Communications Security Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.

Canada

Commissaire du Centre de la sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

TOP SECRET/COMINT/CEO
(with attachment)

16 October 2007

The Honourable Peter G. MacKay, P.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, Ontario
K1A 0K2

Dear Mr. MacKay:

The purpose of this letter is to advise you of the results of a review by my office of the lawfulness of the activities of CSE's Office of Counter Terrorism in the period from 01 April to 31 July, 2005. The review was undertaken under my general authority articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act* (*NDA*).

By way of background, the Office of Counter Terrorism (OCT) was established in early October 2001 to centralize CSE's signals intelligence (SIGINT) efforts as they relate to threats from international terrorism. The OCT conducts research and analysis of SIGINT data in order to identify terrorist targets and their operational and support networks. The information is shared with Canadian government departments and agencies involved in intelligence and security-related matters, as well as with Canada's four intelligence partners, the UK, USA, Australia and New Zealand.

The review posed a number of questions relating to CSE's authorities and policies and procedures. Of particular interest was how CSE undertook the handling of the private communications of Canadians. Discussions with OCT managers, supervisors and analysts encompassed the policy and procedures that are observed when a client wants to access the suppressed identity of a Canadian.

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

CSE co-operation with other government clients and foreign agencies was discussed. A number of queries dealt with Government of Canada intelligence requirements and CSE's National SIGINT Priorities List. Subsequent interviews noted how OCT analysts and their managers dealt with the collection, reporting, retention and release of Canadian identities to clients.

In summary, this review found that the activities conducted by the OCT during the period of review were in compliance with the law and CSE policy. OCT personnel interviewed during the course of this review were knowledgeable about the authorities governing their work. That knowledge, however, may be undermined by weaknesses in document management practices that were noted during this review. In that regard, my report makes two recommendations that should enhance the measurement of OCT's accountability for responses to the Government of Canada's intelligence priorities and for the use and retention of private communications and information about Canadians.

As is my practice, I have provided officials at CSE an opportunity to review and comment on this report, prior to finalizing and forwarding it to you. I will continue to monitor the issues raised.

Please let me know if you have any questions or comments.

Yours sincerely,

Charles D. Gonthier

c.c. Mr. John Adams, Chief, CSE ✓
Ms. Margaret Bloodworth, National Security Advisor, PCO
Mr. Robert Fonberg, Deputy Minister, National Defence

TOP SECRET/COMINT/CEO

Review of the activities of CSE's Office of Counter Terrorism (OCT)

16 October 2007

REVIEW OF THE ACTIVITIES OF CSE's OFFICE OF COUNTER TERRORISM (OCT)

I. AUTHORITY

This report was prepared on behalf of the Communications Security Establishment (CSE) Commissioner under his general authority articulated in Part V.1, par. 273.63(2)(a) of the *National Defence Act* (*NDA*).

II. PERIOD OF REVIEW

The period of review was from 01 April to 31 July, 2005.

III. OBJECTIVES

The purpose of this review was to assess the lawfulness of the activities carried out by CSE's Office of Counter Terrorism (OCT).

The objectives of the review were to:

1. identify and describe the origin, mandate and scope of activities of the OCT;
2. identify and examine all related authorities and policies that govern OCT activities;
3. review OCT data collection and reports from the review period to verify that the information was collected, used and retained in compliance with the law; and
4. identify and report on any other issue of concern that might impact on the ability of CSE to conduct its activities lawfully and to safeguard the privacy of Canadians.

IV. METHODOLOGY

The review commenced with a briefing from the A/Director of [redacted] Group (responsible for the OCT), with subsequent briefings from the OCT Production Manager (PM) and supervisory and analytical personnel. These briefings assisted in establishing the history, mandate and methodology of OCT while clarifying CSE's mandate under par. 273.64 (1)(a) of the *NDA*. Relevant documentation was examined, including OCT-related policy directives, as well as all reporting and intercepts produced by OCT during this period.

