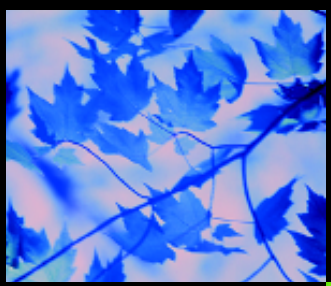
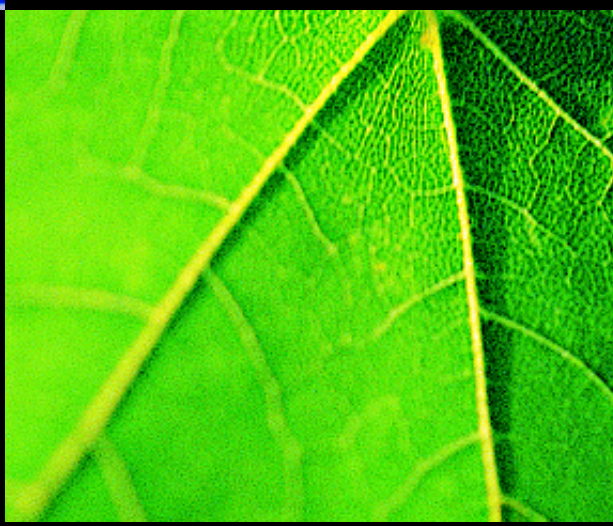
Communications Security Establishment Commissioner

Annual Report





2004-2005

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

ISBN 0-662-40229-4
Cat. No. D95-2005E-PDF

Communications Security Establishment Commissioner

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

CANADA

Commissaire du Centre de la sécurité des télécommunications

Le très honorable Antonio Lamer, c.p., c.c., c.d., L.L.D., d.u.

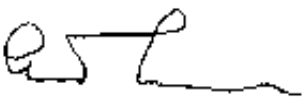
April 2005

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 2004-2005 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,



Antonio Lamer

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

Kathryn Randle

1950-2004

Our first editor

TABLE OF CONTENTS

INTRODUCTION

In the two years since my appointment as the Communications Security Establishment (CSE) Commissioner, an array of dramatic events has captured the world's attention, including the Cedar Revolution in Lebanon, and calls for the withdrawal of Syrian forces from that country, the Orange Revolution in the Ukraine, a renewed interest in the peace plan for Palestine, an election in Iraq, and parliamentary debates on equal rights for women in Kuwait. Meanwhile, Canada continues to deploy forces in Afghanistan so as to provide a secure environment suitable for the peaceful economic and political development of that nation. The positive scope of these political events is heartening.

Paralleling these changes in the geo-political landscape is the continued threat of terrorism globally. As evidenced by the bombings that killed or injured thousands in Madrid on March 11, 2004, international networks of terrorists continue to operate. This is the global environment in which CSE operates, one that is uncertain and volatile. At the same time, we are witnessing dramatic technological advances that, in the wrong hands, pose an ongoing threat to government information systems and assets, and ultimately, to Canada's security and economic competitiveness.

In the face of challenges such as these, CSE plays an essential role and makes a vital contribution to Canada's security and national interests. An integral part of Canada's security and intelligence community, CSE provides foreign intelligence to the Government of Canada and ensures the protection of the Government's electronic information and its information infrastructures. Today's national security realities make it imperative that CSE maintain its capacity and a high state of technological and operational readiness to meet Canada's evolving needs in these areas.

As the CSE Commissioner, my role is to determine if CSE's activities comply with the laws of Canada in general and, in particular, to assess whether CSE appropriately safeguards the privacy of Canadians. Over the past two years as Commissioner, I have gained an appreciation for the complex and important issues involved. Moreover, I can rely on the extensive expertise, loyalty and commitment of my staff to assist me in carrying out the Commissioner's review role effectively and efficiently.

