Communications Security Establishment Commissioner

Annual Report

2000 ↓ 2001

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 0-662-65817-5
Cat. No. D95-2001

Communications Security
Establishment Commissioner

The Honourable Claude Bisson, O.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

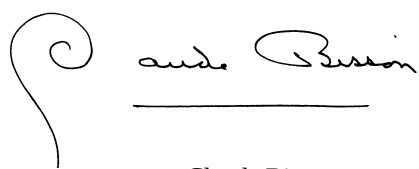
May 2001

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

Dear Mr. Eggleton:

Pursuant to paragraph (g) of Order in Council P.C. 1999-1048 re-appointing me Communications Security Establishment Commissioner, I am pleased to submit to you my 2000-2001 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,



Claude Bisson

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

In the five-year period since my appointment, I have observed the emergence of complex global communications technologies, together with evolving political, social and economic realities. This environment has led to the identification of new threats to Canada's security, defence and national interests and a pressing need for the Government of Canada to determine how to counter these threats.

During this same period, the Communications Security Establishment (CSE) has sought to maintain its ability to meet the government's evolving foreign intelligence priorities and to protect the integrity of its communications and information systems.

I believe that a failure to maintain CSE's capabilities would have serious implications for Canada's national interests. For example, if CSE were unable to report on the activities and intentions of foreign states and persons, Canada's political and economic well-being would be at risk. Furthermore, if CSE could no longer protect government information systems and assets, the government's efforts would be crippled in the areas of electronic service delivery and e-commerce, ultimately to the detriment of Canada's economic competitiveness.

Technological advancements will certainly continue and may even accelerate. CSE's senior management has informed me that they are convinced CSE must refocus its efforts to meet its responsibilities to government, or risk lagging behind. As a result, in consultation with its stakeholders, CSE has adopted a renewed strategic approach to its mandate.

This is the environment in which I continue to examine CSE's activities to determine their compliance with the laws of Canada and to assess CSE's efforts to safeguard the privacy of Canadians.

As in my previous annual reports, I will look back in this 2000-2001 Annual Report on CSE's performance over the past year.

CSE TODAY

Mandate

CSE, an agency of the Department of National Defence, assists the Government of Canada in two distinct but related areas:

- It provides the government with foreign intelligence by collecting, analyzing and reporting on foreign radio, radar and other electronic signals (signals intelligence, or SIGINT).
- It helps ensure the Canadian government's telecommunications and information technologies are secure from interception, disruption, manipulation or sabotage (information technology security, or ITS).

The Minister of National Defence is fully accountable to Parliament for CSE. He is supported by two senior officials — the Deputy Minister of National Defence, for financial and administrative matters, and the Deputy Clerk of the Privy Council, Counsel and Security and Intelligence Coordinator, for policy and operational matters.

Signals Intelligence

CSE's SIGINT program is guided by the foreign intelligence priorities established annually by the Meeting of Ministers on Security and Intelligence, chaired by the Prime Minister.

To fulfill its SIGINT mandate, CSE acquires various modes of foreign communications signals. The collection and processing of these signals involve highly sophisticated and complex technologies. Processing often includes the decryption and translation of encrypted communications to make them intelligible.

Encryption falls within the science known as cryptology, which uses mathematical algorithms to hide or disguise communications.

I have learned from CSE that advancements in global transmissions present continuing challenges to the collection and processing of foreign signals. The tremendous volume of communications signals produced every day, together with the increased use and public availability of encryption software, has added to these challenges.

As a result, CSE has dedicated additional resources to the research and development of techniques to acquire and process communications, so that the government can be kept apprised of threats to Canada's interests. To accomplish this, CSE relies on the capabilities of a cross-section of skilled workers, including computer scientists, mathematicians and linguists. To produce intelligence reports it also needs analysts knowledgeable in such matters as international political, economic and military affairs, terrorism, and transnational crime. These reports are the vehicle through which CSE communicates foreign intelligence information to its Government of Canada clients. More than 100,000 SIGINT reports are made available to CSE's readership every year.

Information Technology Security

The development and application of new technologies in recent years has transformed the focus and complexity of the activities undertaken by CSE to protect government communications and communications systems, the mandate of its Information Security Technology (ITS) program.

Until fairly recently, computer hardware, software and networks were not widely available and had limited application. Today, however, the computer is a fully established means of daily

communication among people. It drives many of the technologies that make up Canada's critical information infrastructure.

