Summary authorized, see Annex A.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

TOP SECRET//SI//CEO
CERRID#9852524
ECT# 14-7616

COMMUNICATIONS SECURITY ESTABLISHMENT (CSE)

MINISTERIAL AUTHORIZATION YEAR END REPORT

2012-2013

Canada

COMMUNICATIONS SECURTY ESTABLISHMENT MINISTERIAL AUTHORIZATION (MA) YEAR END REPORT

PART I: 2012-13 SIGNALS INTELLIGENCE (SIGINT) MINISTERIAL AUTHORIZATION END REPORTS

SIGINT MA REPORTING REQUIREMENTS 3

1) [redacted] Collection Activities 5

2) [redacted] Collection Activities 7

3) [redacted] Collection Activities 9

PART II: 2012-13 INFORMATION TECHNOLOGY SECURITY (ITS) MINISTERIAL AUTHORIZATION END REPORTS

ITS MA REPORTING REQUIREMENTS 11

1) Cyber Defence Activities 12

Annex:

A. 2012-2013 Total Collection/Interception Statistics 14

B. The 2012-2013 National SIGINT Priorities List 15

PART I

CSE SIGNALS INTELLIGENCE MINISTERIAL AUTHORIZATION YEAR END REPORT

(For the period between 1 December 2012 to 30 November 2013)

REPORTING REQUIREMENTS

REQUIRED REPORTING: Following the expiration of the 2012-13 SIGINT MAs, CSE 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: The SIGINT MAs require that CSE report serious issues that arise in the implementation of MAs 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 MA in question.

There are no significant issues to report for SIGINT MAs during the 2012-13 reporting period.

SUPPLEMENTAL INFORMATION: While not required by MA, CSE 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. CSE has also provided information on the MA rationalization; and improved reporting metrics for the 2012-13 reporting period.

Ministerial Authorization Rationalization

CSE rationalized the SIGINT MAs for the 2012–2013 reporting period to make clear that the MAs apply to classes of activities rather than [redacted] Since MAs are not program approval mechanisms, the MAs have been consolidated according to classes of activities. This better aligns with the approval process outlined in part V.1 of the *National Defence Act*. The MA request memoranda for 2012–2013 were also restructured in order to better describe how mandated classes of activities risk interception of private communications and how these risks are mitigated.

As a result of this rationalization, CSE now conducts three distinct classes of SIGINT collection activities under Ministerial authority: [redacted] collection (which includes the same class of activities included the 2011-2012 MAs for [redacted] and for interception activities conducted in support of the Government of Canada mission in Afghanistan); [redacted] collection (which includes the same class of activities included in the 2011-2012 MAs for [redacted] and [redacted] collection.

Improved Reporting Metrics

In previous years, the number of collected communications reported by CSE as part of the annual review of SIGINT MAs and intercepted PCs was based on the [redacted]

During the 2012–2013 reporting period, CSE began reporting the volume of communications as the [redacted] Essentially, CSE now has [redacted] It is important to note that since a communication [redacted] communications during the 2012-2013 reporting period [redacted]

As a result of this [redacted] methodology, a direct comparison to the previous reporting period has not been provided. Should a direct comparison to the previous reporting period be requested, it will be provided using the former reporting methodology. However, a direct comparison between reporting periods will be provided in future MA Year End Reports.

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

For example, this means that communications data recognized as a "private communication" at one time could be deemed as essential; however, based on new information obtained, that same data could be deemed as non-essential and subsequently deleted. This can produce minor variations in the number of private communications in CSE databases from one reporting period to another. The metrics provided in this end report accurately reflects the content of CSE data repositories at the time the report was written.

1. [redacted] COLLECTION ACTIVITIES

CSE collected [redacted] communications under the [redacted] Collection Activities program during the 2012-13 reporting period.