I am pleased to submit this Annual Report for 2004-2005, summarizing the work of my office over the past year. As this report demonstrates, much has been accomplished during that time. More importantly, the report provides clear support for the essential role of the Commissioner's review function and the assurances it brings to Canadians.

THE YEAR IN REVIEW

Largely as a result of the three-year review of Bill C-36, the omnibus *Anti-Terrorism Act*, there has been heightened attention over the past year to Canada's security and intelligence community, including CSE. When the Bill was enacted in December 2001, it resulted in key amendments to existing Acts. Of particular interest to my office were the amendments to the *Official Secrets Act (*now the *Security of Information Act)* and the *National Defence Act (NDA)*. The latter provided the legislative basis for CSE and this Office. Since December 2004, this omnibus legislation has been the subject of a required three-year review by committees of the House of Commons and the Senate. I will be watching the outcome of this review with keen interest.

A number of other activities initiated during 2004-2005 have the potential to significantly affect either my office or the broader security environment in which we operate. For example, last year saw a commitment by the Prime Minister to create a National Security Committee of Parliamentarians. This commitment was made in response to a proposal set out in Canada's first-ever national security policy, which was tabled in Parliament on April 27, 2004. In this regard, an Interim Committee of Parliamentarians was struck to examine the proposal. I appeared before this committee on September 8, 2004.

Of interest to my office as well are the deliberations and outcomes of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, chaired by Mr. Justice Dennis O'Connor. In addition to investigating the role of Canadian officials in Mr. Arar's deportation from the United States to Syria, the Commission is examining options for review mechanisms for certain activities of the RCMP. I responded to the opportunity to make a submission to the Commission about some of the review options put forward. In my submission, I identified the relative strengths and weaknesses of each approach and made a recommendation on how best to proceed, given the need to safeguard the rights of persons in Canada, the realities of today's security environment and the highly sensitive nature of the RCMP's activities.

In my opinion, the most effective and logical approach is to establish one review mechanism to examine activities of the RCMP. This model would recognize the unique mandate of the RCMP, provide for a corresponding review body with the required expertise, and limit the changes required to the two organizations directly affected, the RCMP and the existing Public Complaints Commission. Furthermore, implementing this

structure would not affect other organizations or review groups in Canada's security and intelligence community where change in my respectful view is neither sought after nor required.

That being said, the Arar Commission's goal will be to strike an appropriate balance that is in the best interests of Canada. Again, I will be watching the deliberations with interest.

I had expressed concerns in last year's annual report about two legislative proposals: Bill C-7, the *Public Safety Act, 2002*, which introduced legislative amendments on a range of subjects, from transportation safety and immigration to biological weapons; and Bill C-14, which proposed amendments to the *Criminal Code* and the *Financial Administration Act*, among others. The concerns I had initially expressed about this legislation were later addressed. I am satisfied that, as passed, the legislation establishes uniform responsibility and accountability for all departments for the protection of their computer systems and networks.

Bill C-11, the so-called *whistle-blower* legislation, was first introduced as Bill C-25 on March 22, 2004, but to date has not been passed by Parliament. Although CSE is exempt from such legislation, passage of the Bill would place an onus on CSE to establish a parallel system, with a possible review role for the Commissioner. Obviously, this legislation is of interest to me and I will continue to monitor its progress in Parliament, as well as any response by CSE.

2004-2005 ACTIVITIES

Each year, my office undertakes extensive reviews of CSE activities in areas that were identified as priorities as part of a multi-year workplan. Most often, these are areas within the intelligence production cycle where there is the potential for privacy issues to be raised. I report to the Minister of National Defence on all my reviews, either to provide assurance of the lawfulness of CSE activities or to bring his attention to specific concerns that arise as a result of the reviews. My activity as Commissioner properly remains confined to *ex post* review, and not to oversight, which entails a role in relation to CSE's ongoing activities.

During 2004-2005, I submitted a total of five classified reports to the Minister – two under my general review mandate and the remainder in compliance with my mandate to review specific activities authorized by the Minister.