This communications environment has introduced new vulnerabilities to government information systems that require alternative solutions to counter threats to security and privacy.

The government looks to CSE to protect information stored or transmitted on its computer systems while, at the same time, departments and agencies work toward making a multiplicity of services available to the public on-line. Meanwhile, by law, personal information about Canadians must be protected, despite the fact that government computer systems are increasingly interconnected and vulnerable to disruption and to such threats as denials of service.

Relationships with allies

Canada benefits from longstanding arrangements between CSE and its counterparts in the United States, the United Kingdom, Australia, and New Zealand. These arrangements, which were formalized after the Second World War and maintained during the Cold War, allow for the exchange of signals intelligence, technology and information about sources and techniques of shared interest.

As part of my ongoing review of CSE's activities, I am satisfied that CSE does not use its partners to circumvent the laws of Canada, nor does it provide partners with communications they could not legally collect for themselves.

Controls on CSE's activities

Based upon my review activities to date, I have observed that CSE's activities are guided by law and policy and the government's priorities, not by its technical capabilities. In addition to my own reviews, CSE is also subject to the independent

scrutiny of many, including the courts, the Privacy Commissioner, the Information Commissioner, the Canadian Human Rights Commission, and the Auditor General of Canada.

Today's global communications networks generate an inordinate volume of information with which CSE must contend. This volume is in and of itself a control. In practical terms, CSE must stay focused on its mandate in order to meet the foreign intelligence priorities it is given.

CSE's recent contributions

The government uses CSE's intelligence reporting to further Canada's economic and political interests in its relationships with foreign states.

The Canadian Forces enter peacekeeping operations abroad with an enhanced understanding of the situation on the ground as a result of CSE's contributions.

CSE provides its government clients responsible for protecting public safety with information derived from foreign intelligence that contributes to efforts directed at countering terrorism, weapons proliferation, drug smuggling, illegal migration, and transnational crime. More recently, CSE has begun to provide these same clients with technical assistance.

CSE is working closely with the Canadian Forces Information Operations Group (CFIOG) to enhance support to Canadian military operations, with direct service now provided by CFIOG. (CFIOG was created in April 1998 from a consolidation of various National Defence elements, including the Canadian Forces Supplementary Radio Systems. It provides a focal point for Information Operations).

Through its ITS program, CSE continues to encourage and support Canadian firms in the development of new security products.

Additionally, CSE has an ongoing relationship with several government departments and agencies and assists them in assessing their ITS needs as they migrate toward on-line service delivery.

CSE provided senior level expertise to the government's Critical Infrastructure Protection Task Force. Created in April 2000, the Task Force recommended what the federal government should do to protect that part of Canada's infrastructure that is critical to the health, safety, security, and economic well-being of Canadians.

EVOLUTION OF CSE

The pressures for change

CSE must contend with the revolutionary pace of technological change. The foundation of its activities is technology, which affects CSE, like its partners, in several ways:

- The channels through which foreign communications travel are multiplying. The new wireless, fibre optic and Internet communications technologies continue to advance, requiring CSE's computer scientists and engineers to expand and upgrade their knowledge base constantly.
- The targets of foreign intelligence collection activities, including terrorist groups, now have easy access to the sophisticated products of a multi-trillion dollar telecommunications industry, including digital encryption technology, available as freeware on the World Wide Web, making it difficult if not impossible to decipher their communications.
- Increasingly, vast amounts of information are moving through new channels of communication, making it highly labour-intensive for CSE to identify useful information.
- Canadian government departments and agencies are also using new modes of communication that interconnect with computer systems that contain

sensitive information or control critical infrastructure. They look to CSE's ITS experts for advice to protect their communications networks and computer systems.

- The number of attacks on government networks and systems is growing. A September 2000 study on threats to federal Internet sites estimated that a typical site is subject to 10 or more threat incidents each week. Moreover, the frequency of foreign attacks on US systems that originate or pass through Canada is becoming an issue.
- The government's new Office of Critical Infrastructure Protection and Emergency Preparedness, announced in February 2001 and charged with developing and implementing a comprehensive approach to protecting Canada's critical infrastructure, will look to CSE for technical support.

CSE's strategic plan

During the year under review, CSE embarked upon an important strategic exercise to identify alternative approaches to delivering its mandate.

As a starting point, CSE defined its vision: "to be the agency that masters the global information network to enhance Canada's safety and prosperity". In so doing, CSE has effectively returned to its roots with the recognition that its core strength is its ability to understand and protect communications and communications systems. CSE's ability to exploit these systems to provide foreign intelligence flows from this core strength.

