Communications Security Establishment Commissioner

# Annual Report

2006-2007

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: http://csec-ccst.gc.ca


ISBN 978-0-662-69804-3
Cat. No. D95-2007

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

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

May 2007

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 2006–2007 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

# TABLE OF CONTENTS

# INTRODUCTION

This is my first report as Communications Security Establishment (CSE) Commissioner, since my appointment effective August 1, 2006. I have a three-year mandate that expires in August 2009.

My own background includes 30 years' experience on the bench, most recently as a Supreme Court Justice from 1989-2003. I believe there are strong parallels between the role of a judge and that of the CSE Commissioner. A judge's fundamental concern is to ensure fair trials and protect personal liberty, while maintaining peace and security. Correspondingly, the CSE Commissioner's fundamental concern is to balance the right to privacy with the need for information to protect national security. The similarity between these roles is reflected in the legislation specifying that the Commissioner be a supernumerary judge or a retired judge of a superior court.

*The CSE Commissioner's fundamental concern is to balance the right to privacy with the need for information to protect national security.*

There is, however, an important difference in context. While secrecy issues do arise in court proceedings in certain instances, for the most part the judicial process takes place in public. Secrecy, on the other hand, is at the very heart of foreign intelligence collection. Nevertheless, the balancing principles are the same. I see the role of my office as providing Canadians with the assurance that the CSE's critical intelligence work is being carefully examined by an impartial authority to ensure it is lawful, and that their rights are being protected, without compromising the secrecy required to protect national security.

In October 2006, I was presented with an exceptional opportunity to attend the International Intelligence Review Agencies Conference in Cape Town, South Africa. One of the conference themes was the need to balance the traditional rights and liberties of citizens with the need for increased powers to meet threats to national security. It was a remarkable experience to meet with the practitioners in security and intelligence review from 14 countries, including my own, and to hear from them first-hand about the challenges we all face. I remain grateful for this

opportunity because it provided an occasion for me, as the new CSE Commissioner, to become totally immersed in topics of mutual interest in the company of experts.

During the early days following my appointment, I met the Minister of National Defence and the Chief of CSE. I was also provided with extensive briefings and tours, many of them at CSE, and I am particularly grateful to my briefers for their comprehensive presentations. As time progressed, I had the opportunity to meet other federal government officials, including the Auditor General of Canada and the Privacy Commissioner, the Chairs of the Security Intelligence Review Committee and the Commission for Public Complaints Against the RCMP, the Deputy Minister of National Defence, and the National Defence Ombudsman.

Most important, of course, has been the time I have spent involving myself in the work of my office, and familiarizing myself with the activities and preoccupations of my predecessors, which will be discussed later in this report.

## THE REVIEW ENVIRONMENT

A number of key issues helped shape the environment in which this office carried out its work over the past year. Some of these have been described and commented on by my predecessors in past Annual Reports. Below, I draw attention to some themes that have not been mentioned before, as well as some new developments in ongoing issues.

### Legal interpretations

Since the omnibus *Anti-Terrorism Act* was proclaimed in December 2001, the persons who have occupied the position of CSE Commissioner have faced a persistent dilemma arising from the amendments this Act introduced to the *National Defence Act.* Particularly troublesome has been the Commissioner's duty to review the activities of CSE conducted under ministerial authorizations issued for the sole purpose of obtaining foreign intelligence, given the lack of agreement on the interpretation of key provisions of the Act.

On the one hand, my predecessors and I have recognized the importance of CSE's work, and the benefit the Government of Canada derives from the foreign intelligence CSE provides, particularly during a time when the threat of global terrorism continues unabated, and the safety of our soldiers in Afghanistan remains at risk.

On the other hand, during our respective terms as Commissioner, each of us has been unequivocal in the position that the legal interpretation and advice regarding ministerial authorizations provided to CSE by the Department of Justice is not supported by a simple reading of the appropriate provisions of Part V.1 of the *National Defence Act,* and each of us so advised the Minister of National Defence of the day. In addition, my immediate predecessor, the Right Honourable Antonio Lamer and I both made our positions known to officials at the Office of the Attorney General of Canada.