MA Required Reporting:

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

Supplemental:
- [redacted] private communications were intercepted through [redacted] collection activities during the 2012-13 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 CSE used or retained: **0**

Supplemental:
- [redacted] solicitor-client communications were intercepted through [redacted] collection activities during the 2012-13 reporting period.
- [redacted] intercepted solicitor-client communications were destroyed since they were not deemed essential to international affairs, defence or security.
- All recognized solicitor-client communications intercepted under the [redacted] program are accounted for.

iii) The number of intelligence reports CSE 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 - see Annex). CSE NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the Ministerial Directive on Government of Canada Intelligence Priorities for Fiscal Year 2012-13.

[redacted] of the [redacted] intelligence reports issued by CSE/Canadian Forces Information Operations Group (CFIOG) were based in whole or in part on intercepted private communications. [redacted] of the [redacted] reports were deemed "exceptional"; [redacted] "satisfied an intelligence requirement" for one or more of CSE's clients; and [redacted] provided actionable intelligence.

Of the [redacted] private communications used or retained, [redacted] were used in the [redacted] foreign intelligence reports, all of which addressed Government of Canada intelligence 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:

CSE/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 2012-13. This reporting was viewed by clients in [redacted] Government of Canada departments and agencies and was of particular interest to the Canadian Security Intelligence Service (CSIS), the Department of Foreign Affairs Trade and Development (DFATD), the Department of National Defence (DND), the Royal Canadian Mounted Police, the Privy Council Office (PCO), and the Canada Border Services Agency.

CSE's SIGINT allies (National Security Agency [NSA], Government Communications Headquarters [GCHQ], Australian Signals Directorate, and Government Communications Security Bureau) issued an additional [redacted] foreign intelligence reports derived from CSE [redacted] collection. The sharing of Canadian SIGINT collection facilitates CSE's participation in, and access to, intelligence production from similar allied programs.

[redacted] continues to be CSE's [redacted] collection asset. Collection from [redacted] supports all major SIGINT requirements of the Government of Canada and its allies, including [redacted] This collection asset ranks among the [redacted] collection assets within the Five-Eyes SIGINT community. Not only is [redacted] a highly valued source of Foreign Intelligence to the GC and its allies, it is also an excellent source of information which directly enables CSE's [redacted] program.

2. [redacted] COLLECTION ACTIVITIES

CSE collected [redacted] communications under the [redacted] Collection Activities program during the 2012-13 reporting period. [redacted]

MA Required Reporting:

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

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

iii) The number of intelligence reports CSE 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 NSPL. CSE NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the Ministerial Directive on Government of Canada Intelligence Priorities for Fiscal Year 2012-13.

Supplemental Reporting:

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

There were [redacted] communications collected under the [redacted] program during the review period from [redacted] of those [redacted] communications were recognized as private communications.

Over the past year, CSE has expanded capabilities in [redacted] This has enhanced reporting on [redacted]

During the reporting period, the [redacted] Following [redacted] Allied and CSE [redacted] have been identified as vital assets in the [redacted] Consequently, CSE's contribution to FI reporting on [redacted] is expected to pick up substantially as [redacted] for a [redacted]

[redacted]

There were [redacted] communications collected under the [redacted] program during the review period. [redacted] of the [redacted] communications were recognized as private communications.

During the review period, CSE continued development of [redacted] capabilities to support [redacted] collection activities [redacted] which commenced or [redacted] Developments included several changes to [redacted] collection activities. Currently, the [redacted]

3. [redacted] COLLECTION ACTIVITIES

CSE collected a total of [redacted] communications under the [redacted] program during the 2012-13 reporting period. [redacted] % ([redacted]) of communications were [redacted] and [redacted] % [redacted] were communications transmitted on [redacted]

MA Required Reporting:

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

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

iii) The number of intelligence reports CSE 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 NSPL. CSE NSPL foreign intelligence priorities are based on the Government of Canada's stated intelligence requirements, as outlined in the Ministerial Directive on Government of Canada Intelligence Priorities for Fiscal Year 2012-13.

Supplemental Reporting:

CSE/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] [redacted] per cent.

CSE's SIGINT allies (NSA, GCHQ, Australian Signals Directorate, 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 PCO, DFATD, CSIS, DND, Public Safety Canada, and the CBSA.