The review posed a number of questions relating to CSE's authorities and policies and procedures. Of particular interest was how CSE undertook the handling of the private communications of Canadians. Discussions with OCT managers, supervisors and analysts encompassed the policy and procedures that are observed when a client wants to access the suppressed identity of a Canadian.

CSE co-operation with other government clients and foreign agencies was discussed. A number of queries dealt with GoC intelligence requirements and the National SIGINT Priorities List (NSPL). Subsequent interviews noted how OCT analysts and their managers dealt with the collection, reporting, retention and release of Canadian identities to clients.

V. REVIEW FINDINGS

Objective 1: Origin, Mandate and Scope of Activities of the OCT

Origin

Countering the threat posed by terrorism, in all its varied manifestations, has been and will continue to be a source of concern to the Government of Canada and its allies.

Prior to the 11 September 2001 attacks (9/11), CSE did not have an established counterterrorism effort in place. In the immediate aftermath of 9/11, an informal cell was brought together to address CSE's expanded responsibilities in the wake of the attacks. The Office of Counter Terrorism (OCT) was formally established in early October 2001 to centralize CSE's signals intelligence (SIGINT) efforts as they relate to threats from international terrorism.

Mandate and Scope of Activities

All of the mandated activities of OCT in the period under review came under the authority of par. 273.64(1)(a) of the *NDA*, known as mandate (a), which enables CSE "to acquire and use information from the global information infrastructure (GII) for the purpose of providing foreign intelligence, in accordance with GoC intelligence priorities." Under this mandate, the OCT is responsible for conducting research and analysis on data drawn from the intelligence repository. This research and analysis is aimed at identifying terrorist targets and their operational and support networks. The information is shared with Canadian departments and agencies involved in intelligence and security-related matters, as well as with Canada's four intelligence partners, the UK, USA, Australia and New Zealand, known as the second parties.[1] OCT also responds to requests for information (RFIs) from Canadian departments and agencies, and from Canada's four allies. To facilitate these and other departmental and agency intelligence requirements, CSE has in place a Client Relations Officers (CROs) program, which is described in the OCSEC review report

[1] CSE's cooperation with [redacted] is described below, beginning on page 5.

entitled "Role of the CSE Client Relations Officers and the Operational Policy Section (D2) in the Release of Canadian Identities," dated 30 March 2007.

Objective 2: OCT Authorities and Policies

We identified and examined the following authorities and policies that govern OCT's activities:

- Part V.1 of the *NDA*;
- GoC Foreign Intelligence Priorities 2004-2005;
- Ministerial Directive on the Privacy of Canadians;
- Ministerial Directive on Accountability Framework;
- Policies and Procedures of CSE, principally OPS-1, "Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities", and OPS-1-1 "Release of Suppressed Information;" and
- UKUSA Agreement on SIGINT Co-operation, signed on 1 November 1945, between Canada, the UK, USA, New Zealand and Australia.[2]

More details about these authorities and policies and OCT's compliance with them are provided below.

Objective 3: Compliance with Authorities and Policies

It was the expectation of this review that OCT information would be collected, used and retained in compliance with the following authorities:

- *NDA*, par. 273.64(1)(a), 273.64 (2)(a) and 273.64(2)(b);
- CSE Policy and Procedures, including OPS-1 ("Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities") and OPS-1-1 ("Procedures for the Release of Suppressed Information from SIGINT Reports"); and
- Government of Canada (GoC) Intelligence Priorities.

Requests for Information from Government of Canada Clients

OCT analysts are tasked to review both open and classified databases to produce intelligence reports. Once approved according to CSE policy (i.e., OPS-1, S.6.10, "Report Release Authorities"), the reports are formally distributed to the GoC clients that have submitted requests for intelligence on these topics. The most important consumers of OCT reports are the Canadian Security Intelligence Service (CSIS), the Department of National Defence (DND), Foreign Affairs Canada (FAC) and the Canadian Border Services Agency (CBSA).[3] It is important to note here that

[2] This agreement is an issue of concern; see Annex A.
[3] A complete list of OCT client departments is provided in Annex B.

