COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

Annual Report

2007-2008

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984
Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096
Website: www.ocsec-bccst.gc.ca

ISBN 978-0-662-48603-9
Cat. No. D95-2008E-PDF

Cover photos: Malak

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.

May 2008

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my 2007–2008 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Charles D. Gonthier

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

This report is dedicated to the memory of

The Right Honourable Antonio Lamer
P.C., C.C., C.D., LL.D., D.U.

1933–2007

TABLE OF CONTENTS

Introduction /1

The Review Environment /2
- House of Commons Subcommittee and Special Senate Committee recommendations on the *Anti-terrorism Act* /2
- Proposed amendments to the *National Defence Act* /3
- Iacobucci Internal Inquiry and the Major Commission of Inquiry /6

The Year in Review /7
- Workplan /7
- Reviews undertaken of the activities of CSEC /9
- Methodology /10
- Overview of 2007–2008 findings /11

2007–2008 Review Highlights /13
- Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) /13
- Review of information technology security activities at a government department /14
- Review of CSEC's activities carried out under a ministerial directive /15
- Review of CSEC's counter-terrorism activities /17
- Review of CSEC's support to CSIS /18
- Reviews underway and planned /19
- Complaints about CSEC activities /20
- Duties under the *Security of Information Act* /20

The Commissioner's Office /20

A Tribute /22

Annex A: Mandate of the Communications Security Establishment Commissioner /23

Annex B: Classified Reports to the Minister, 1996–2008 /25

Annex C: Statement of Expenditures, 2007–2008 /29

Annex D: History of the Office of the Communications Security Establishment Commissioner (OCSEC) /31

Annex E: Role and Mandate of the Communications Security Establishment Canada (CSEC) /33

INTRODUCTION

This is my second annual report as Communications Security Establishment Commissioner, and its publication occurs at the mid-point in my three-year term.

I seek assurance of compliance with the spirit of the law, and not just the letter.

The fact that I am halfway through my first mandate gives me pause for reflection. Like my predecessors, I seek assurance of compliance with the spirit of the law, and not just the letter. In this regard, I am concerned with situations where lack of compliance with the law may arise, and I tailor my recommendations to safeguard against that possibility. If I determine there may not have been compliance with the law, I must of course inform the Minister of National Defence and the Attorney General of Canada.

This leads me to contemplate one of my personal preoccupations—the role of the individual in doing the right thing. In the case of the Communications Security Establishment Canada (CSEC),[1] the people who are doing the work must have more than just technical ability. They must also have a fundamental respect for the rule of law and for democracy, which includes a reasonable expectation of privacy for all Canadians. CSEC's organizational culture must reflect these values, and CSEC must develop and follow policies and procedures that flow from the law and the values.

It is very clear to me that as a result of the terrorist acts of 2001, as well as subsequent terrorist activities, many Canadians continue to live with a heightened sense and level of risk, and there is little likelihood that these will diminish. This places a greater burden on people such as those employed at CSEC, because the government relies upon them to go beyond the mechanical aspects of information collection. They are called upon to reach for information that will support good decision making and thereby protect Canadians, but in a way that safeguards privacy.

[1] The name was changed to Communications Security Establishment Canada effective September 27, 2007, in order to comply with the Government of Canada's Federal Identity Program.

During the past year, I may at times have been critical of certain of CSEC's practices that, in my opinion, could be strengthened. I hold the view, however, that the striking point of the last several months has been the CSEC Chief's handling of an operational issue that came to light at the end of 2006 that had the potential for non-compliance. The Chief informed me about the matter at once, and has kept me apprised on a regular basis of all corrective steps taken. CSEC management's measured response addressed the needs of the organization, and was at the same time respectful of the people who serve in it, while leaving no doubt as regards their obligations.

THE REVIEW ENVIRONMENT

House of Commons Subcommittee and Special Senate Committee recommendations on the *Anti-terrorism Act*

In its Final Report presented to the House of Commons on March 27, 2007, the Subcommittee of the House of Commons reviewing the omnibus *Anti-terrorism Act* made a number of recommendations concerning CSEC and my office, dealing particularly with the legal ambiguities in the provisions allowing for ministerial authorizations. Since the *Anti-terrorism Act* received Royal Assent in December 2001, my predecessors and I have faced a persistent dilemma arising from the amendments this Act introduced to the *National Defence Act*. Particularly troublesome has been the lack of agreement between my office and CSEC concerning the legal advice provided to CSEC by the Department of Justice. At issue is the interpretation given to the provisions relating to ministerial authorizations.

