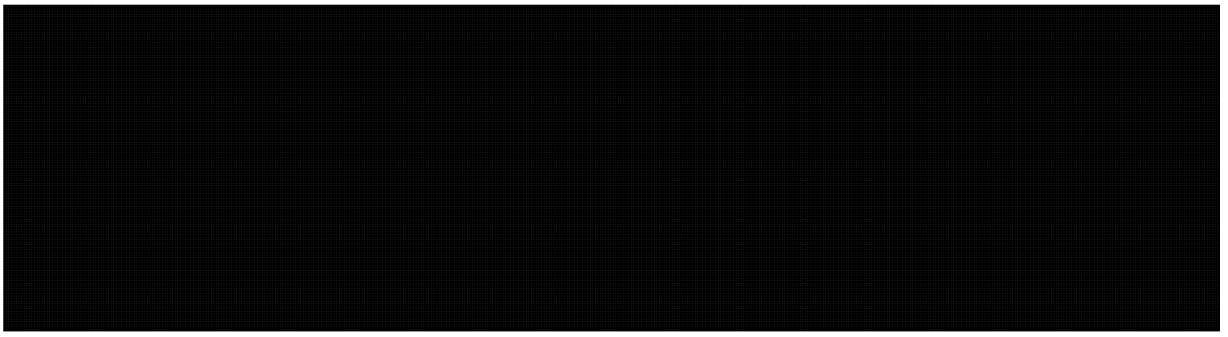
Foreign Intelligence Value – All communications collected under this program were derived from selection criteria directed at Foreign Intelligence targets approved in accordance with the National SIGINT Priorities list (NSPL – see Annex). CSEC NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the 2011-12 Ministerial Directive on Intelligence Priorities.

Supplemental Reporting:

CSEC/CFIOG issued [redacted] foreign intelligence reports based in whole or in part on collection from [redacted] and [redacted] These reports covered [redacted] issues and were viewed by CSEC clients in [redacted] government departments or agencies. This reporting was of particular interest to the Privy Council Office, the Department of Foreign Affairs and International Trade, the Canadian Security Intelligence Service, and the Department of National Defence.

During the same timeframe, CSEC's SIGINT ally, the NSA, issued [redacted] foreign intelligence reports derived from [redacted] reports), [redacted] reports), and [redacted] report). These reports related [redacted]

A new [redacted]



5. [redacted]

CSEC collected [redacted] communications transmitted on [redacted] collected under the [redacted] program during the 2011-12 reporting period. [redacted]

MA Required Reporting:

i) The number of recognized private communications intercepted that CSEC used or retained: [redacted]

ii) The number of recognized solicitor-client communications intercepted that CSEC used or retained: [redacted]

iii) The number of intelligence reports CSEC produced from the information derived from private communications intercepted pursuant to these MAs: [redacted]

iv) The foreign intelligence value of these reports, as they relate to international affairs, defence or security: [redacted]

Foreign Intelligence Value – All communications collected under this Ministerial Authorization were derived from selection criteria directed at Foreign Intelligence targets approved in accordance with the National SIGINT Priorities list (NSPL – see Annex). CSEC NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the 2011-12 Ministerial Directive on Intelligence Priorities.

Supplemental Reporting:

CSEC/CFIOG issued [redacted] foreign intelligence reports based in whole or in part on information derived from [redacted] collection. [redacted] per cent of the reports were derived from a [redacted] operation [redacted] per cent.

CSEC's SIGINT allies (NSA, GCHQ, DSD, and Government Communications Security Bureau) issued [redacted] foreign intelligence reports derived in whole or in part from Canadian [redacted] collection. The reports covered a number of [redacted]

This reporting was viewed by clients in twenty-seven 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, Public Safety Canada, and the Canada Border Services Agency.

6. CSEC INTERCEPTION ACTIVITIES [redacted]

[redacted] had not yet commenced at the [redacted] site during the 2011-12 reporting period. No end product reports were issued during the review period, as [redacted]

Required Reporting:

i) The number of recognized private communications intercepted that CSEC used or retained: [redacted]

ii) The number of recognized solicitor-client communications intercepted that CSEC used or retained: [redacted]

iii) The number of intelligence reports CSEC produced from the information derived from private communications intercepted pursuant to these MAs: [redacted]

iv) The foreign intelligence value of these reports, as they relate to international affairs, defence or security: [redacted]

Supplemental Reporting:

During the reporting period, CSEC continued development and preparation [redacted] This included changes to [redacted] to support collection activities.

[redacted]

PART II

CSEC INFORMATION TECHNOLOGY SECURITY (ITS) MINISTERIAL AUTHORIZATION END REPORTS

(For the period between 1 December 2011 to 30 November 2012)

REPORTING REQUIREMENTS

REQUIRED REPORTING:

Following the expiration of the 2011-12 ITS MA, CSEC is required to report to the Minister of National Defence on:

i) A per federal institution basis, 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.

DYNAMIC NATURE OF CSEC DATABASE INFORMATION: CSEC analysis may alter the tagging of some communications data residing in CSEC databases over time. These changes are normal and unavoidable as CSEC continually reassesses data as new information about it becomes available following collection or from deeper analysis.