When I am asked to consider whether an activity is lawful, I must first determine what the law states in respect of that activity. The relevant Act, then, is the yardstick by which the lawfulness of the activity is measured. The difficulty arises, in instances such as this, when there is a fundamental difference of opinion about what the Act states.

I do not question the role of the Department of Justice in the drafting of legislation, nor do I view my role as Commissioner as arbiter of statutory interpretation. However, as I have informed the Minister of National Defence and the Attorney General of Canada, the legislation lacks clarity and it ought to be amended, a view I share with both my predecessors.

*The legislation lacks clarity and it ought to be amended.*

This matter has been under deliberation for some time, and I hope the government will make the required amendments at the earliest opportunity. I am confident that this will not be too onerous a task because other countries have successfully adopted and are applying legislation to meet similar requirements.

## Legislation lagging behind technological advances

As time goes on, there is an ever-widening knowledge gap between the general public and evolving technologies. In a number of respects, Canada's laws have also not kept pace with technological advances. We need a more imaginative approach. Today, criminal and terrorist elements are masters of these complex technologies and, unlike democratic institutions, are unimpeded by legal constraints. Those involved in the legislative process need to avoid laws that are driven by the technology of the day, which will in short order be superseded by new developments. Instead, we must ensure our laws have a broad enough scope, and are so structured — be it by providing for regulations or otherwise — that they can accommodate new technologies, and continue to protect both our privacy and security.

## Three-year review of the *Anti-Terrorism Act*

The *Anti-Terrorism Act* amended the *Official Secrets Act* and the *National Defence Act*, among other legislation. The amendments to the *National Defence Act* included a legislative basis for CSE and the CSE Commissioner.

The *Anti-Terrorism Act* required a review of its provisions and operation within three years of receiving royal assent, to be carried out by a designated or specially established committee of the Senate or the House of Commons, or of both chambers. A Subcommittee of the House of Commons Standing Committee on Public Safety and National Security was established for this purpose in autumn 2004. At the same time, the Senate established a Special Committee to carry out a comprehensive review of the Act. As described in the 2005-2006 Annual Report, my predecessor appeared before the Senate Special Committee on June 13, 2005, and two days later before the House of Commons Subcommittee. The Senate Special Committee reported on February 22, 2007, and the House Subcommittee reported on March 27, 2007.

## Senate Special Committee recommendations

The Senate Special Committee made several recommendations concerning CSE as well as this office. As regards CSE, the Committee focussed primarily on ministerial authorizations, stating that it accepted the explanations as to why CSE needs to intercept private communications when undertaking its foreign intelligence and information technology security activities. It also accepted Commissioner Lamer's explanation that ministerial authorizations were the proper instrument to use for intercepting private communications, rather than prior judicial authorization, because warrants from Canadian courts have no jurisdiction outside Canada.[1] The Committee drew comfort from the fact that this office is required to review the lawfulness of CSE's activities, including the interception of private communications under ministerial authorizations. However, it remained concerned, as was Commissioner Lamer, that the standard required to satisfy the Minister that all necessary preconditions to intercepting private communications have been met is unclear. Accordingly, the Committee recommended that subsections 273.65(2) and (4) of the *National Defence Act* be amended to clarify whether these preconditions should be based on reasonable belief or reasonable suspicion.[2] This has been an issue of interest to my office, and a clarification would be welcome.

*The Committee drew comfort from the fact that this office is required to review the lawfulness of CSE's activities.*

Because the Committee wished to ensure that intercepted information is disposed of if it has been determined to be non-essential or when it is no longer essential, it recommended that CSE develop information retention and disposal policies, containing specific timeframes for the disposal of intercepted information, and that it make these policies publicly available.[3]

---

[1] 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, p. 77.
[2] *Ibid*., Recommendation 18, p. 78.
[3] *Ibid*., Recommendation 19, p. 79.