OCT's foreign targets and their relative priorities continually shift in response to constantly evolving GoC requirements, which, as previously noted, are reflected in CSE's National SIGINT Priorities List (NSPL).

As one example, a Canadian department or agency might submit an RFI pertaining to foreign phone and/or fax numbers to CSE's Client Relations Officer. CSE will then ensure that the RFI conforms with CSE's authorities and can be fulfilled in accordance with the government's foreign intelligence priorities and its capabilities (in this case related to terrorism). Once this assessment is completed, the request is provided to OCT so that it can conduct a comprehensive search of the CSE data banks. If necessary, CSE can forward the RFI to its allies for a search of their respective data banks.

During the period of review a total of [redacted] RFIs were sent to CSE. Of these, [redacted] were counterterrorist-related under mandate (a) and were responded to as follows:

Agency	Total	Unassigned	FYI/No Action Taken	Declined
RCMP	[redacted]			
CSIS				
CBSA				

"Unassigned" refers to RFIs that the Director General Intelligence (DGI) did not assign to any analyst for reasons such as workload or other intelligence priorities. "Declined" refers to those requests not actioned due to legal or policy concerns, or because they were not listed on the NSPL. Of the [redacted] OCT-related RFIs, [redacted] from CSIS were refused because DGI management determined that they could not be actioned under mandate (a).[4] There were no follow-up requests from CSIS to proceed under the (c) mandate.[5]

If there is no record of a target's telephone/fax number, the number is first entered into the target knowledge base and then incorporated into the CSE SIGINT selector dictionary for future reference, collection and reporting purposes. This ensures that telephone/fax numbers of intelligence and security interest are retained for investigative/analytical follow-up. It was our expectation that OCT would take action on an RFI only if the numbers provided related to an identifiable foreign entity that resides outside Canada, and the request fell within the GoC foreign intelligence collection program relating to the counterterrorism mandate of OCT. In other words, we expected that OCT would comply with both mandate (a) and with the *NDA*, par. 273.64(2)(a), which provides that mandate (a) activities "shall not be directed at Canadians or any person in Canada."

[4] These numbers do not include client or CRO requests that were directly input into [redacted] a system that facilitates the production and dissemination of SIGINT to clients.

IRRELEVANT

Finding:

It is our assessment that the RFIs reviewed were in compliance with NDA, *par. 273.64(1)(a) and 273.64(2)(a) and OPS policy and procedures.*

Requests for Information from [redacted]

To fulfil the mandate of OCT in providing foreign intelligence in response to GoC client requirements related to terrorism, terrorist threats and organizations, OCT must also collaborate with its Second Party partners, [redacted]

[redacted] uses the [redacted] to share SIGINT on counterterrorism up to and including the Top Secret/Special Intelligence (TS/SI) level. After 9/11, the [redacted] expanded their sharing from traditional military intelligence targets to include counterterrorism and force protection operations. The [redacted] is of interest because [redacted] to communications and metadata [redacted] OCT sharing is limited primarily to selectors, some trace checks, and selected reporting. In discussions with CSE, it was underlined that there would be some limits on the sharing of methodologies, such as not divulging details on how OCT approaches issues from a technical stand point. The objective of sharing with [redacted] to CSE's clients.

OCT runs trace checks from second parties in CSE's [redacted] collection and then scrubs any sensitive data. Moreover, trace checks are only done on Digital Network Intelligence (DNI) data, which is [redacted] This is considered to be under the umbrella of technical methodology that is generally shared [redacted] selectors or other related reporting. As required, OCT would obtain permission to share data that comes from other agencies, such as CSIS.

To facilitate these exchanges with the second parties, OCT [redacted]

No private communications or details about Canadians were shared [redacted] during this period of review.