For example, this means communications data identified as "private" at one time may be reassessed in light of new information and be deemed "foreign", and vice versa. This can produce minor variations in the number of private communications residing in CSEC databases from one reporting period to another. The metrics provided in this end report accurately reflect CSEC's best assessment of the nature and content of CSEC data repositories at the time the assessment was conducted.

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

CSEC processed approximately [redacted] or [redacted] of communications data under the CDO program during the 2011-12 reporting period.[1]

MA Required Reporting:

The number of private communications that CSEC used or retained pursuant to the 2011-12 MA on per federal institution basis:

i) During protection activities carried out at [redacted]

ii) During protection activities carried out at the [redacted]

iii) During protection activities carried out at the [redacted]

iv) During protection activities carried out at [redacted]

The total number of private communications that CSEC used or retained pursuant to the 2011-12 MA: [redacted]

Supplemental Reporting:

Established in 2009, CSEC's Cyber Threat Evaluation Center (CTEC), supports *Canada's Cyber Security Strategy* by monitoring cyber threats to Government of Canada networks and providing incident response. Over the course of the 2011-12 reporting period, CTEC remained operationally focused on developing new capabilities to detect and guard against a variety of cyber threats with the goal of increasing the security posture of the Government of Canada. An [redacted] in protection activities and the development of new detection and analysis tools reflect the [redacted] in CSEC's ITS cyber defence activity and reporting levels.

CTEC detected [redacted] network compromises which included [redacted] and produced a total of [redacted] reports based on [redacted] incidents (note that one report can include several incidents) from cyber defence operations under this Ministerial Authorization. CTEC cyber defence reporting includes alerts, and analysis of current or potential compromises, proactive cyber security best practices based on past compromises, time sensitive mitigation guidance and in-depth analysis of key cyber threat actors, applied tradecraft and methodologies.

These reports provide a clear picture of the impact of cyber threats to the Government of Canada. They were distributed to federal institutions for mitigation and awareness, Second

[1] This quantity of communications data is equivalent to the contents of [redacted]

Parties for threat analysis sharing programs that benefit Canada, and to CSEC's SIGINT program to enhance targeting of foreign cyber threats.

[redacted] of the private communications used and retained during this MA period involved attachments containing malicious code, or a seemingly legitimate web link to a site hosting malicious code intended to harm Government of Canada computer systems or networks. 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.

SIGNIFICANT ISSUE: ADJUSTMENT OF 2010-11 ITS MINISTERIAL AUTHORIZATION END REPORT

Given the large volume of communications data processed by CSEC in the course of its cyber defence operations, CSEC must rely on computer systems and programs to identify, categorize and manage the data collected to support these activities. In January 2013, CSEC analysts discovered an error in software relied upon to count private communications used or retained by CSEC in the course of cyber defence activities conducted under Ministerial Authorization.

This led CSEC to under-report [redacted] private communications used or retained in cyber defence operations in the 2010-11 Year End Report to the Minister. The error has been corrected, and the verified total number of private communications used or retained by CSEC under the 2010-11 Cyber Defence Operations Ministerial Authorization was [redacted] as opposed to [redacted]

Nature of the Error: In order to manage communications data residing within cyber defence databases, automated programs assign an identity to communications data within the database. This identifying information is critical to the functioning of the rest of the system, since whether a communication is identified as "MA-related" or "non-MA-related" will alter how the system processes and accounts for that data.

The error that led to the 2010-11 undercount of private communications resulted from a coding error in the software that is relied upon to assign identities to communications data as it enters key cyber defence systems. This error resulted in [redacted] MA-related private communications being mischaracterized by that program as unrelated to communications data collected under Ministerial Authorization, and accordingly, they were not included in the 2010-11 MA end-reporting to the Minister.

Resolution: Upon recognition of this significant issue, CSEC cyber defence analysts engaged appropriate management, policy, and legal stakeholders to understand and develop solutions to the problem. Technical solutions have been developed, and the coding error responsible for the undercount has been addressed. CSEC has manually verified its cyber defence databases to ensure the issue has been addressed.

Privacy Impact: Under the ITS cyber defence program, private communications that are identified as non-MA related are handled with more safeguards than those that are MA-related. The sharing of private communications not obtained under MA is in accordance with

Criminal Code provisions, which are more restrictive than the sharing provisions for private communications obtained under MA. CSEC assesses that there has been no privacy impact as a consequence of this incident.

More detailed reports on this incident and the CSEC response are available upon request.

ANNEX: The 2011-2012 National SIGINT Priorities List

NATIONAL SIGINT PRIORITIES LIST (2011-12) Version – 11.xx CSEC (e)		
Tier	Standing Issue	[redacted]
0	[redacted]	
1		
2		

[redacted]

[redacted]

[redacted]

NATIONAL SIGINT PRIORITIES LIST (2011-12)

Version – 11. xx CSEC (e)

Tier	Standing Issue	[redacted]
3	[redacted]	
4