The Subcommittee's Final Report urged government counsel and me to resolve the issues concerning ministerial authorizations. As well, the Subcommittee requested that the Government's response to the Final Report indicate, to the extent possible, what the issues of disagreement are and how they have been resolved. Failing this, the Subcommittee encouraged me to provide these details in my 2007–2008 Annual Report.

The Government issued its response on July 18, 2007. It noted that "CSE is working with Department of Justice officials to address these issues, with a view to bringing forward proposed legislative amendments in due course."[2] One year later, there appears to have been a lack of progress. In the meantime, I wish to respond to the Subcommittee's request and to describe two of my principal recommendations relating to ministerial authorizations.

The Government noted that legislative amendments would be brought forward "in due course". One year later, there appears to have been a lack of progress.

Proposed amendments to the *National Defence Act*

The provision relating to ministerial authorizations issued for the sole purpose of obtaining foreign intelligence reads as follows:

Ministerial authorization

273.65 (1) The Minister may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

Conditions for authorization

(2) The Minister may only issue an authorization under subsection (1) if satisfied that

(a) the interception will be directed at foreign entities located outside Canada;

(b) the information to be obtained could not reasonably be obtained by other means;

[2] *Response of the Government of Canada to the Final Report of the House of Commons Standing Committee on Public Safety and National Security Subcommittee on the review of the* Anti-terrorism Act, p. 20.

(c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and

(d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

[…]

My first principal recommendation concerns the term *activity or class of activities* as it relates to CSEC and to the Commissioner. My predecessors and I have long held the view that a plain reading of the *National Defence Act* supports the interpretation that the interception authorized by the Minister is that of a private communication in relation to an *activity or class of activities* which is targeted or the object of inquiry, and not to a method of collection as contended by CSEC. Therefore, an important amendment would be to clarify the meaning of the term *activity or class of activities*.

My second principal recommendation is to define the terms *intercept* and *interception*, or to provide a reference to the existing definition of *intercept* in the *Criminal Code*. At present, these terms are not defined in the *National Defence Act*. However, they have both legal and operational significance for CSEC.

In the absence of definitions that are universally understood and consistently applied, it is difficult for me to interpret CSEC's legislated authority and to review how it has been applied.

The Special Senate Committee on the *Anti-terrorism Act* also made recommendations relating to ministerial authorizations. Notably, the Committee recommended "that subsections 273.65(2) and (4) of the *National Defence Act* be amended to clarify whether the facts and opinions, which are necessary to satisfy the Minister of National

Defence that all of the preconditions for issuing a written authorization to intercept private communications have been met, should be based on reasonable belief or reasonable suspicion".[3] Clarifying in law the standard to be used remains an issue of interest to my office, and I continue to support making such an amendment to the *National Defence Act*.

In addition, I have made other recommendations to officials at CSEC and at the Department of Justice for amendments that I think would be worthwhile to enact.

In response to another recommendation of the House of Commons' Subcommittee, the Government indicated that it did not intend to modify the *National Defence Act* to specify that my office should review interception activities for compliance with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*. As I pointed out in last year's Annual Report, my office's review methodology has always included an examination of compliance with all relevant laws, including the *Charter* and the *Privacy Act*.

The Subcommittee's Final Report also recommended that the Government proceed with legislation to establish a National Security Committee of Parliamentarians responsible for the review of national security matters, and that this Committee be called upon to conduct a further comprehensive review of the *Anti-terrorism Act* after a fixed period. The Government responded that it has not determined if this is the best way to proceed. However, it went on to note that it "will propose an approach to national security review that will meet the basic objectives set out in the second report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar and is considering options for an enhanced role for Parliamentarians as a key

[3] Special Senate Committee on the *Anti-terrorism Act, Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the* Anti-terrorism Act, February 2007, recommendation 18, p.78.

part of these proposals for an improved national security review framework."[4] As I commented in my report last year, I concur with my predecessor's position that welcomes "the prospect of more active parliamentary review of national security activities," while also noting "challenges such as the composition of the committee and its access to classified information and documents."[5]

Iacobucci Internal Inquiry and the Major Commission of Inquiry

The Honourable Frank Iacobucci is in the process of conducting an internal inquiry into the actions of Canadian officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin. He is to determine, amongst other matters, whether the detention or any mistreatment of these individuals in Syria or Egypt resulted, directly or indirectly, from actions of Canadian officials, particularly in relation to the sharing of information with foreign countries and, if so, whether those actions were deficient in the circumstances.