Suppressing and Releasing Canadian Identities

The foreign intelligence reports that follow from this research and analysis will, on occasion, include Canadian identities. For this reason, there is the expectation that OCT will comply with *NDA* par. 273.64(2)(b), which provides that mandate (a) activities "shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information". To maintain privacy, the identities of Canadians are "suppressed" by CSE. These identities are substituted in OCT reports by a generic descriptor such as "a Canadian individual" or "a Canadian firm". In the wake of the reporting, should a client require the identity for investigative/analytical purposes, a formal request outlining the reasons behind the submission would then be forwarded to CSE.

All requests must be accompanied by sufficient justification, in accordance with procedures set out in CSE policy OPS-1-1. Of the [redacted] intelligence reports generated by OCT in the period under review, [redacted] were the subjects of Requests for Release of Suppressed Information. All [redacted] CSIS requests were reviewed and found to be appropriately documented and released in accordance with CSE policy OPS-1-1. These [redacted] reports were derived in part from sources other than CSE, or reflected traffic containing information about Canadians, but were not based on a private communications. ([redacted] from Canadian collection IRRELEV IRRELEVANT

[redacted] other reports were generated from private communications intercepted by CSE. The information derived from the private communication was verified as essential to international affairs, defence and security as per *NDA*, par. 273.65(2)(d). [redacted] of these reports was the subject of a Request for Release. When queried, OCT suggested that CSIS might not have required the suppressed information because CSIS likely had more pertinent/contextual information.

We note that CSE policy concerning requests for suppressed information has recently been updated, and such requests must now be approved by the Manager of Operational Policy (D2). D2 has instituted a double sign–off requirement for the release of suppressed information. This means that all requests for release are reviewed by the Manager of Operational Policy, or his/her designated replacement. D2 has also instituted a formal audit, on a regular basis (quarterly), for all releases of suppressed information.

The requests are now transmitted electronically, including those from the second parties. The "window" in CSE's [redacted] database that includes Canadian identities restricts access to the report's author or the contributor(s) to the report, the reviewer (e.g. Team Leader) and the manager(s) who authorizes the release of a report. We were satisfied that the enhanced approval process for the release of suppressed information and the restricted access to Canadian identities in the database is consistent with CSE's obligation to protect the privacy of Canadians as per *NDA*, par. 273.64(2)(b).

Once a client has requested and received identities for the suppressed information, CSE procedures (OPS-1-1, S 7.2) state that clients "may retain hard copy in an approved container" for a maximum of [redacted] while "soft copies are to be deleted from all e-mail folders". OCT was asked if it followed up to verify that these messages were retained appropriately and that the soft copies were deleted within the scheduled time limits. OCT advised that it does not, because responding to the policy is the sole responsibility of the receiving department or agency. We were pleased to note that, subsequent to the period of review, a caveat on the "Request for Release of Suppressed Information Form," dated 03 January 2006, advised that the requesting department must handle the material in accordance with the *Access to Information Act* and the *Privacy Act*.

Two recommendations from recent reports by this office are also relevant to this issue, as follows:

- In June 2005, the Commissioner reported to the Minister of National Defence on a review of CSE's [redacted] Recommendation 3 of that report was as follows:

> "to ensure the privacy of Canadians is safeguarded: (i) periodic audits be conducted on SIGINT reports to verify that proper authorities have been obtained for releasing reports based on private communications or containing information about Canadians; and (ii) in accordance with OPS-1-1, 2.6, audits be conducted on activities related to the release of suppressed information (i.e. Canadian identities)."

CSE accepted this recommendation. Under the auspices of the Director General Audit, Evaluation and Ethics (DGAEE), CSE was auditing compliance of reports by the fall of 2005. Another audit, conducted in the Fall of 2006, addressed a directed sample of Director General Intelligence (DGI) reporting. A third audit, conducted from September 2006 to April 2007, focussed in particular on the question of whether the appropriate release authorities were obtained as it relates to the SIGINT End-Product Reporting Audit. As a result of the audits, DGI implemented a process to ensure all necessary authorizations are in place. With the restructuring of Director General Programs (DGP) as of 01 April 2007 and the creation of SIGINT Programs Oversight and Compliance (SPOC) out of [redacted], individuals have been identified to follow up on this issue, and CSE intends to conduct regular audits on reports incorporating suppressed information that has been released.