In the interests of accountability and transparency, the Committee also recommended that the Minister of National Defence or the CSE be required to report annually to Parliament on the number of ministerial authorizations issued during the year, the number still in force by the end of the year, and the general purpose for which each authorization was issued (i.e., to obtain foreign intelligence or to protect computer systems or networks).[4]

The *Anti-Terrorism Act* also amended the *Official Secrets Act*, and renamed it the *Security of Information Act,* known as SOIA. SOIA establishes a process that persons permanently bound to secrecy must follow if they wish to claim a public interest defence for divulging classified information. The Commissioner may receive classified information as part of the process (see Annex A). However, the *Security of Information Act* does not describe what should be done once the Commissioner receives that information.[5] The Committee recommended that the Government specify the procedure to be followed in such cases.[6] I should point out that my office does have internal policies and procedures in place to fill the gap that the Committee identified.

Lastly, the Committee discussed the oversight and review of Canada's national security and anti-terrorism framework. The Committee mentioned that this office is "generally perceived to be an effective oversight mechanism."[7] The Committee recommended that a standing Senate committee be established to monitor and periodically report on Canada's anti-terrorism legislation and national security framework on an ongoing basis. In addition, the Committee called for a comprehensive parliamentary review of the provisions and operation of the *Anti-Terrorism Act* every five years.

---

[4] *Ibid.*, Recommendation 20, p. 79.
[5] To date, I have not received any information under the *Security of Information Act*.
[6] *Supra*, footnote 1, Recommendation 26, p. 94.
[7] *Supra*, footnote 1, p.116.

## House of Commons Subcommittee recommendations

The House Subcommittee's Final Report on its review of the *Anti-Terrorism Act* also addressed the issue of ministerial authorizations. In particular, I was pleased to note that the Subcommittee drew attention to the remarks of my predecessor in his 2005-2006 Annual Report about the legal ambiguities and uncertainties in the provisions allowing for ministerial authorizations, and the disagreement regarding interpretation of these provisions between this office and the Department of Justice. Without making a specific recommendation in this regard, the Subcommittee urged government counsel and me to resolve these issues as expeditiously as possible. As well, the Subcommittee requested that the Government's response to the Final Report indicate what the issues of disagreement are and how they have been resolved, to the extent possible. Failing this, the Subcommittee believes I should provide these details in my 2007-2008 Annual Report.[8] I intend to revisit this recommendation as the time for that report approaches.

*My office's review methodology always includes an examination of compliance with the Charter and the Privacy Act.*

The Subcommittee also supported a recommendation by the Privacy Commissioner that subsection 273.65(8) of the *National Defence Act* be amended to require the CSE Commissioner to review the private communication interception activities carried out under ministerial authorization to ensure they comply with the requirements of the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, as well as with the authorization itself. This position was reinforced with an additional recommendation that section 273.66 of the *National Defence Act* be amended to require the CSE only to undertake activities consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, in addition to the restraints on the exercise of its mandate already set out in that section.[9] I should point out that my office's review methodology always includes an examination of compliance with the *Charter* and the *Privacy Act*.

---

[8] Subcommittee on the Review of the *Anti-Terrorism Act*, *Rights, Limits, Security: A Comprehensive Review of the* Anti-terrorism Act *and Related Issues. Final Report of the Standing Committee on Public Safety and National Security,* March 2007, p. 56.

[9] *Ibid.*, Recommendations 44 and 45, pp. 55-56.

With respect to the issue of review and oversight, the Subcommittee recommended that Bill C-81 from the 38th Parliament, the proposed *National Security Committee of Parliamentarians Act*, or a variation of it, be introduced in Parliament at the earliest opportunity. The Subcommittee further recommended that the mandate of the proposed committee include undertaking compliance audits of departments and agencies, such as CSIS, CSE, and national security elements of the RCMP, in relation to the provisions of the *Anti-Terrorism Act*.[10] In last year's Annual Report, my predecessor welcomed the prospect of more active parliamentary review of national security activities, but also noted challenges such as the composition of the committee and its access to classified information and documents. I concur with that position in general, and intend to offer specific comments once a bill is introduced.