The Honourable John Major is conducting an inquiry into the investigation of the bombing of Air India Flight 182. In particular, he is to determine whether any changes in practice or legislation are required to prevent the recurrence of similar problems of cooperation between the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) in the investigation of terrorism offences, and to recommend how government should go about establishing a reliable and workable relationship between security intelligence and law enforcement agencies regarding the use of intelligence as evidence in a criminal trial.

I have an interest in the sharing of information about Canadians, particularly when that information is to be shared outside Canada. This is an area that my office continues to examine. In this context, the outcomes of the Iacobucci and Major Commissions may have an impact on security and intelligence agencies, as well as review agencies, including my office.

---

[4] *Supra*, note 2 at p. 25.

[5] Communications Security Establishment Commissioner, *Annual Report 2006–2007*, p. 8.

THE YEAR IN REVIEW

Last year, I referred to the independent management review of the operations of my office, and to recommendations to improve our methodology. These matters have been thoroughly examined, and changes have been incorporated in new operational policies and procedures. My office has been implementing these changes in the conduct of reviews. One of the most notable is a new approach that involves examining processes which are common to several different CSEC activities. As a result, the review function is expected to be more effective in at least two ways: first, by avoiding a certain amount of duplication; and second, by creating a greater and readier understanding of underlying activities at the core of CSEC's mandate. CSEC has been kept informed throughout the process of implementing these changes, and specific issues of methodology that have a direct impact on that organization and on our working relationship have been discussed.

At my request, CSEC provided several briefings to my staff during the past year. Some of the briefings have become annual occurrences, such as those related to policy developments and updates, and also to the implementation of a new information management system. Other briefings have dealt with cyber-threat activities and with certain aspects of cooperation with CSIS. As is standard practice, and at our request, CSEC also provided briefings at the beginning of most reviews initiated during the year.

Workplan

A three-year workplan guides the activities of my office. It is an integral component of the review process as well as being a focal point in the relationship between my office and CSEC. It is updated on a regular basis. Each update involves a re-assessment of the priority of planned and potential review projects and incorporates new information that may have come to our attention. For example, a review that has just been

completed may identify an area outside the scope of that review but which I believe needs to be examined further, perhaps to assess compliance with the law or to ensure the protection of the privacy of Canadians. In my report last year, I listed other criteria that contribute to determining what areas or topics will be included in the workplan. I must, however, always weigh what is reviewed against what is not, and be satisfied to the extent possible that those areas of greater risk to compliance with the law or to privacy are being examined.

CSEC is consulted on the workplan. There are several reasons for this. This is a standard practice in review to ensure that no one area of the organization is unduly burdened. There must be balance between my review mandate and CSEC's operational requirements mandated by the government. Another significant reason is that there is a need to ensure that the scheduling and scope of review projects is reasonable and can be carried out in a timely manner, taking into consideration the resources and mandates of both organizations.

An important initiative agreed upon by both CSEC and my office was to organize a roundtable discussion focussed on the working relationship. The objective was to optimize the review process, which as well means minimizing any adverse impact on the activities of CSEC. The meeting reviewed the business processes of both groups, identified points where improvement was desirable and proposed how to achieve those improvements. A number of issues related to the workplan were also identified and have been implemented. There was general agreement that this type of meeting was useful and served the interests of both organizations to keep open the lines of communication and to ensure that review works as intended.

Reviews undertaken of the activities of CSEC

My general review mandate is set out in paragraph 273.63(2)(a) of the *National Defence Act*.[6] Under subsection 273.65(8) of the Act, I also have an obligation to review and report to the Minister as to whether the activities carried out under a ministerial authorization are authorized.

Ministerial authorizations for foreign intelligence collection are issued under the authority of subsection 273.65(1) of the *National Defence Act*, whereas ministerial authorizations for information technology security activities are issued under subsection 273.65(3) of the Act. My reviews of CSEC's activities conducted under ministerial authorizations are undertaken after the ministerial authorization has expired.

