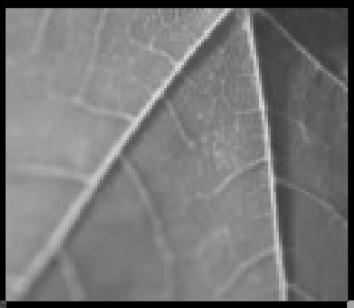
COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report



2003-2004

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 0-662-68250-5
Cat. No. D95-2004

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.

June 2004

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 sub-section 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2003-2004 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

CONTENTS

INTRODUCTION

This is my first report as Communications Security Establishment (CSE) Commissioner following my appointment on June 19, 2003.

During my twenty years on the Supreme Court of Canada, ten of them as Chief Justice, I witnessed and participated in the evolution of human rights and freedoms in this country, as we grappled with the application and impact of the *Canadian Charter of Rights and Freedoms*. This experience dovetails very well with my duties as CSE Commissioner, because safeguarding the rights of Canadians, including in particular the right to privacy, is an important element, although not exhaustive, of my mandate. In accepting this order-in-council appointment last June, therefore, I was honoured and pleased to have the opportunity to continue serving my country in a meaningful way.

Since retiring from the Court, I have participated in independent reviews and inquiries. One lesson I took from those experiences was the value of working collaboratively when seeking change and reform. With this background, my approach to reviewing the activities of the Communications Security Establishment is essentially proactive and preventive. When reviewing CSE operations to ensure that no unlawful activity has occurred, I also look for the existence of preventive counter-measures to safeguard against situations arising in which unlawful activity *could* occur. In areas as vital as security and intelligence where Canadians' privacy is at stake, I believe this approach is not only warranted but essential in establishing the appropriate balance between the demands of security and intelligence and the privacy rights of Canadians.

Under this approach, if I had concerns as a result of a review conducted by my office, my first step would be to share those concerns with the relevant persons — the Chief of CSE and those who report

to him. This would afford them an opportunity to institute corrective measures or to explain to me why my concerns were unjustified. By proceeding in this way, it is my hope that when I submit classified reports to the Minister of National Defence, most of the problem areas I have identified will already have been addressed, and my report will have been rendered moot.

This approach has proved useful in the past, often resulting in prompt administrative action. As a result, it has been possible to improve the way things are done expeditiously and without confrontation. In this way, the review and reporting process becomes a vehicle not just for detecting unlawful activity but for preventing it in the first place. When constructive criticism is accepted in the spirit in which it is intended, this approach works to the benefit of all concerned.

THE YEAR IN REVIEW

To prepare myself for the work ahead, in the first few months after my appointment I received several briefings from my own staff and from officials at CSE, including meetings with the Chief and his executive team. I met with the Minister of National Defence as well as his predecessor. I also met with the Security Intelligence Review Committee and with the Security and Intelligence Coordinator, who is also the National Security Advisor to the Prime Minister, and to whom the Chief of CSE reports for matters of operations and policy.

What quickly became apparent to me was the array of challenges facing CSE and the rest of the intelligence community in light of globalized threats with implications for Canada's international affairs, defence and security. The need to monitor and understand these threats is vital, yet efforts to do so have been curtailed in recent years by what has become an increasingly complex web of global communication technologies. Significant

challenges to foreign intelligence collection — one of CSE's primary mandates — also arise in this environment.[1]

These and other new demands led to legislative amendments and the development of new legal frameworks that should meet two objectives: first, facilitating the activities of intelligence agencies; and second, requiring that those agencies meet certain standards and respect certain thresholds that allow them to define and account for their activities.

In parallel with technological development to permit foreign intelligence collection in an ever expanding and complex global communications environment, it is also important to develop technologies that enable intelligence agencies to protect the rights and privacy of Canadians. In other words, technology developed for purposes of acquiring information from the global information infrastructure *must* be complemented by technology that can be used to protect privacy. It is in this context that the need for review of CSE's activities remains high.

Against this backdrop, several general issues related to foreign intelligence collection drew my attention in the past year; two in particular warrant discussion here.

Governing authorities for foreign intelligence collection

Canada's intelligence requirements, including its foreign intelligence priorities, are established annually by the Ad Hoc Committee on Intelligence Priorities (formerly the Meeting of Ministers on Security and Intelligence), chaired by the Prime Minister. Several federal agencies, including the Communications Security Establishment, contribute to meeting these priorities.