Finally, the Subcommittee recommended that there be another comprehensive review of the provisions and operation of the *Anti-Terrorism Act*, to begin no later than December 31, 2010, and to be completed no later than December 31, 2011. It noted that the proposed committee of parliamentarians would be well-equipped to carry out this review.[11]

## The O'Connor Commission of Inquiry

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar was established February 5, 2004. It was mandated to investigate and report on the actions of Canadian officials in relation to Maher Arar (Factual Inquiry) as well as to recommend an arm's-length review mechanism for the activities of the RCMP with respect to national security (Policy Review). The Honourable Dennis O'Connor was appointed Commissioner of the Inquiry. He released his Policy Review report on December 12, 2006.

[10] *Ibid.*, Recommendations 58 and 59, pp. 84-86.
[11] *Ibid.*, pp. 83-85.

In order to provide integrated review of integrated national security activities, Commissioner O'Connor recommended that statutory gateways be enacted linking the proposed Independent Complaints and National Security Review Agency for the RCMP, the Security Intelligence Review Committee and the Office of the CSE Commissioner to provide for exchange of information, referral of investigations, conduct of joint investigations, and coordination and preparation of reports. [12] I welcome this proposal, although to date the absence of gateways has never been an operational impediment.

I was pleased to note the following observation from Justice O'Connor's report: "I am not recommending that SIRC's mandate be expanded to include the CSE, as I understand that the Office of the CSE Commissioner functions very well and I see no reason to interfere with that operation."[13] I was also pleased to see that my office was recognized for the creation of the Review Agencies Forum in 2005-2006.[14] The Forum is described further on in this report.

I do have reservations, however, regarding Justice O'Connor's recommendation to establish an Integrated National Security Review Coordinating Committee.[15] I am concerned that introducing such a coordinating committee by way of statute, and amendments to related legislation, may create an unnecessary and counter-productive level of bureaucracy between independent review agencies and Parliament.

---

[12] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), p. 578.
[13] *Ibid*., Recommendation 11, p. 580.
[14] *Ibid*., p. 282.
[15] *Ibid*., Recommendation 12, p. 591.

## THE YEAR IN REVIEW

### Independent Reviews of OCSEC

In spring 2006, two independent management reviews of my office were commissioned. One focussed on administration, including the management and control of financial, human and information resources. The other dealt with operations, by assessing whether the office carries out the Commissioner's mandated responsibilities efficiently and effectively.

*I was pleased to note that the findings of the administrative review were all positive.*

The reports of these management reviews were available to me at the time of my appointment, thus providing me with an independent assessment of my new area of responsibility. I was pleased to note that the findings of the administrative review were all positive. The recommendations of the operational review were discussed in detail at a review workshop held on August 21, 2006, with the review consultants as moderators. The operational review also raised methodology issues, which will be briefly referred to later in this report.

### Workplan

My office's activities are guided by a regularly updated three-year workplan. To facilitate scheduling, my staff consult with CSE about the review components of this plan. Criteria that determine their selection of topics for review include: CSE activities or programs that have not previously or recently been reviewed; areas identified from briefings requested of CSE; the status of recommendations from previous reviews; and activities where privacy is most likely to be at risk. My staff, who have extensive knowledge of CSE, ask themselves fundamental questions such as: what can go wrong; what is the probability of something going wrong; and what are the consequences if they do go wrong.

Also during the year, considerable staff time and resources were devoted to work on legal interpretation issues, which I have already described in detail above in my discussion of the review environment.

## Reviews undertaken of CSE

My general review mandate is set out in paragraph 273.63(2)(a) of the *National Defence Act*.[16] 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. Reviews of CSE's activities conducted under ministerial authorizations are undertaken only after the ministerial authorization has expired.

During 2006-2007, my office submitted classified reports of four reviews to the Minister. Two of the reviews dealt with CSE's activities conducted under ministerial authorization; one pertained to foreign intelligence collection, while the other concerned information technology security. The other two reviews were conducted under my general mandate, to ensure the activities were in compliance with the law.

[16] Please see Annex A for the text of the relevant sections of the *National Defence Act*.