As I noted in my Annual Report last year: "The characteristics of contemporary communications technology mean that the interception of communications by CSE, directed at foreign entities outside Canada, runs the inherent risk of acquiring the private communications of Canadians. It is for this reason that a ministerial authorization is sought for this collection."[7]

The ministerial authorization provisions do not allow CSEC to target Canadian communications. However, "for the sole purpose of obtaining foreign intelligence"[8], the Minister may authorize the interception of private communications of Canadians or persons in Canada as long as the interception was the result of CSEC's targeting a foreign entity located outside Canada. Ministerial authorizations for information technology security activities also authorize the interception of private communications that may be incidentally obtained by CSEC while protecting the systems and networks of a federal government department or agency.

---

[6] Please see Annex A for the text of the relevant sections of the *National Defence Act*.
[7] *Supra*, note 5 at p. 18.
[8] Subsection 273.65(1) of the *National Defence Act*.

Further, when collecting foreign intelligence, CSEC may also incidentally acquire information about Canadians. This information may only be retained if it is assessed as essential to the understanding of the foreign intelligence, and it may be included in foreign intelligence reporting if it is suppressed (i.e., replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC requires federal government departments and agencies to explain their authority to collect this information under their own respective mandates and to provide an operational justification of their need to know this information. If these conditions are met, CSEC may release the suppressed information. This year, two of my reports included detailed reviews of such releases.

During 2007–2008, my office submitted to the Minister five classified reports based on reviews completed during the year. Two of the reviews dealt with CSEC's activities conducted under ministerial authorization; one of these pertained to foreign intelligence collection, while the other concerned information technology security. The other three reviews were conducted under my general mandate, to assess whether CSEC's activities were in compliance with the law, and the extent to which it protected the privacy of Canadians in carrying out the activities.

Methodology

Prior to beginning a review, my office provides CSEC with terms of reference that set out the objective, scope, criteria, a summary of the approach to be taken, and a timetable for the review. In conducting a review, OCSEC reviewers employ standard fact-finding tools and techniques to gather evidence, including examination of all relevant written and electronic records, and the associated authorities, policies and procedures. Reviewers also conduct extensive testing and sampling. Interviews are held with management and other personnel involved in the activities under review. Officials from other federal government departments and agencies may also be interviewed. In addition, legal

opinions and advice are examined. CSEC provides briefs and demonstrations of activities as well as answers to written questions. At the conclusion of the review process, reviewers meet with CSEC officials prior to finalizing their report. The purpose of this meeting is to outline review findings and conclusions.

Overview of 2007–2008 findings

Although the five reviews reported on this year differed in subject, there were recurring themes, some of which are noted below. Overall, I am able to report that the activities of CSEC examined during the year complied with the law.

Interpretation of ministerial authorizations

As noted earlier, CSEC and my office are still on opposite pages as regards the interpretation of the provisions of the *National Defence Act* relating to ministerial authorizations. However, pending legislative amendments, I have continued my predecessor's practice of reviewing and reporting on whether CSEC's activities conducted under ministerial authorization comply with the Act as it has been interpreted by the Department of Justice. On this basis, I am able to report that the two reviews of activities conducted under ministerial authorizations complied with the *National Defence Act* as interpreted by the Department of Justice.

Information management

The theme of weak document and information management has been a consistent one over time. Good information management ensures that all relevant information and documentation is entered into the corporate record. However, as I and my predecessors have noted in previous reports, inadequate or missing information in CSEC's corporate records can impair my ability to conduct reviews and to determine whether CSEC's activities comply with the law. This has left me, in some instances, in a position of providing only a negative assurance to the Minister that I have no

Inadequate information can impair my ability to conduct reviews.

evidence of non-compliance with the law, rather than providing positive assurance, supported by evidence of compliance. CSEC is well aware of my concerns in this regard, is committed to addressing this issue, and is making progress in implementing a corporate records management system. CSEC is keeping me informed of its efforts. Future reviews will continue to seek documentation that demonstrates compliance with authorities, provides a record of all activities conducted, and confirms that supervisors are monitoring the performance of their staff.