In support of its vision, CSE aims to become a centre of excellence that develops and applies its technical expertise and understanding of global communications networks and helps Canada meet its critical information needs.

CSE has adopted three strategic goals for the next 10 years:

- to be the acknowledged governmental centre of excellence in understanding and addressing the capacities of the global network
- to protect and enable the Canadian information infrastructure
- to modernize CSE services, products and delivery.

As a first step, CSE has strengthened the linkage between its SIGINT and ITS programs. Although their activities are related, they have traditionally operated at arm's length from each other. To achieve its strategic goals, CSE intends to benefit from the synergies created by drawing the two programs closer. By exploring the vulnerabilities of communications and information systems together, SIGINT and ITS experts now pool their knowledge to identify threats to Canadian systems as well as opportunities for foreign intelligence collection.

In June 2000, the Chief of CSE briefed me on this topic. Subsequently, my office has discussed the strategy in detail with CSE's senior management. I do not believe this approach will change how I review CSE's activities in any fundamental way, since my focus will remain on their lawfulness. In the meantime, I have expressed my support of this undertaking.

REVIEWING CSE

My mandate to review the activities of CSE and to report to the Minister of National Defence is contained in an Order in Council (see Annex A).

The Commissioner's role

Each year, my office identifies areas within CSE's operations where, at first view, questions of lawfulness might be presumed. Under my authority, my office then conducts systematic reviews of these

operations. I pass the results of these reviews to the Minister of National Defence in the form of classified reports. The fact that I have issued a classified report is not an indication that I have uncovered an incident of unlawfulness. Rather, it is an indication that the report contains sensitive information that requires classified handling.

The effort that goes into researching and preparing my reports to the Minister accounts for the bulk of the work of my office and gives me a detailed understanding of various aspects of CSE's operations.

I have reviewed CSE's authorities to collect foreign intelligence on behalf of the Government of Canada and its mandate to protect the security of the government's information technology. On an ongoing basis, I examine CSE's policies, directives and actual practices to ensure they contribute to lawfulness and to protecting Canadians' privacy.

Among other issues, my reviews have looked at how CSE provides intelligence reports to its clients, and the receipt of intelligence from its Second Party partners. I regularly monitor CSE's operational activities, as well as circumstances that have led to internal security investigations.

Annex B contains a list of the classified reports I have passed to the Minister since my appointment in 1996.

2000-2001 activities

Foreign intelligence product

During the past year, I continued to review CSE's activities as they relate to the intelligence cycle and the handling and production of intelligence product. As I outlined in my last annual report, CSE conducts daily reviews of the raw traffic it receives from multiple sources and assesses its foreign intelligence value against the government's

priorities. CSE then passes the results to its government clients in the form of intelligence product.

This past year, I reviewed the policies and handling practices associated with CSE's receipt and retention of foreign intelligence traffic. I examined how CSE identifies issues of intelligence interest within the raw traffic it receives and the practices associated with its retention and subsequent dissemination in the form of intelligence reporting. And, as is my practice, I reviewed CSE's policies and practices, within this cycle of activities, that deal specifically with safeguarding the privacy of Canadians.

Information management

I also reviewed CSE's information management policies in light of the National Archives of Canada Act and Treasury Board policy and guidelines related to the management of information holdings.

Government departments and agencies are required to establish Records Disposition Authorities for their operational and administrative holdings. These Authorities grant permission to departments and agencies to dispose of certain holdings and require them to forward to the National Archives other holdings identified to be of archival interest, for preservation.

I observed that these Authorities do not constitute a requirement to destroy records, nor do they provide direction regarding the timing of records destruction. Moreover, they do not provide or authorize records retention periods. Retention and disposal periods are determined by the designated Minister of the institution and must, of course, conform to any other applicable legislation.

I was satisfied that CSE's policies conform with existing law and policy requirements related to the management of government information holdings. I recommended, however, that CSE give priority to completing its retention and disposal schedules.

Policy authority

In my 1998-99 Annual Report, I indicated my intention to examine the new framework for policy authority, accountability and coordination that CSE had recently adopted. Of particular interest to me were two of the objectives of the framework: to identify the appropriate level of authority for various policies; and to provide a desirable level of operational flexibility in support of day-to-day activities.