[1] *Foreign intelligence* is defined in the *National Defence Act* as information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security (Part V.1, section 273.61).

To carry out its foreign intelligence mandate, the CSE relies on the authority of the *National Defence Act (NDA)*,[2] which empowers CSE 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". When CSE does this, it is acting as a *principal* provider of foreign intelligence.

In addition, CSE, under the authority of the *NDA*, assists other federal agencies in the performance of their lawful duties. In these instances, CSE does so as an *agent*. In providing technical and operational assistance to federal law enforcement and security agencies, CSE is strictly governed by the terms and conditions of the principal's governing authorities, which in some instances may be a warrant from the Federal Court of Canada.

These two roles — as principal and agent — were formalized in legislation in 2001, but they are not new for CSE. What is new is CSE's authority under the *NDA* to intercept private communications, under prescribed conditions, if authorized to do so by the Minister of National Defence.[3] With a ministerial authorization, CSE can intercept and use a communication with a connection to Canada (that is, a 'private communication') acquired in the course of targeting a foreign entity abroad, provided it meets certain conditions laid out in the

---

[2] R.S.C. 1985, c. N-5.

[3] *Private communications* are the communications of Canadians or persons in Canada. Specifically, *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.

NDA. This provision adds a new authority to the legal framework within which foreign intelligence can be lawfully acquired.

From my initial review of some foreign intelligence collection activities, I had concerns that, in some instances, the linkages between these activities and the authorities that govern them were not being given due consideration. I was pleased to learn, therefore, that during the past year the legal frameworks available to the intelligence community for foreign intelligence collection were revisited to ensure that all available authorities had been fully considered before foreign intelligence activities were authorized. I encourage the government to continue to do so.

Ministerial authorizations

Historically, governments have relied on intelligence gathering as part of their efforts to protect and promote national interests and to identify and counter threats to those interests. The advent of new technologies, along with revolutionary developments in the communications industry over the past decade, have hindered some traditional forms of intelligence collection, including the foreign signals intelligence collection performed by CSE.

In the not so distant past, foreign intelligence collection was fashioned around predictable communications patterns and technologies. As a result, it could be conducted within relatively neatly defined legal frameworks. This environment facilitated the review and assessment of foreign intelligence collection activities. During my first year as CSE Commissioner, however, I quickly understood that this is no longer the case. Governments have had to reassess their ability to protect national interests and counter activities such as terrorism that threaten domestic and international security. Canada is no exception.

New legal mechanisms were needed to respond to this changing environment. One response was the ministerial authorization (MA) provisions in Part V.1 of the *National Defence Act*, added to the Act in 2001.[4]

Today's integrated technologies carry different kinds of traffic and follow complex communication paths that transit international borders and mix foreign communications with private communications. The MA provisions do not allow CSE to target Canadians or their communications. (CSE has never been allowed to do this.) Today, however, CSE is in a better position to fulfil its foreign intelligence responsibilities because, with the Minister's consent, it can follow targeted foreign communications even if they have a connection with Canada. I believe that few Canadians would disagree with the intent of this provision and the authority it provides in today's context of terrorism and threats to Canadians' safety and security.

Since the new legislation was passed, I can confirm that CSE has exercised this authority. As CSE Commissioner, I understand the need for it and support its objective. Subsection 273.65 (8) of the *NDA* requires that I review CSE activities carried out under an MA to ensure that they are authorized and report annually to the Minister.

---

[4] Part V.1 was added to the *National Defence Act* by the *Anti-Terrorism Act*, which became law on December 24, 2001. Before issuing a ministerial authorization, the Minister must be satisfied that the four conditions set out in subsection 273.65 (2) of the *NDA* have been met:

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

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

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

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

I believe CSE's policies, instruments and processes must require and facilitate the management and accountability of any activities it conducts under the authority of an MA, particularly activities that relate to intercepting private communications and safeguarding the privacy of Canadians. While this is an evolving process, I can report that CSE has continued to improve the MA structure and strengthened the MA management and accountability mechanisms.