Interpretation of foreign intelligence mandate

In last year's Annual Report, I noted that one of the issues raised by my review of CSEC's foreign intelligence collection in support of the RCMP was "whether [the foreign intelligence part of CSEC's mandate] was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations."[9] Pending a re-examination of the legal issues raised, I decided that no assessment would be made of the lawfulness of CSEC's activities in support of the RCMP under the foreign intelligence part of CSEC's mandate as it is currently interpreted and applied. This issue remained unresolved as of March 31, 2008. My review of CSEC's support to CSIS, which is reported on below, raised similar issues. As I note in this instance, and unlike the matter of ministerial authorizations, I am in agreement with the advice that the Department of Justice has provided to CSEC. However, in certain cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities. Discussions on these matters are ongoing.

[9] *Supra,* note 5 at p. 13.

Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II)

Background

This report is the second and final phase of a review of certain foreign intelligence collection activities conducted under three ministerial authorizations that were in effect from March 2004 to December 2006. The first phase, which I reported on in last year's Annual Report, established an understanding of this foreign intelligence collection. It also examined the authorities, policies, procedures and management framework put in place to oversee the activities, and established the review criteria for this second phase.

The objective of this second phase was to assess and verify whether the activities that were authorized under the ministerial authorizations complied with the law as well as with the expectations set out in a ministerial directive relating to these activities.

Findings

With respect to the conditions imposed by the ministerial authorizations, which are articulated in subsection 273.65(2) of the *National Defence Act*, and the conditions imposed by the Minister as part of the authorization process, I found no evidence of non-compliance with the law. For a number of conditions, however, a lack of information and documentation did not allow my office to verify compliance. The review also found that, in some instances, CSEC had not complied with expectations set out in the ministerial directive, and I have so advised the Minister.

Operational policies were found to be in place and to provide direction to CSEC in the protection of the privacy of Canadians. No information was found to indicate that the actions of CSEC staff were in contravention of the operational policies. However, the absence and incompleteness of recorded information limits me to providing only a negative assurance to the Minister. That is to say that I have found no evidence of non-compliance with the law.

Review of information technology security activities at a government department

Background

This review examined information technology security activities conducted by CSEC under ministerial authorization in 2004–2005 at a government department. The objective was to assess compliance with the law and with the provisions of the ministerial authorization.

The *National Defence Act* mandates CSEC to help protect the Government of Canada's computer systems and networks by analyzing the vulnerability of selected computing and telecommunications systems and by providing information technology security advice and services to government departments and agencies.

CSEC's information technology security activities may result in the inadvertent interception of private communications of Canadians or personal information about a Canadian. For this reason, subsection 273.65(3) of the *National Defence Act* provides that:

> The Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

The CSEC Chief is responsible for seeking authorization on behalf of the department or agency requesting the activity to be covered. This ministerial authorization enables CSEC to undertake a complete security assessment of a department's networks.

Findings

The review found that CSEC's information technology security activities at the department were in compliance with the law and with the ministerial authorization. The process by which CSEC acquired the ministerial authorization was in accordance with the requirements of the *National Defence Act* and the processes outlined in CSEC's related policies. It was also determined that the five conditions set out in subsection 273.65(4) of the Act were complied with satisfactorily. Measures were in place to protect the privacy of Canadians, and CSEC's use and retention of personal information about Canadians was found to comply with the law and CSEC policy.

Review of CSEC's activities carried out under a ministerial directive

Background

This review focused on certain activities undertaken by CSEC under a ministerial directive and, in the context of ministerial authorizations, in support of its foreign intelligence mandate articulated in paragraph 273.64(1)(a) of the *National Defence Act* for the period of April 1, 2005 to March 31, 2006.

Technology and telecommunications networks continue to increase in complexity. In order to fulfill its legislative mandate, CSEC conducts activities for the purposes of understanding the global information infrastructure and of locating foreign intelligence, in accordance with the intelligence priorities of the Government of Canada.

The objective of this review was to increase my office's knowledge of these activities and the authorities under which the activities are conducted. The review assessed CSEC's compliance with the ministerial directive and with the laws of Canada, including the *National Defence Act*, the *Charter*, and the *Privacy Act*, which governs the collection, use and disclosure of personal information. The review also assessed whether the activities conformed to CSEC's policies and procedures.