The review process

As in all my work, I place a high priority on collaboration during the review process. In practice, this means sharing any concerns with relevant personnel in CSE at the earliest possible stage so that appropriate corrective action can be taken, if required. As part of my office's efforts to effect change in a timely way, my staff now provide a summary briefing to all concerned CSE personnel following the review process.

One of the underlying principles guiding review is the anticipation of problem areas before they arise. That means looking beyond the issue of whether an unlawful activity has occurred, to whether one might occur and what measures can be put in place to prevent it. I believe this type of proactive and preventive approach is essential in balancing the undisputable need for security and intelligence activities with the fundamental privacy rights we have come to expect in Canada.

Reviews under the Commissioner's general mandate

In the period covered by this report, I submitted two classified reports to the Minister of National Defence on subjects related to my general mandate[1] to review CSE's activities to ensure they conform with the law.

One of the reports involved a review of an operational program conducted by CSE under the authority of subsection 273.64(1)(a) of the *NDA*, often referred to as CSE's foreign intelligence mandate. In this instance, my findings indicated that CSE had acted lawfully in respect of this program. Moreover, employees assigned to this program demonstrated knowledge and awareness of the relevant law and policy that governed it.

The other classified report to the Minister concerned my review of a subset of activities conducted by CSE under the authority of subsection 273.64(1)(c) of the *NDA*, in response to requests for assistance received from federal law enforcement agencies.[2] In this regard, the RCMP is CSE's primary client. When providing assistance to the RCMP, the scope of which is limited and defined in policy, CSE does so as an agent. Before agreeing to act in that capacity, however, CSE must first satisfy itself that the RCMP is authorized to make the request and then be satisfied that it has the authority to provide the assistance the RCMP has requested.

My office examined CSE's assistance to the RCMP under mandate (c) for the year 2003. Based on the activities reviewed, CSE's assistance was found to be in compliance with the law.

---

[1] See Annex A.

[2] 273.64(1) The mandate of the Communications Security Establishment is:
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

That being said, however, both reports included recommendations, many of which concerned certain weaknesses in CSE's policies and procedures, an area that has drawn similar attention and mention in previous reviews. I have also recommended that CSE accelerate efforts to improve and update existing information and records management systems. At the time of writing, CSE had resolved some of these issues and had committed to address the remainder in the coming months.

Reviews of activities under ministerial authorization (MA)

As stated, it is my practice to conduct *ex post* review. In the case of CSE's MA-related activities, my reviews are undertaken once the authorizations in question expire.

My focus for the year under review was on activities conducted by CSE under the authority of three MAs, all of which concerned foreign intelligence collection and were the subject of classified reports to the Minister.

In conducting review activities for MAs, my office is guided directly by the legislation, which dictates what activities CSE can and cannot undertake. Specifically, my reviews in this area focus on the interception of private communications, which is what an MA authorizes. A private communication is defined in section 183 of the *Criminal Code* as

> … any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone

> communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it…

For the purpose of foreign intelligence collection, the *NDA* authorizes CSE to intercept private communications as long as the interception was the result of its having directed activities at a foreign entity located outside Canada. Over the past two years, I have focused much of my attention on foreign intelligence MAs because of their broad scope and potential degree of intrusiveness on the privacy of Canadians. While information technology security (ITS) MAs also authorize the interception of private communications, CSE seeks such authority in every instance at the request of the client agency whose systems and networks are being verified.

In my last annual report, I observed that a number of my concerns had been resolved, while some others remained. During this past year, I have been able to bring clarity to points of law and interpretation with respect to CSE's activities conducted under the authority of these provisions. My office engaged in discussions with staff and officials at CSE throughout this process.

For jurists who are accustomed to dealing with warrants issued by judges, a foreign intelligence MA is a strange sort of creature. However, one must take into account that, when collecting foreign intelligence, CSE is directing its interception efforts at foreign communications, or at least at the foreign end of communications, and a warrant issued by a Canadian court has no jurisdiction outside Canada in this instance.