Report of the Auditor General of Canada

The Auditor General's November 2003 report was tabled in Parliament on February 11, 2004. Chapter 10 of the report — Other Audit Observations — included an audit note, headed *Independent reviews of security and intelligence agencies*, that went on to state, "The activities of security and intelligence agencies are not subject to consistent levels of review and disclosure."

The report suggested that the CSE Commissioner's annual report should be expanded beyond considering CSE's compliance with the law to include such topics as management issues or potential problems at CSE. I believe that a review of the annual reports produced by this office to date will confirm that these areas have, in fact, been considered as they relate to two of the organization's business lines, foreign intelligence collection and the protection of government information systems and networks.

For example, over the past several years, reviews have led to observations in such areas as CSE's strategic planning activities; internal policies, procedures and handling practices; and management and control frameworks. These observations have always been made, however, in the context of lawfulness and CSE's efforts to safeguard the privacy of Canadians.

I believe the content of the CSE Commissioner's public annual report must be guided by his mandate, which is to review and report on CSE's activities to ensure that they are in compliance with the law, and to report to the Minister of National Defence annually on the Commissioner's activities and findings.

2003-2004 ACTIVITIES

I submitted a total of five classified reports to the Minister of National Defence over the period covered by this report. Two of these were initiated by my predecessor and completed during the first year of my term.

Reviews under the Commissioner's general mandate

In 2003-2004, I submitted three classified reports to the Minister of National Defence on subjects related to my general mandate to review CSE's activities to ensure they conform with the law.

Submitting a classified report to the Minister does not mean that a lack of compliance with the law or ministerial authority has been detected. It indicates only that the report contains material that requires classified handling. I report to the Minister on all my reviews, either to provide assurance or to bring concerns to his attention, as each specific situation requires.

Reviews of activities under ministerial authorizations

CSE conducted activities under seven ministerial authorizations in 2002-2003; two of these concerned foreign intelligence collection, while five related to information technology security. Within the time frame covered by this report, my office reviewed activities under five of the MAs; the others were nearing completion at the end of the reporting year. The five reviews resulted in two reports to the Minister, both covering information technology security activities.

None of the reports raised issues of unlawfulness.

However, a more general issue about the structure of and process for using ministerial authorizations did arise. Certain weaknesses in policies and procedures related to these activities were brought to CSE's attention. While some issues have been resolved, others remain. I hope to be able to report further on these issues in next year's report.

Annex C provides a list of all classified reports to the Minister submitted by my predecessor and me since the Commissioner's office was established in 1996.

Review of past recommendations

This year my staff reviewed all recommendations made by my predecessor and me in classified reports submitted to the Minister of National Defence since the creation of this office in 1996. The goal was to follow up with CSE on these recommendations and to determine whether the issues identified had been dealt with satisfactorily. I will be asking CSE for an annual update of this information.

The review showed that CSE's response to the recommendations has not been uniform. This is not surprising, given the diverse nature of the recommendations made to date: some could be implemented immediately; some related to policy or procedures; some were of a technical nature; and some required further study to determine their feasibility. Many related to how CSE can better manage and account for its activities.

Based on this review, I would observe that CSE has responded to many of the Commissioner's recommendations, but that a number of issues remain to be addressed, in particular, by establishing work plans and timetables with milestones and completion dates for specific corrective actions that CSE has acknowledged are necessary.

As I have made clear throughout this report, my recommendations and those of my predecessor are intended generally to be preventive, to forestall the

possibility of non-compliance by putting effective controls in place. It is in this spirit that I will continue to follow up on CSE's response to recommendations from my office.

2003-2004 Findings

I can report that the activities of CSE that my office reviewed during the past year complied with the law and with ministerial authority. It is important to place this assertion in context. It should not be taken to mean that I am certifying that all CSE's activities in 2003-2004 were lawful. I cannot make this assertion, because I did not review all their activities — and no independent reviewer could. However, my office reviews a wide range of activities in considerable depth, based on our assessment of where the risks of unlawful activity are likely to be greatest. This is the appropriate context for the assurance my work provides.

I should add, however, that during the course of reviews, I occasionally identify circumstances where there are clear and evident risks that unlawful activity might occur (arising, for example, from deficiencies in policies or practices). My predecessor and I have made a practice of reporting these circumstances to CSE and to the Minister. As I made clear in the introduction to this report, I believe it is ultimately more useful to prevent unlawful activity than to identify it after the fact.