Findings

This was my office's first examination of this activity, as governed by the ministerial directive. I am satisfied that CSEC takes measures to protect the privacy of Canadians in the use and retention of data obtained from this activity. However, I made a number of recommendations, as follows.

First, I believe that CSEC should re-examine its practice that only those private communications recognized by certain staff be accounted for. I recommended that other staff that observe and handle private communications should also be responsible for accounting for them. Second, CSEC should re-assess which part of its legislative authority ought to be used to conduct certain of these activities, particularly those involving information provided by federal law enforcement and security agencies. Finally, I also believe that CSEC should augment its policy and procedures in order to better guide and support these activities.

Staff that observe and handle private communications should be responsible for accounting for them.

My office has since been advised that CSEC is re-examining these activities and associated policies and procedures. I support CSEC's initiative, and will continue to monitor the issues raised during this review.

Review of CSEC's counter-terrorism activities

Background

This review examined the lawfulness of CSEC's counter-terrorism activities in the period from April 1 to July 31, 2005.

In early October 2001, CSEC centralized foreign intelligence efforts as they relate to threats from international terrorism. The activities involve research and analysis of foreign intelligence data in order to identify terrorist targets and their operational and support networks. The information may be shared with federal government departments and agencies involved in intelligence and security-related matters, as well as with Canada's principal intelligence partners.

The main objectives of the review were to examine data collection and reports from the review period to verify that the information was collected, used and retained in compliance with the law, and to identify and report on any other issue of concern that might impact on the ability of CSEC to conduct its activities lawfully and to safeguard the privacy of Canadians.

Findings

This review found that the activities conducted were in compliance with the law and with CSEC policy. Personnel who were interviewed during the course of this review were knowledgeable about the authorities governing their work. The report makes two recommendations. One would enhance accountability regarding linkages between CSEC reporting and the intelligence priorities of the Government of Canada, and the other would enhance accountability for the use and retention of private communications and information about Canadians.

Review of CSEC's support to CSIS

Background

The objective of this review was to assess the lawfulness of CSEC's activities in providing support to the Canadian Security Intelligence Service (CSIS) under CSEC's foreign intelligence mandate in the period from April 1, 2004 to March 31, 2005 and a sampling from November to December 2006.

CSEC provides regular foreign intelligence reporting to CSIS. Most of this reporting addresses general areas of interest that complement and support CSIS' own mandated responsibilities. CSEC also receives and responds to specific CSIS requests for intelligence-related information, provided that the requirement is consistent with documented Government of Canada intelligence priorities. A final aspect of CSEC's support to CSIS is that it responds to requests for the release of Canadian identities that have been suppressed in foreign intelligence reporting. Upon receipt of a formal request, CSEC must be satisfied with the justification and lawful authority for requiring the information.

Findings

Overall, I am of the opinion that CSEC acted within its mandate in conducting activities in support of CSIS. I am in accord with the advice and guidance provided by the Department of Justice to CSEC respecting this support. However, in some cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities and I have recommended that CSEC re-examine this matter. As of March 31, 2008, this was the subject of ongoing discussions between my officials and CSEC.

In addition, my office identified concerns respecting requests for the release of suppressed information, and respecting the CSIS-CSE Memorandum of Understanding of 1990 that guides the agencies' cooperation. Many of my findings reinforced those of two previous reviews of CSEC's foreign intelligence collection in support of the

RCMP and of the roles of CSEC's client relations officers and Operational Policy Section in the release of personal information, both of which are described in my 2006–2007 Annual Report.

I am pleased to note that since the period of review, CSEC continues to review its internal processes, policies and procedures, in order to make improvements in areas where deficiencies have been identified.

CSEC continues to make improvements in areas where deficiencies have been identified.

I have, however, recommended that CSEC re-visit the Memorandum of Understanding between CSIS and CSEC which is out of date and does not reflect current arrangements or practices between the two agencies. Given the international threat environment, it is my view that cooperation between security and intelligence agencies must be continually examined and the frameworks for cooperation kept up to date.

Reviews underway and planned

My office has several reviews underway that I will be reporting on to the Minister in the coming year and will include in my next Annual Report. The subjects of these reviews include: activities conducted by CSEC under several foreign intelligence ministerial authorizations; the disclosure of information about Canadians to federal government departments and agencies; an examination of certain common practices of CSEC related to its mandated activities, and a comprehensive study of its information technology security activities. Some reviews that will begin in the next fiscal year will carry through to 2009–2010. Last year I indicated that I would be reporting on CSEC's use of technology to protect the privacy of Canadians. At fiscal year-end, this review was being finalized, and therefore it will be reported on in next year's Annual Report.