- Additionally, the Commissioner's March 2007 report on the CSE's client relations officers and release of Canadian identities recommended that CSE include a section of the *Privacy Act* that is the appropriate disclosure authority. CSE sponsored a review following consultations between CSE's Directorate of Legal Services and Justice colleagues from the Information Law and Privacy Section. The result is that the CSE release form will be slightly modified to indicate the authority for the release of personal information (identities).

Finding:

It is our assessment that identities of Canadians were released in compliance with NDA, *par. 273.64(2)(b), and in accordance with the procedures set out in CSE policy OPS-1-1.*

Reports Issued by OCT during the Review Period

We were pleased to note that report release forms were affixed to all of the [redacted] reports. However, a total of [redacted] accompanying release forms did not include the origin of the report (i.e. a private communication from a Canadian source at one end, or from foreign sources at both ends). Moreover, [redacted] reports of the [redacted] had been archived and had to be retrieved manually. The reports themselves were filed by the month in hard copy, with some misfiled. An electronic storage/ retrieval system would facilitate information management and retrieval as well as ensure that report release forms are readily accessible and are appropriately filled out and signed off. There have been numerous previous OCSEC recommendations on this subject. Nevertheless, we believe it is important to reiterate the importance of implementing a computerized system of records management, as described in Recommendation 1 below. This will allow the release authorities and the respective report to be fully recorded, retained and easily retrieved in accordance with OPS-1, S.6.10, "Report Release Authorities".

Recommendation no. 1:

That CSE incorporate into a computerized records management system a mechanism that will, among other benefits, ensure that the Release Form for Security Line Product Reports is duly filled out and signed off.

GoC Intelligence Priorities and the National SIGINT Priorities List (NSPL)

As noted previously, mandate (a) requires that the CSE conduct its foreign intelligence operations "in accordance with Government of Canada intelligence priorities". These foreign intelligence priorities (also known as intelligence requirements—or IRs) are then forwarded by CSE to client departments and agencies for consultations and to refine the targeting of the priorities. The end product is the CSE's National SIGINT Priorities List (NSPL). This is a detailed list of the government's foreign intelligence priorities, which are prioritized 0-4, [redacted] priority. The priorities during the period of review were as follows:[6]

1. [redacted]

[6] These priorities remain current as of June 2007.

2. [redacted]
3. [redacted]
   - [redacted]
   - [redacted]

The NSPL is regularly reviewed and amended to address the evolving foreign intelligence requirements of the Canadian government.

There are a number of procedural steps that CSE follows, beginning from the GoC IR, to the NSPL, to analyst implementation/collection and reporting. This CSE/OCT process uses various mechanisms for identifying foreign targets and networks possibly involved in terrorist operations. Foreign lead information may be derived from GoC clients, other intelligence agencies, open source research, or from their associations with existing targets of interest. Information about each OCT target is entered into a target knowledge base called [redacted] which allows CSE analysts easy access to SIGINT target knowledge, including the ability to uncover any links between different targets. [redacted] contains all information retained about a target, the source of the information and what analysis has been done concerning the target. Analysts must also relate a GoC IR to each of these entries. These GoC IRs can then be matched to the NSPL using [redacted], CSE's SIGINT production and dissemination system. [redacted] links the OCT report to the GoC IR and all pertinent issues are mapped to the NSPL. However, this linkage is not clear to the uninitiated, because it does not directly link to the GoC IR.

One of the objectives of reviewing the reports and intercepts was to examine the private communications of Canadians that were used by OCT during the period of review and to assess their intelligence value in relation to the Government of Canada (GoC) intelligence priorities and the CSE National SIGINT Priorities List (NSPL). It was ascertained that the two reports containing information from the private communications were deemed to be of intelligence import and appropriately contributed to the GoC intelligence requirements and the NSPL.