## 2006-2007 REVIEW HIGHLIGHTS

# Review of CSE's foreign intelligence collection in support of the RCMP

### Background

In January 2005, my office submitted a report to the Minister of National Defence examining the technical and operational assistance CSE provided to the RCMP under paragraph 273.64(1)(c) of the *National Defence Act*, also known as mandate (c).[17] The second and final phase of the review was completed and in June 2006, my predecessor submitted a follow-up report reviewing CSE's foreign signals intelligence collection activities in support of the RCMP under pararagraph 273.64(1)(a) of the *National Defence Act*, also known as mandate (a). Further details on the first phase of the review may be obtained in the 2004-2005 Annual Report of this office.

Under mandate (a), CSE provides two kinds of foreign intelligence information to its government clients, including the RCMP. Most of its reports address general areas of interest that complement and support the client's own mandated responsibilities. In addition to this proactive support, CSE provides reactive support by responding to specific requests by the client for intelligence-related information.

### Methodology

OCSEC staff examined CSE's mandate (a) activities in support of the RCMP for the period January 1 to December 31, 2003. They received briefings and answers to both verbal and written questions that were posed to CSE officials. They also obtained a listing of the agency's requests for intelligence-related information and chose several to examine in detail. As part of this in-depth examination, two separate demonstrations illustrating the activities under review were provided to OCSEC staff by those CSE officials who had been directly involved in responding to the requests.

[17] CSE's mandate is described in Annex E of this report.

## Findings

Many of the findings and recommendations made in my office's first report also applied to this second-phase review of assistance provided under mandate (a). For example, it was recommended CSE amend and/or update the instruments that guide its support activities to the RCMP. My predecessor was pleased to report that, for the most part, CSE had accepted these recommendations and is working to implement them.

*CSE has advised that high priority has been given to the development and implementation of a corporate records management system.*

CSE also acknowledged the need to implement a formal system of record keeping. This is a continuing concern, as was noted in my office's 2005-2006 Annual Report. CSE has advised that high priority has been given to the development and implementation of a corporate records management system that will deal with their hard-copy and electronic records requirements.

During the second phase of the review, a detailed examination of CSE's response to RCMP requests for intelligence-related information identified two issues of concern that required further legal study by CSE. The first was whether mandate (a) was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations. Pending a re-examination of this issue by CSE, no assessment was made of the lawfulness of CSE's activities in support of this agency under mandate (a) as currently interpreted and applied by CSE. My staff is monitoring the issue.

The second issue related to CSE's policies and practices as they relate to the disclosure of Canadian personal information to its clients. When collecting foreign intelligence, CSE may incidentally acquire personal information about Canadians. This information may be retained if 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 full details of Canadian personal information, CSE requires its clients, including the

RCMP, to justify their authority to collect this information under their own respective mandates and provide an operational justification of their need to know this information. If these conditions are met, CSE releases the information.

An in-depth examination of relevant sections of the *National Defence Act* and the *Privacy Act* raised questions as to CSE's conformance with the various authorities that govern disclosure. Thus, my office recommended that CSE also re-examine its authority to collect, use and disclose personal information to certain federal government departments and agencies. In addition, my office has recommended that CSE establish agreements with client agencies to formalize the circumstances when such information may be disclosed while providing assistance under its (c) mandate.

CSE acknowledged that the report "raises a number of issues that, from a policy/legal perspective, will generate further in-depth analysis by CSE and Department of Justice legal counsel." I anticipate that this analysis will include a discussion and perhaps even a formal articulation by CSE of its position regarding the application of the *National Defence Act* as it relates to the provision of foreign intelligence in accordance with the Government of Canada intelligence priorities.

## Review of information technology security activities at a government department

### Background

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

Individuals conducting personal and business affairs with the Government of Canada have a reasonable expectation of privacy. However, when the security of government computer systems and networks is being tested, personal information or private communications can be inadvertently intercepted with certain types of necessary testing. Subsection 273.65(3) of the *National Defence Act* provides that:

*Individuals conducting personal and business affairs with the Government of Canada have a reasonable expectation of privacy.*

> 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.