PART II

CSE INFORMATION TECHNOLOGY SECURITY (ITS) MINISTERIAL AUTHORIZATION YEAR END REPORT

(For the period between 1 December 2012 to 30 November 2013)

REPORTING REQUIREMENTS

REQUIRED REPORTING:

Following the expiration of the 2012-13 ITS MA, CSE 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, that contained information that was essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

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

For example, this means that communications data recognized as a "private communication" at one time could be deemed as essential; however, based on new information obtained, that same data could be deemed as non-essential and subsequently deleted. This can produce minor variations in the number of private communications residing in CSE databases from one reporting period to another. The metrics provided in this end report accurately reflect CSE's best assessment of the nature and content of CSE data repositories at the time the assessment was conducted.

1. PROTECTION OF GOVERNMENT OF CANADA COMPUTER SYSTEMS AND NETWORKS: CYBER DEFENCE ACTIVITIES

CSE processed approximately [redacted] of communications data under the Cyber Defence Activities program during the 2012-13 reporting period.[1]

MA Required Reporting:

The number of private communications that CSE used or retained pursuant to the 2012-13 MA on a per federal institution basis:

i) During protection activities carried out at CSE: [redacted]

ii) During protection activities carried out at the Department of Foreign Affairs, Trade and Development: [redacted]

iii) During protection activities carried out at the Department of National Defence: [redacted]

iv) During protection activities carried out at Shared Services Canada (SSC): [redacted]

The total number of private communications that CSE used or retained pursuant to the 2012-13 MA: [redacted]

Supplemental Reporting:

Established in 2009, CSE'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 2012-13 reporting period, CSE remained operationally focused on producing 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.

Cyber threat actors routinely conduct network reconnaissance on Government of Canada networks in order to discover vulnerabilities, which can be exploited to gain access to that network. [redacted]

CSE's increase in protection activities and the development of new detection and analysis tools reflect upon the increase in CSE's ITS cyber defence activity and reporting levels. During the 2012-13 reporting period, CTEC detected [redacted] In addition, activities conducted under this Ministerial Authorization detected [redacted] A total of [redacted] CTEC cyber defence reports were issued

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

based on these discoveries. CTEC reporting includes alerts, analysis of current or potential compromises, proactive cyber security best practices based on past compromises, time sensitive mitigation, and in-depth analysis of key cyber threat actors, applied tradecraft and methodologies.

These reports contribute to building cyber threat awareness and its impact on the Government of Canada's cyber security posture. Reports were distributed to federal institutions for mitigation and awareness, Five-Eye partners for threat analysis sharing programs that benefit Canada, and to CSE's SIGINT program to enhance targeting of foreign cyber threats.

All of the private communications used and retained during this MA period involved attachments containing malicious code, or seemingly legitimate web links to a site hosting malicious code intended to harm Government of Canada computer systems or networks. CSE notes that the number of used or retained private communications referenced above constitutes a minute fraction of the vast volume of data monitored by CSE under this MA in the course of protecting Government of Canada systems and networks.

Annex A: 2012 – 2013 Total Collection/Interception Statistics

Mandate	Total Collection	Total PC (private communications) Intercepted	Total PC Intercepted that CSEC used or retained
Part A (Foreign Signals Intelligence Collection - SIGINT)	[redacted] communications	[redacted]% of total collected)	[redacted]% of PCs intercepted, and [redacted]% of total collected)
Part B (Cyber Defence - ITS)	[redacted] of communications data	[redacted]	[redacted]
Total PCs that CSEC used or retained pursuant to the 2012-13 MAs			[redacted]

*IT Security Cyber Defence Activities under MA transpire on Government of Canada Computer systems and networks. It is expected that a large portion of the data collected through these activities will fall within the definition of an intercepted Private Communication.

ANNEX B: The 2012-2013 National SIGINT Priorities List

NATIONAL SIGINT PRIORITIES LIST (2012-13)	
Tier	**Standing Issue**
0	
1	
2