Finding:

As noted above, OCT issued [redacted] reports during the period under review. This review examined all [redacted] reports, as well as relevant documentation, including OCT targeting procedures. Also as noted, a total of [redacted] of these reports contained suppressed information. The review was advised by CSE that [redacted] of the reports responded to tier [redacted] standing issues and focus areas. (See attached WATCHING BRIEFS and SIGINT PRIORITIES listing, Annex B)

Recommendation no. 2:

That CSE consider establishing a more refined tracking system that will provide a snapshot of how effective CSE SIGINT efforts are in addressing GoC intelligence priorities.

Objective 3: Other Issues

There were no other issues of concern.

VI. CONCLUSIONS

This review found that the activities conducted and reviewed during this period by the OCT during the period of review were in compliance with the law and CSE policy. More specifically:

- **OCT's activities in the period under review were carried out lawfully under the provisions of *NDA*, par. 273.64(1)(a) (mandate (a)).**
- **The requests for information (RFIs) to which OCT responded were in compliance with *NDA*, par. 273.64(1)(a) and 273.64 (2)(a) and OPS policy and procedures.**
- **Identities of Canadians were released in compliance with *NDA*, par. 273.64(2)(b), and in accordance with the procedures set out in CSE policy OPS-1-1.**

OCT personnel interviewed during the course of this review were knowledgeable about the authorities governing their work. That knowledge, however, may be undermined by weaknesses in document management practices that were noted during this review. In that regard, this report makes two recommendations that should enhance the measurement of OCT's accountability for responses to the Government of Canada's intelligence priorities and for the use and retention of private communications and information about Canadians.

ANNEX A

The United Kingdom -United States of America (UKUSA) Agreement and Co-operation with other Foreign Governments

The United Kingdom-United States of America (UKUSA) Agreement, signed in 1945, covers SIGINT co-operation between the five second parties (the USA- National Security Agency (NSA.), Canada- Communications Security Establishment (CSE), United Kingdom-Government Communication Headquarters (GCHQ), Australia- Defence Signals Directorate (DSD) and New Zealand-Government Communications Security Bureau (GCSB)). There were two addendums: one was added in 1949 (CANUSA Agreement) and the second in 1960 (CANUKUS Agreement). While the documents remain the originating manifesto that underscores the continuing co-operation among the signatories, the agreements have never been fully revised or updated to address new technology, contemporary privacy issues or the legal framework that governs the respective signatories. It also does not take into account the new intelligence, political and international security realities that the allies and the global community, must contend with in the 21st century. CSE's response to this issue has been that each member of the UKUSA Agreement respects and works within its own privacy and legal frameworks, and follows its own information handling policies. This situation has been reportedly deemed adequate by CSE as well as other participating members. This issue was highlighted in the OCSEC [redacted] Review of 28 February 2005.

ANNEX B

OCT Clients During Review Period

The clients for OCT reports span a spectrum of Canadian government departments and agencies.

Clients at the following departments received OCT reports in response to queries and standing requirements that are input in [redacted]

Department of National Defence – DND – ([redacted] users)
Foreign Affairs Canada – FAC – ([redacted] users)
Canadian Security Intelligence Service – CSIS – ([redacted] users)
Intelligence Advisory Secretariat – IAS – ([redacted] users)
Privy Council Office – PCO – ([redacted] users)
Public Safety and Emergency Preparedness Canada – PSEPC – ([redacted] users)
Integrated Threat Assessment Centre – ITAC – ([redacted] users)
[redacted] – ([redacted] users)

In addition, the following GoC clients also accessed OCT reports by running their own ad-hoc queries in [redacted]

- CSIS [redacted]
- FAC [redacted]
- DND [redacted]
- [redacted]
- IAS [redacted]
- ITAC [redacted]
- International Trade Canada (ITCAN) [redacted]
- Privy Council Office (PCO) [redacted]
- PSEPC [redacted]
- [redacted]
- [redacted]
- Others [redacted] (This refers to feedback from second parties that is input by CSER via e-mail, and entered into [redacted] for informational purposes)

It should be noted that CSE is in the midst of establishing a process to monitor its clients' use of [redacted] This will be the subject of a future review.