Foreign intelligence MAs are a unique solution to an equally unique set of circumstances that can arise when CSE recognizes that an intercepted communication either leads into or flows out of Canada. While the interception has not been directed at a communication in Canada, one end of the communication is in Canada and is therefore, by law, a *private communication*. If this communication contains information essential to international affairs, defence or security, as specified in CSE's legislation, it is reasonable that the Government of Canada would want CSE to retain and report on it.

The foreign intelligence MA provisions in Part V.1 of the *NDA* include four conditions that must be met before the Minister of National Defence will authorize the interception of a private communication. I am of the opinion that their inclusion is both reasonable and consistent with other legislation that establishes an authority to engage in activities that would, in the absence of adequate justification, be judged an infringement on the rights of individuals as protected by the *Charter of Rights and Freedoms*.

In my view, these MA provisions are an exception to Part VI of the *Criminal Code* that protects against the invasion of privacy. I have no doubt as to their purpose because the *NDA* explicitly authorizes the interception of private communications subject to the threshold established by the four conditions, and to ministerial review. From my examination of private communications intercepted by CSE, I am able to determine if CSE has met the conditions imposed in the MA – for example, I know if the interception was a result of activities directed at a foreign entity outside of Canada. I can also determine if the communication was lawfully used, retained or destroyed – that is to say, whether or not it was

essential to the international affairs, defence or security of Canada.

In light of the above, I believe my review of activities that CSE has conducted under a foreign intelligence MA must focus on the intercepted private communications that CSE identifies to me as having been recognized and retained during the term of the authorization.

The Minister of National Defence is aware of how I have interpreted and will continue to discharge my mandate in respect of foreign intelligence MAs. I have also provided the Minister with my interpretation of the MA provisions, as currently written, and what they allow for in law. Further, I have made specific suggestions as to what could be done to remove ambiguities and to ensure a common understanding of the operational application of these provisions.

Review of past recommendations

There is substantial evidence that I believe supports my office's review function and the impact it has had on CSE's internal processes over the years. When warranted by the review findings, I may include recommendations for action on the part of CSE. My recommendations are, appropriately, non-binding. Binding recommendations would usurp the prerogative of both the Minister, who has overall responsibility for CSE, and of the Chief of CSE, who is responsible under Part V.1 of the *NDA* for the management and control of the organization. However, one of the concerns with a review body whose recommendations are non-binding is whether that review is effective or not. I can say with confidence that review works, based on my experience with CSE's response to the recommendations made by my office.

As I outlined in my previous annual report, last year we began a process to track CSE's response to the recommendations my predecessor and I made in

classified reports submitted to the Minister of National Defence since 1996. I am pleased to provide an update. A process has also been put in place to ensure a timely response to recommendations made in upcoming reports from my office.

Over the past year, my staff worked closely with CSE to monitor their response and subsequent actions with respect to the recommendations – including establishing timetables and target dates for completion. Of the 77 recommendations made from 1996 to the end of the current fiscal year, the majority have been accepted and implemented, and I am awaiting what I believe will be a positive response from CSE on a number of others. Many of the recommendations address broad policy issues such as formalizing relations, while others focus on technical and operational practices, including ensuring consistent definitions and appropriate accountability structures. That being said, the ultimate goal of all recommendations I make is to prevent conditions or practices that have the potential to lead to unlawfulness or that could affect the privacy of Canadians. I believe that this tracking process for recommendations is fundamental to achieving this goal.

I commend the Chief of CSE on the extent to which he has accepted review as an integral part of the vision for his organization. As well, I would like to express my appreciation to CSE for their co-operation and willingness to monitor the recommendations.

2004-2005 findings

Each year, I state my findings about the lawfulness of CSE's activities based on the reviews my office has conducted over the past year. I am able to report that I am satisfied that the CSE activities examined during the period under review complied with the law. Moreover, I am satisfied that the intercepted private communications I examined were lawfully acquired, used and retained.