In such cases, CSE is responsible for seeking authorization on behalf of the department or agency requesting the activity to be covered. This ministerial authorization enables CSE to undertake a complete assessment of a department's computer systems and networks.

## Methodology

The review was conducted initially through examination of documents and files related to the ministerial authorization and the conditions imposed by it. Fact-finding and verification interviews were then held with CSE and selected client representatives who were identified as having direct involvement in the authorization process or ensuing activities.

## Findings

With the qualification set out below regarding one of the conditions of the ministerial authorization, this review found that CSE's work at the department was in compliance with the law and with the ministerial authorization.

The review found that the process by which CSE acquired the information technology security ministerial authorization for its activities at the department was found to be in accordance with the requirements of the *National Defence Act*. It was also determined that four of the five conditions set out in subsection 273.65(4) of the Act were complied with satisfactorily. However, with respect to one of the conditions, the review found that certain information was retained even though its retention was not essential. While CSE personnel acted in a manner that was consistent with the direction they were given, there were aspects that could be improved upon, and CSE has undertaken to do so. CSE has also indicated that future Memoranda of Understanding with client departments where information technology security activities under ministerial authorizations are to be conducted will reflect these improvements.

Other recommendations from the review included ensuring that future policy and practice promote conformance with CSE's legislated authorities as they relate to staff activities during information technology security exercises.

## Review of the roles of CSE's client relations officers and the Operational Policy Section in the release of personal information

### Background

The objective of this review was to assess the lawfulness of the activities of both the CSE client relations officers and the Operational Policy Section, as they relate to the request for and release of personal information about Canadians that has been suppressed in CSE foreign intelligence reports, as referred to previously. This information is made available to authorized Government of Canada clients, only under certain conditions.

CSE has provided foreign intelligence reports based on signals intelligence to officials in government departments since its formal establishment in 1946. Reports were delivered by hand until the creation of the on-site client relations officer programme in 1985. Client relations officers provide intelligence reports, explain to individual clients and potential

clients the role of CSE and signals intelligence, and assist in determining client needs based on Government of Canada intelligence priorities.

To protect privacy, CSE suppresses personal information about Canadians in foreign intelligence reports. If a client has both the authority and the need to know the information, it must make a formal request and provide justification. Requests for release of this information are centralized in CSE's Operational Policy Section.

*To protect privacy, CSE suppresses personal information about Canadians in foreign intelligence reports.*

The majority of requests are now made via a secure communication network directly to CSE. Client relations officers play a role in the release of Canadian identities in CSE foreign intelligence reports because they continue to deal with requests from clients who do not have access to this secure network.

## Methodology

This review examined relevant documentation, including the authorities that govern the activities of client relations officers and the CSE unit authorized to release this information. All requests for and releases of suppressed information during a six-month period were reviewed in detail to ensure compliance with law and policy. Interviews were conducted with client relations officers, their managers, and the manager of the Operational Policy Section.

## Findings

The review concluded that the activities of the CSE client relations officers and the Operational Policy Section were in compliance with the *National Defence Act* and with CSE's related policies. There were some inconsistencies in requests and releases, as well as areas where both policy and practice could be improved to enhance the protection of privacy, as required by the *Privacy Act*. Recommendations included more comprehensive training for clients who make requests, and providing more clients with secure, electronic access to CSE as a means of reducing errors and enhancing control over the process. I was pleased to note that

since the period of review there has also been increased training for and supervision of personnel in the Operational Policy Section at CSE as regards the release of suppressed information.

## Review of CSE signals intelligence collection activities conducted under ministerial authorizations

### Background

Certain foreign intelligence collection activities were conducted under three ministerial authorizations that were in effect from March 2004 to December 2006. These ministerial authorizations focused on acquiring communications of foreign intelligence value from the global information infrastructure.[18]

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. In addition to the conditions set out in subsection 273.65(2) of the *National Defence Act*, a ministerial directive established other conditions for managing the collection.

My office is undertaking a two-part review of the activities under these ministerial authorizations, as the law is interpreted by the Department of Justice, a point which is discussed below. The objective of this first phase was to provide background to, and criteria for, the detailed review of these complex activities. I provided the Minister of National Defence with a brief report on this study phase in February 2007.