Complaints about CSEC activities

My mandate includes undertaking any investigation I deem necessary in response to a complaint. During the 2007–2008 fiscal year my office received no complaints that warranted formal investigation.

Duties under the *Security of Information Act*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy and seek to defend the release of classified information about CSEC on the grounds that it is in the public interest. No such matters were reported to my office in the 2007–2008 fiscal year.

THE COMMISSIONER'S OFFICE

I continue to be supported in my work by a full-time staff of eight people, together with a number of subject matter experts who make themselves available, as required, under contract.

Keeping sufficiently current with technology to support my review of CSEC's activities is always a challenge. It was facilitated this year by CSEC itself. In the fall of 2007, CSEC opened its doors to members of my staff who attended two courses for CSEC employees, one respecting information technology security, and another course covering foreign intelligence.

In May 2007, I addressed a meeting of the Advisory Council on National Security that was held in Ottawa. The Advisory Council was created in April 2004 as a feature of the National Security Policy. It is made up of individuals from outside the government whose function is to provide advice on security matters.

Also in May, my office hosted a meeting of the Review Agencies Forum, which brings together the staff members of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service, the Commission for Public Complaints against the Royal Canadian Mounted Police and my own office. The Forum provides an opportunity for review analysts to compare best practices and discuss issues of mutual interest and concern. In this regard, my office's review methodology initiative was discussed at length.

In June 2007, I had the pleasure of introducing U.S. Supreme Court Justice Antonin Scalia at the *International Conference on the Administration of Justice and National Security in Democracies*, held in Ottawa. The Conference, which was jointly sponsored by the Federal Court of Canada and the Canadian Centre of Intelligence and Security Studies at Carleton University, also provided me with an opportunity to renew my contacts with colleagues from other countries, some of whom I had met at the last *International Intelligence Review Agencies Conference* (*IIRAC*) in South Africa in October 2006.

Also in June, I was represented by the Executive Director at an international conference on Accountability of Intelligence and Security Agencies and Human Rights, held in The Hague under the auspices of the Dutch Review Committee on the Intelligence and Security Services and the Faculty of Law of Radboud University, Nijmegen. In September, I was represented by the Director of Operations at the annual conference of the Canadian Association for Security and Intelligence Studies in Calgary, where participants explored the many challenges facing the security and intelligence community.

Also in September, I attended a two-day conference entitled *Protecting Security and Human Rights: The Case for Migration in Canada* and sponsored by the Institute for Research in Public Policy.

All these initiatives demonstrate increasing interest, in Canada and abroad, in security and intelligence matters and their many dimensions.

Since its creation in 1996 by Order in Council pursuant to Part II of the *Inquiries Act*, the Office of the CSE Commissioner has been funded by the Department of National Defence, but has received administrative and other support from the Privy Council Office.

Over the fall months, a decision was taken that the long-standing relationship with the Privy Council Office would be severed, and that the administrative and other support activities for my office would be taken over by National Defence. I view this change in a positive light. I would be remiss, however, if I failed to take note of the outstanding help and support provided by the staff of the Privy Council Office over the last twelve years. Thank you from all of us.

In the interest of providing information about OCSEC's work, my office hosts a website (www.ocsec-bccst.gc.ca) that describes our mandate and activities. In fiscal year 2007–2008, there were over 98,000 visits to the site, including visitors from approximately 40 countries outside North America.

In 2007–2008, my office's expenditures were $1,220,999, which was well within budget for the period. Annex C to this report provides a summary of 2007–2008 expenditures.

A TRIBUTE

On November 24, 2007, the Right Honourable Antonio Lamer, my predecessor as CSE Commissioner, died at age 74. Antonio Lamer was a renowned lawyer and jurist. He was appointed to the Supreme Court of Canada in 1980, and was named Chief Justice in 1990, a position that he occupied until his retirement in 2000.

For my part, he was my colleague on the bench for over 11 years, and my long-standing friend. His contribution to Canadian jurisprudence was outstanding, exceeded only by his love of Canada. He is missed.

ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

***National Defence Act* – Part V.1**

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX B: CLASSIFIED REPORTS TO THE MINISTER, 1996–2008

1. Principal vs. agent status – March 3, 1997 (TOP SECRET)

2. Operational policies with lawfulness implications – February 6, 1998 (SECRET)

3. CSE's activities under *** – March 5, 1998 (TOP SECRET Codeword/CEO)

4. Internal investigations and complaints – March 10, 1998 (SECRET)

5. CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)

6. On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

7. How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)

8. A study of the *** collection program – November 19, 1999 (TOP SECRET Codeword/CEO)

9. On *** – December 8, 1999 (TOP SECRET/COMINT)

10. A study of CSE's *** reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)

11. A study of selection and *** — an overview – May 10, 2000 (TOP SECRET/CEO)

12. CSE's operational support activities under *** — follow-up – May 10, 2000 (TOP SECRET/CEO)

13. Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)

14. On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)

15. CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. A study of the *** reporting process — *** (Phase II) – April 6, 2001 (SECRET/CEO)

17. A study of the *** reporting process — *** (Phase III) – April 6, 2001 (SECRET/CEO)

18. CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

19. CSE's support to ***, as authorized by *** and code-named *** – August 20, 2001 (TOP SECRET/CEO)

20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)

21. CSE's support to ***, as authorized by *** and code-named *** – November 13, 2002 (TOP SECRET/CEO)

22. CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

23. Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)

24. CSE's activities pursuant to *** Ministerial authorizations including *** – May 20, 2003 (SECRET)

25. CSE's support to ***, as authorized by *** and code-named *** — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)

26. CSE's support to ***, as authorized by *** and code-named *** — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)

27. A review of CSE's activities conducted under *** Ministerial authorization – March 19, 2004 (SECRET/CEO)

28. Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)

29. A review of CSE's activities conducted under 2002 *** Ministerial authorization – April 19, 2004 (SECRET/CEO)

30. Review of CSE *** operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

31. CSE's support to *** – January 7, 2005 (TOP SECRET/COMINT/CEO)

32. External review of CSE's *** activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

33. A study of the *** collection program – March 15, 2005 (TOP SECRET/ COMINT/CEO)

34. Report on the activities of CSE's *** – June 22, 2005 (TOP SECRET)

35. Interim report on CSE's *** operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)

36. External review of CSE *** activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)

37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)

38. Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/ COMINT/CEO)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/ COMINT/CEO)

41. Review of information technology security activities at a government department under ministerial authorization – July 20, 2007 (TOP SECRET)

42. Review of CSEC's counter-terrorism activities – October 16, 2007 (TOP SECRET/ COMINT/CEO)

43. Review of CSE's activities carried out under a ministerial directive – January 9, 2008 (TOP SECRET/COMINT/CEO)

44. Review of CSEC's support to CSIS – January 16, 2008 (TOP SECRET/ COMINT/CEO)

45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – March 28, 2008 (TOP SECRET/ COMINT/CEO)

ANNEX C: STATEMENT OF EXPENDITURES, 2007–2008

Standard Object Summary

Salaries and Wages	$713,135
Transportation and Telecommunications	37,431
Information	21,239
Professional and Special Services	257,488
Rentals	151,894
Purchased Repair and Maintenance	3,538
Materials and Supplies	8,652
Acquisition of Machinery and Equipment	23,258
Other Expenditures	4,364
Total	**$1,220,999**

ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER (OCSEC)

The Office of the Communications Security Establishment Commissioner (OCSEC) was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., Chief Justice of Canada (retired) for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act.* During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-terrorism Act* which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act,* by adding Part V.1 and creating legislative frameworks for both OCSEC and CSEC. It also gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act.* This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest.

Under the Commissioner's current mandate, which entrenched in law the original mandate established in 1996 as well as the additional responsibilities described above, the Commissioner has retained the powers of a commissioner under Part II of the *Inquiries Act*.

ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSEC employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign intelligence services. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign intelligence products and services support government decision-making in the fields of national security, national intelligence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable its clients (other government departments and agencies) to effectively secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC has a three-part mandate under subsection 273.64(1) of the *National Defence Act.* These are known as parts (a) (b) and (c) of its mandate:

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.