Complaints and concerns about CSE Activities

Under Paragraph 273.63 (2)(b) of the *National Defence Act*, I am required to respond to a complaint by undertaking any investigation I consider necessary to determine whether CSE is engaging in unlawful activity. At various fora, people have expressed their surprise at the limited number of complaints directed toward my office over the years.

To my mind, the likelihood of a public complaint is diminished by the nature and focus of CSE's activities, which are technology-based and directed at foreign entities outside Canada. Unlike other federal intelligence or law enforcement agencies, CSE neither has a public profile nor engages in activities that place it in the public domain. During 2004-2005, I received no complaints about CSE activities from any source.

THE COMMISSIONER'S OFFICE

The reviews that my office conducts are in-depth and multi-faceted, taking months to complete. I place great importance on ensuring that they are carried out with methodological rigour and consistency. Last year, I requested an internal study of my office's own review processes and I am satisfied that it employs the full range of appropriate analytical and investigative review methodologies that are best practices in the public and private sectors. Briefings, multi-level interviews, the examination of a broad range of hard and soft copy records holdings, (including authorities, policies, legal opinions and operational files), legal research, inter-agency consultation and debriefing sessions are just some of the elements that constitute this process.

During the past year, my staff also upgraded its electronic record-keeping system, known as RDIMS (records/document information management system). It is designed to improve the security, retention and access to both

non-electronic and electronic documents. This has enhanced my office's ability to track and manage its internal records.

In support of the review function, my office maintains a full-time working staff of eight, as well as a complement of contract professionals who bring a range of expertise and experience in a variety of related fields. For example, some of my staff have had considerable exposure to Canada's security and intelligence community; others have special expertise in information technology, research, policy development and communications. As a result of a multi-phase staffing initiative that was completed in June 2004, my office has been operating at full strength for almost a year. I do not anticipate further staffing requirements in the near future, provided the tempo of activity remains unchanged.

To ensure that my staff stays connected to and engaged in the broader issues facing the security and intelligence community, we host informal presentations by representatives of government and academia working in the security field. Last year, on five occasions, we invited presenters to speak about, and share in discussions on, Canadian intelligence priorities in such subject areas as terrorism, information technology and the law, and privacy.

As part of my efforts to ensure awareness of the role of the Commissioner, last year my staff – at CSE's invitation – began to give presentations to new CSE employees as part of their orientation course. This contributes directly to CSE's fulfillment of the Ministerial Directive on Accountability Framework, which is designed to ensure that CSE personnel are aware of the Commissioner's mandates of *determining whether those activities (of CSE) are in compliance with the law and of investigating complaints by citizens,*

including CSE employees, or permanent residents of Canada concerning the lawfulness of such activities. The Chief of CSE is also directed to ensure CSE employees extend *full support and cooperation* to the Commissioner in carrying out his mandate.

In the interests of sharing expertise and learning about timely issues, my staff attended two conferences in October 2004: the International Intelligence Review Agencies Conference (IIRAC) in Washington D.C., and the annual Canadian Association for Security Intelligence Studies (CASIS) in Ottawa. In March 2005, I was invited to participate in a symposium on Counter-terrorism and the Law held at the University of Ottawa. While I declined to be a member of the panel, I took the opportunity offered me to address the participants, and I offered a few thoughts for their consideration. In addition, and for the second year, one of my staff will participate in the National Security Studies Seminar organized by the Canadian Forces College and planned for April. These events allow for the exchange of ideas and information on issues of mutual interest and concern, and help to keep us abreast of developments in the world that affect intelligence and review.

During the past year, my office's annual expenditures were $966,781. I am able to report that, once again, I discharged my mandated activities within budget. Annex B to this report provides a statement of my office's expenditures.