[18] "Global information infrastructure" includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions, systems or networks. (*National Defence Act*, section 273.61)

### Methodology

In order to establish an understanding of this foreign intelligence collection and the unique challenges it presents, this first phase of the review: studied the authorities given to and the conditions imposed upon CSE by the ministerial authorizations, ministerial directive and related articles; and examined how CSE has responded in terms of the policies and procedures that it has developed, and the management framework that has been put in place to oversee these activities.

### Findings

This study phase developed an historical perspective and appreciation of the rationale for this collection activity. It also provided an appreciation of the organizational complexities, the authorities under which it operates, the conditions imposed and the programs in place to implement the authorities while respecting the conditions. Finally, it established the review criteria for the second and final phase, which is now underway.

## Overview of 2006-2007 findings

I am able to report that, overall, the activities of CSE examined during this reporting period complied with the law, with one qualification. It concerned a condition of an information technology security ministerial authorization, which CSE has already undertaken to rectify. A report of CSE's assistance to the RCMP did not provide an assessment of the lawfulness of the activities reviewed, pending a re-examination by CSE of the legal issues raised.

With respect to the review of CSE's signals intelligence collection activities conducted under ministerial authorization, I would highlight once again my disagreement with the Department of Justice's interpretation of the ministerial authorization provisions of the *National Defence Act*. When assessing the lawfulness of activities conducted under ministerial authorizations, I have agreed to use the Department of Justice's interpretation for the present pending amendments to the legislation, which I have already urged be made at the earliest opportunity. I commend the Chief of CSE for supporting this initiative.

## Reviews underway / future reporting

Reviews currently underway that I will be reporting on in the next fiscal year include examinations of CSE's activities related to counter-terrorism, its use of metadata, its support to CSIS, its use of technology to protect the privacy of Canadians, and its activities under a number of foreign intelligence collection and information technology security ministerial authorizations. In addition, my office will begin a number of other reviews, under both my general mandate and my duties under the ministerial authorization provisions.

## Complaints about CSE activities

My mandate includes undertaking any investigation I deem necessary in response to a complaint, to determine whether CSE engaged, or is engaging in unlawful activity.

During the 2006-2007 reporting year my office received no complaints that warranted formal investigation. However, OCSEC did complete one investigation in spring 2006 in response to a complaint that was received in the previous reporting year. A full report was delivered to the Minister of National Defence outlining the facts of the complaint and the findings resulting from the investigation.

*I am able to report that the investigation found no unlawful activity on the part of CSE.*

While the substance of the complaint is classified, I am able to report that the investigation found no unlawful activity on the part of CSE. My office made recommendations that were accepted by CSE, and would strengthen compliance.

## 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 if they wish to claim a "public interest" defence for divulging classified information. No such matters were referred to my office in 2006-2007.

## THE COMMISSIONER'S OFFICE

I am supported in my work by a full-time staff of eight. Their extensive experience in the security and intelligence community is supplemented by subject matter experts in areas such as informatics, technology, research, policy development and communications, with whom my office contracts as required.

Many of my office's interests and concerns are shared by other Canadian security and intelligence review agencies. As Justice O'Connor noted, in 2005-2006 my staff initiated the Review Agencies Forum, which brings them together at regular intervals with the staffs of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service and the Commission for Public Complaints Against the RCMP. In 2006-2007, the Forum met twice to discuss issues such as the recommendations of Justice O'Connor's Policy Review report, and amendments to the *Public Servants Disclosure Act* resulting from the new *Federal Accountability Act* (Bill C-2). In addition, Forum participants discussed how to provide their respective agencies with reasonable turnaround times in responding to reviews, and the different approaches that have been used when delays are encountered.

My staff also participated in other conferences and symposia that provided them with new perspectives on their work, including the International Intelligence Review Agencies Conference in Cape Town, which I described above, and the conferences of the Canadian Association for Security and Intelligence Studies (CASIS) and the Ontario Bar Association. In addition, as a developmental opportunity, my office hosted two promising students at the CASIS conference.