Complaints and concerns about CSE activities

There were two complaints in the period covered by this report, but neither led to a formal investigation.

If I am to be in a position to assure complainants that CSE is not engaging in unlawful activity, my approach to complaints must take into account the mandate assigned to CSE under Part V.1 of the *National Defence Act*. Now, as before the introduction of Part V.1, CSE must not target

the communications of Canadians or persons in Canada. As discussed earlier, however, it is no longer possible to state unequivocally that both ends of a communication intercepted by CSE are foreign. CSE can now intercept (though it cannot target) private communications, provided it obtains a ministerial authorization in advance. CSE may also use and retain that communication, provided it adheres to guidelines that are also established in Part V.1 of the *NDA* (see footnote 4).

Any complaint submitted to me about CSE's activities must therefore be examined in this light.

No persons approached me to avail themselves of the public interest defence provisions of the *Security of Information Act*, subparagraph 15 (5)(b)(ii).[5]

THE COMMISSIONER'S OFFICE

Office expenditures and staff

Since 1996, when the position was first created, the mandate of the Communications Security Establishment Commissioner — and hence the staff and other resources required to carry out that mandate — have undergone considerable evolution. Between June 1996 and December 2001, the Commissioner's role was twofold: to review CSE's activities to determine whether they conformed with the law, and to receive complaints about the lawfulness of CSE activities.

As discussed at length in previous annual reports and alluded to earlier in this report, two features of the *Anti-Terrorism Act* of December 2001 had a direct bearing on the Commissioner's functions: the review of CSE activities conducted under ministerial authorization and the Commissioner's duties under the *Security of Information Act*.

---

[5] R.S.C. 1985, c. O-5.

To fulfil these new responsibilities, my office was allocated additional resources to carry out review activities. A bigger workload and more staff have affected the way we organize and manage our work. For example, our internal policies and procedures for managing the office have been enhanced to reflect the maturation of the organization and the increase in staff during the fiscal year.

We have also paid attention to our work methods. Tools such as a standardized methodology, scope statements, and guidelines structure our reviews of CSE's activities in such a way that all reviewers are working to the same standards of rigour and thoroughness. With the addition of more staff involved in these endeavours, my office has embarked on an initiative to record and document these processes wherever possible.

With a new Commissioner and the evolution of the Commissioner's mandate over the past three years, it was time to look at how my office relates to the broader context in which it operates — in particular the federal government community and the security and intelligence community in Canada and internationally. A communications plan, developed this year with input from key players in Canadian intelligence, will help guide my office through the rapidly evolving intelligence and policy worlds.

For example, one objective of the plan is to communicate more regularly and systematically with interested groups and individuals — including the Canadian intelligence community, organizations that deal with intelligence issues, and academics specializing in the intelligence field — about the nature of my mandate, my approach to the job, and the activities of my office. This type of interaction could lead, for instance, to productive partnerships with academic specialists in areas of mutual interest and concern. In addition, conveying accurate,

timely information about the office will help avoid misunderstandings or speculation about who we are and what we do.

Among the first steps in implementing the plan were my meetings with the current and former Ministers of National Defence, the chair and members of the Security Intelligence Review Committee, and the National Security Adviser to the Prime Minister, mentioned earlier.

In addition, my staff met with academics specialized in security and intelligence matters and participated in meetings of the Canadian Association of Security and Intelligence Studies. My staff also took steps toward greater participation in the public service community — notably through meetings with other small agencies, particularly those whose mandates include reviews and complaints.

With regard to the broader security and intelligence community, my office received visiting parliamentarians from Sweden and the United Kingdom — both countries with similar concerns but different review models from Canada's. In the past the office would not have had sufficient staff resources to undertake this range of activities, but the hiring of a director of review and government liaison and a director of review and military liaison will permit continued involvement in these communities in the future.

LOOKING AHEAD

New national security policy

On April 27, 2004, the government tabled in Parliament its first national security policy, entitled *Securing an Open Society: Canada's National Security Policy*. The policy addresses a range of national security issues and provides guidance in six strategic areas: intelligence, emergency planning and management, public health, transport security, border security, and international security.

The policy also calls for the development of new structures and strategies that the government believes will enable it to anticipate and manage current and future threats to Canada's national security interests.