SHAPING THE REVIEW ENVIRONMENT

It goes without saying that Canada's security and intelligence sector – as well as its various review mechanisms – will be shaped by the important parliamentary and government initiatives currently underway. As discussed earlier in this report, the ongoing three-year review of the omnibus

Anti-Terrorism Act, the recommendations on review mechanisms for the RCMP that are anticipated from the Arar Commission and the proposed National Security Committee of Parliamentarians, all have the potential to make a substantial impact on the security and intelligence sector over the coming months and years.

As CSE Commissioner, I will continue to monitor these initiatives carefully and, wherever possible, make a positive contribution to the outcomes. I believe that the review community has much to offer and I welcome the opportunity to be part of the process. One of the principles guiding my input will be the need for a thoughtful approach to these issues, one that does not attempt to change what works, merely for the sake of change itself. While changes may certainly be called for, we must take care not to dilute what Parliament has put in place without due consideration and reflection.

CONCLUDING THOUGHTS

Despite the fact that the past year has posed many challenges, I look back upon it with no small degree of satisfaction. It has been a successful year. Addressing certain ambiguities in law in respect of CSE's activities under Ministerial authorizations, and establishing how my office will increase its effectiveness in reviewing them, for example, are positive steps. I am heartened by the number of recommendations made since the creation of my office that CSE has accepted and implemented, and by the ongoing dialogue between CSE and ourselves.

On a broader note, I am fully persuaded that review agencies such as my own can make an important contribution to the ongoing debate between the considerations of security and of privacy. Western democracies must make difficult choices as to where to draw the line at a time when asymmetric

threats are a part of our reality, and it is not an easy debate.

At a recent symposium on Counter-terrorism and the Law held at the University of Ottawa, and referred to earlier, my former colleague Supreme Court Justice Ian Binnie raised questions for discussion by the panel. He observed that the greatest threat to our rule of law is terrorism, and in matters of security it is absolutely necessary for the courts to show deference to state agencies because they have more expertise, information and resources on such matters than the courts. He questioned, however, at what point this deference should stop. While I do not have an easy answer to Mr. Justice Binnie's question, I know that it is one that merits serious contemplation given the challenges our contemporary society faces.

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.

"**15.** (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:

"**15.** (5) (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."

Statement of Expenditures 2004-2005

Standard Object Summary

Salaries and Wages	514,130
Transportation and Telecommunications	20,688
Information	18,293
Professional and Special Services	216,889
Rentals	142,454
Purchased Repair and Maintenance	105
Materials and Supplies	8,581
Acquisition of Machinery and Equipment	45,464
Other Expenditures	177
Total	**$966,781**

Classified Reports, 1996-2005

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

Classified Report to the Minister
– Operational Policies with Lawfulness Implications – February 6, 1998 – (SECRET)

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

Classified Report to the Minister
– Internal Investigations and Complaints – March 10, 1998 (SECRET)

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

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

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)

Classified Report to the Minister
– A Study of the *** Collection Program – November 19, 1999 (TOP SECRET Codeword/CEO)

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

Classified Report to the Minister
– A Study of the *** Reporting Process – an overview (Phase I) – December 8, 1999 (SECRET/CEO)

Classified Report to the Minister
– A Study of Selection and *** – an overview – May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
– CSE's Operational Support Activities Under *** – follow-up – May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
– Internal Investigations and Complaints – follow-up – May 10, 2000 (SECRET)

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

Classified Report to the Minister
– CSE's Policy System Review – September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
– A study of the *** Reporting Process – Phase II *** – April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
– A study of the *** Reporting Process – Phase III *** – April 6, 2001 (SECRET/CEO)

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

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

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)

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

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

Classified Report to the Minister
– Lexicon – 26 March 2003 (TOP SECRET/COMINT)

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

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

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

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

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

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

Classified Report to the Minister
– Review of CSE XXX Operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

Classified Report to the Minister
– CSE's Support to XXX – January 7, 2005 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
– External Review of CSE's XXX Activities Conducted Under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
– A Study of the XXX Collection Program – March 15, 2005 (TOP SECRET/ COMINT/CEO)