During the past year, I reviewed the new framework and found it to be well conceived and sound. It will take time, however, to convert all CSE policy to the framework. While some policy gaps remain, CSE has policies for its major requirements, and the new system should address my earlier concerns about having policy in the right place and signed off at the right level.

During the year under review, I was pleased to learn that officials had opened discussions on having cornerstone internal policies issued to CSE as Ministerial direction. I applaud this initiative, because it will strengthen the accountability linkages between CSE and the Minister of National Defence, who is responsible for CSE in Parliament.

Other activities

My mandate authorizes me to investigate complaints by Canadians or permanent residents of Canada about CSE activities. While there were informal inquiries during 2000-2001, none led to a formal complaint.

During the past year, my office has maintained its informal contacts within the security and intelligence community. We were particularly pleased to receive the Inspector General of South Africa during his autumn 2000 tour of North America. I look forward to renewing acquaintances with my counterparts from other countries at the upcoming conference of review agencies in Washington in October 2001.

2000-2001 findings

I am satisfied that during the period under review, CSE acted lawfully in the performance of its mandated activities and did not target the communications of Canadian citizens or permanent residents. I make this statement on the basis of the thorough review of CSE's activities conducted during the year.

My mandate requires me to inform the Minister of National Defence and the Attorney General of Canada of any CSE activity that I believe may not be in compliance with the law. To date, I have not been required to do so. CSE is aware of its boundaries, receives legal advice from counsel appointed to CSE by the Department of Justice, and has policies and procedures in place to promote lawfulness. These measures have proven to be effective.

Office staff and budget

During the 2000-2001 fiscal year, my budget allocation was $648,800. I can report that actual expenses incurred were well within budget.

My office continues to consist of two full-time employees and a number of subject-matter experts whom I employ on contract. At present, there are five people performing specialized work under this arrangement, all of whom have the required security clearances. This provides me with both continuity and flexibility to obtain the expertise I require to review CSE's activities effectively.

LOOKING AHEAD

Safeguarding the privacy of Canadians

As I have previously observed, CSE's foreign intelligence collection technology must constantly progress to keep pace with advances in communications technology. Despite the efficiencies inherent in new technologies, CSE is still likely to receive inadvertently some small amount of Canadian communications. Moreover, each new collection system or technique that comes on stream seems to bring with it this potential. However, CSE is well aware that it must continually upgrade its capabilities to screen out Canadian communications or risk acting unlawfully if it does not make every effort to do so.

In this regard, I have informed CSE that, in addition to my other review activities, I will be seeking assurance that it is availing itself of all emerging technologies to ensure that the privacy of Canadians is safeguarded.

CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1999-1048
June 8, 1999

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence (in this order referred to as "the Minister")

(*a*) to re-appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("the Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;

(*b*) to authorize the Commissioner to commence that review on his own initiative or at the request of the Minister;

(*c*) to authorize the Commissioner to investigate any complaint, concerning the lawfulness of CSE activities, made by any individual who is a Canadian citizen or a permanent resident of Canada;

(*d*) to authorize the Commissioner not to investigate complaints for which, in the Commissioner's opinion, other avenues of redress are established by statute;

(*e*) to specifically authorize the Commissioner to inform any complainant of the results of his investigation, ensuring that no classified information is disclosed to the complainant;

(*f*) to direct the Commissioner to inform the Minister and the Attorney General of Canada of any CSE activity that the Commissioner believes may not be in compliance with the law;

.../2

(*g*) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not classified, which report the Minister will table in Parliament;

(*h*) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;

(*i*) to direct the Commissioner, before submitting any report to the Minister, to consult with the Deputy Secretary to the Cabinet (Security and Intelligence) at the Privy Council Office for the purpose of ensuring compliance with all security requirements and the preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(*j*) to direct the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

(*k*) to authorize the Commissioner to engage the services of any staff, advisors and counsel that he considers necessary to assist him in the performance of his duties and functions at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

.../3

(*l*) to fix the remuneration of the Commissioner at the per diem rate set out in the annexed schedule, which rate is within the range of $400 to $500; and

(*m*) to authorize that the Commissioner be paid reasonable travel and living expenses incurred by him in the performance of his duties and functions while absent from his ordinary place of residence, in accordance with Treasury Board travel directives;

effective June 19, 1999.

CERTIFIED TO BE A TRUE COPY–COPIE CERTIFIÉE CONFORME

CLERK OF THE PRIVY COUNCIL–LE GREFFIER DU CONSEIL PRIVÉ

Classified Reports, 1996-2001

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
- 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)