Among the changes in government structure announced on December 12, 2003, and confirmed in the national security policy announcement, was a proposal to establish a new committee of parliamentarians whose members would be sworn in as Privy Councillors so they could be briefed on national security issues.

These initiatives obviously have the potential to influence the activities of my office, but it is too early to say what the shape or extent of this influence might be. My staff and I will be following developments closely with a view to providing input where appropriate.

Proposed legislation

Two legislative proposals before Parliament at the end of this reporting year may have additional implications for my office:

- Passage of Bill C-7 (formerly Bill C-17), the Public Safety Act, 2002, would entail new responsibilities for the Commissioner. The bill amends the *National Defence Act* to confer significant new responsibilities on the Commissioner of CSE for reviewing the lawfulness of activities undertaken by the Department of National Defence and the Canadian Forces to maintain and protect their computer systems and networks and for dealing with complaints arising from such activities.[6]

---

[6] Bill C-7, An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety, 3rd Sess., 37th Parl., 2004; Bill C-17, An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety, 2nd Sess., 37th Parl., 2002.

- Bill C-14 (formerly Bill C-32) amends provisions of the *Criminal Code* and the *Financial Administration Act*, among other acts. It introduces new provisions, including a new authority to intercept private communications for the purpose of managing and protecting computer systems and networks. There is a question of how this bill will affect the provisions and passage of the proposed Public Safety Act, 2002, which has similar wording.[7]

My concerns are threefold:

- the fact that passage of both bills would establish different governing authorities dealing with essentially similar activities;
- the fact that passage of Bill C-7 would impose on the Department of National Defence a different accountability regime than would be imposed on other departments by passage of Bill C-14; and
- the difficulties I am likely to encounter in providing meaningful assurance of lawfulness and compliance with ministerial authority as envisaged in Bill C-7.

Developments in two other areas may also have implications for my office:

- Parliament's statutory review of the *Anti-Terrorism Act* three years after its initial passage into law is slated to begin by the end of 2004. I intend to provide my comments based on my observations to date.
- The government introduced Bill C-25, the so-called whistle-blower legislation, on

[7] Bill C-14, An Act to amend the *Criminal Code* and other Acts, 3rd Sess., 37th Parl., 2004; Bill C-32, An Act to amend the *Criminal Code* and other Acts, 2nd Sess., 37th Parl., 2003.

March 22, 2004.[8] Although CSE would be exempt from this legislation, it would have to establish a system to serve essentially the same purpose, raising questions about a possible role for the Commissioner.

We will be following these and other developments closely to determine their likely impact on this office, as well as where and how we can contribute our input most effectively.

Review agencies conference

The next International Intelligence Review Agencies Conference will be held in Washington, D.C., in October 2004. Representatives of review agencies from Australia, Canada, New Zealand, the United States, the United Kingdom and other countries will meet to exchange views on issues of common interest. I look forward to receiving this year's agenda.

CONCLUDING THOUGHTS

Looking back over the year, I would like to thank my predecessor as Commissioner, the Honourable Claude Bisson, O.C., who laid a strong foundation for the Office of the CSE Commissioner and from whom I inherited a superb staff and an organization well positioned to meet the challenges ahead. Thanks to this legacy, the transition between our tenures was smooth, and I was able to assume my responsibilities quickly and efficiently.

Based on my experience over the past nine months, I believe that my mandate and resources as Commissioner are adequate to discharge my legislated duties. I look forward to continuing the productive relationship established with the Minister, with CSE and with other government officials as we fulfil our respective roles in Canada's security and intelligence community.

---

[8] An Act to establish a procedure for the disclosure of wrongdoings in the public sector, including the protection of persons who disclose the wrongdoings. Its short title would be the Public Servants Disclosure Protection Act, 3rd Sess., 37th Parl., 2004.

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 2003-2004

Standard Object Summary

Salaries and Wages	352,505
Transportation and Telecommunications	22,227
Information	43,201
Professional and Special Services	246,323
Rentals	134,794
Purchased Repair and Maintenance	42,019
Materials and Supplies	9,708
Acquisition of Machinery and Equipment	51,451
Other Expenditures	104
Total	**$902,332**

Classified Reports, 1996-2004

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)