*In 2006-2007, there were some 96,000 visits to my website.*

While my office does not have a formal educational mandate, I do believe it is important that Canadians know about OCSEC's work. To this end, my office hosts a website (www.csec-ccst.gc.ca) that describes OCSEC's mandate and activities. Visits to the site originating from outside North America span a global audience ranging from Europe to Asia and the Middle East. In 2006-2007, there were some 96,000 visits to my website.

In 2006-2007, my office's expenditures were $ 1,267,612, which was well within budget for the period. Annex C to this report provides a summary of 2006-2007 expenditures.

## LOOKING TO THE FUTURE

### The Major Commission of Inquiry and the Iacobucci Internal Inquiry

Two new inquiries that may have an impact on the future review environment are the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, led by the Honourable John Major, and the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, led by the Honourable Frank Iacobucci.

The Air India Commission's mandate is to make findings and recommendations regarding the assessments and actions of Canadian government officials before and after the 1985 bombing, and ways that any past mistakes can be avoided in the future. The Internal Inquiry is mandated to examine all aspects of the involvement of Canadian officials in relation to the detention of the three individuals in Syria or Egypt.

## Review methodology

One of the recommendations of the independent operational review of my office conducted in spring 2006 was to document formally the methodology employed by the office to examine CSE's activities. I support this initiative entirely and I am confident that the office will derive benefit from it now and in the longer term. This will be an important preoccupation over the summer months.

## IN CLOSING

Looking back over the last eight months, I would like to express appreciation to my predecessor, the Right Honourable Antonio Lamer, from whom I inherited a fine staff and an organization well positioned to meet the challenges ahead. Thanks to this legacy, I was able to assume my responsibilities immediately upon my appointment, and the transition between our tenures was seamless.

*I anticipate continuing the productive relationships that have been established.*

I anticipate continuing the productive relationships that have been established with the Minister of National Defence, with CSE and with officials at other government departments and agencies involved in Canada's security and intelligence community. In particular, I look forward to discussions that I trust will lead to a resolution of the legal interpretation issues that have beset this office since the passage of Part V.1 of the *National Defence Act*.

# 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, 1996–2007

1. Classified Report to the Minister
   – March 3, 1997 (TOP SECRET)

2. Classified Report to the Minister
   – Operational policies with lawfulness implications – February 6, 1998 (SECRET)

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

4. Classified Report to the Minister
   – Internal investigations and complaints – March 10, 1998 (SECRET)

5. Classified Report to the Minister
   – CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)

6. Classified Report to the Minister
   – On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

7. Classified Report to the Minister
   – 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. Classified Report to the Minister
   – A study of the *** collection program – November 19, 1999 (TOP SECRET Codeword/CEO)

9. Classified Report to the Minister
   – On *** – December 8, 1999 (TOP SECRET/COMINT)

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

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

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

13. Classified Report to the Minister
    – Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)

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

15. Classified Report to the Minister
    – CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

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

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

18. Classified Report to the Minister
    – CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

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

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

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

23. Classified Report to the Minister
– Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

40. Classified Report to the Minister
– 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)

# ANNEX C: STATEMENT OF EXPENDITURES 2006–2007

## Standard Object Summary

| | |
|---|---|
| Salaries and Wages | $594,551 |
| Transportation and Telecommunications | 72,839 |
| Information | 14,071 |
| Professional and Special Services | 402,620 |
| Rentals | 140,315 |
| Purchased Repair and Maintenance | 4,649 |
| Materials and Supplies | 6,404 |
| Acquisition of Machinery and Equipment | 29,977 |
| Other Expenditures | 2,186 |
| **Total** | **$1,267,612** |

## ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

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 Quebec, 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, 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 (CSE) to determine whether they conformed with the laws of Canada; and to receive complaints about CSE'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 CSE. It also gave the Commissioner new responsibilities to review activities carried out by CSE 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 CSE 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

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

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

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

CSE has a three-part mandate under Part V.1, subsection 273.64(1) of the *National Defence Act*. These are known as the (a) (b) and (c) mandates:

*(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 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.