COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report

2008-2009

Canada

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

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

ISBN 978-1-100-12653-1
Cat. No. D95-2009E-PDF

Cover photos: Malak

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

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

June 2009

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 2008–2009 annual report on my activities and findings, for tabling in Parliament.

Yours sincerely,

Charles D. Gonthier

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

TABLE OF CONTENTS

INTRODUCTION

This is my third report as Communications Security Establishment Commissioner. It is an appropriate time, in my view, to reflect upon the nature of the work in which my office is engaged and the quality of the relationship that has evolved between the Communications Security Establishment Canada (CSEC) and my office.

Decades of legal experience have taught me that the most important element in any relationship is trust. This is true of all relationships, including the one between my office and CSEC. Trust, in my opinion, is not an entitlement. It is something that must be earned through integrity and professionalism. In the case of CSEC, it is also earned by demonstrating commitment to the protection of national security in a way that ensures compliance with the law and respect for the privacy of Canadians. In the case of my office, trust is earned through a rigorous, comprehensive and fair review process.

Due to the nature of its work, CSEC is required to operate largely in secrecy. The role of my office is, in part, to represent the public interest in accountability in a way that optimizes effective review while not restricting unnecessarily CSEC's legislated role.

My predecessors and I have consistently recognized prevention as an important aspect of the Commissioner's legislated role. As such, most recommendations address shortcomings in CSEC's policies, procedures and practices in order to strengthen the compliance framework and reduce any risk to privacy.

While I have, over the past three years, reported that I have found no instances of lack of compliance with the law, there may be, and have been, instances where disagreements with CSEC arise over a particular issue or where I am not satisfied with CSEC's explanation or information. In such cases, I direct my staff to pursue the issue as thoroughly as required. The manner in which such matters are handled can enhance professional trust between organizations.

As my first term draws to a close, I take satisfaction in noting that mutual trust and commitment to shared democratic values have fostered a productive working relationship. I acknowledge the leadership of CSEC which has demonstrated its commitment to lawfulness and protecting privacy.

THE REVIEW ENVIRONMENT

Proposed amendments to the *National Defence Act*

Ensuring the integrity of CSEC's activities and the review process

In last year's report I once again repeated my concern over ambiguities in Part V.I of the *National Defence Act* (*NDA*) with regard to CSEC's foreign intelligence activities under ministerial authorization. I recommended a number of amendments, including one to clarify the term *activity or class of activities*. I also recommended that a definition of the terms *intercept* and *interception* be inserted into the Act. I have shared with government officials these and other proposals for amendments to the *NDA* that I believe worthwhile to enact.

Ministerial authorizations — Did you know?

A ministerial authorization is a written authorization provided by the Minister of National Defence which sets out conditions CSEC must meet so as not to be in contravention of the *Criminal Code* if, in the process of conducting its foreign intelligence collection or information technology security activities, it incidentally intercepts private communications of Canadians. Ministerial authorizations may be approved or renewed for a period not exceeding one year.

Applying a qualified opinion

At the end of the 2008–2009 reporting period, I continue to apply the *interim* solution put in place by my predecessors: that is, to review CSEC's foreign intelligence collection activities under ministerial authorizations on the basis of the *NDA* as it is interpreted by Justice Canada. However, in some important respects, I disagree with that interpretation — as have both my predecessors.

In April 2006, my immediate predecessor noted in his last report as CSE Commissioner that "my one regret will be if I leave this position without a resolution of the legal interpretation issues that have bedevilled this office since December 2001." In my 2007–2008 report, I noted the Government had indicated that legislative amendments would be brought forward "in due course". This has yet to occur. I want to emphasize, however, that the length of time that has passed without producing amended legislation puts at risk the integrity of the review process.

Observations of the Auditor General

I am pleased to see that the Auditor General has commented on this important matter. In a report released on March 31, 2009, she recognized that the implications of the CSE Commissioner's qualified opinion of CSEC's lawfulness, due to ambiguities in CSEC's legislation, "are serious" (Section 1.14 of the *2009 Status Report of the Auditor General of Canada*).

Review cooperation

One issue that remained unresolved in 2008–2009, stemming from Justice Dennis O'Connor's report concerning a new review mechanism for the Royal Canadian Mounted Police's (RCMP) national security activities, is whether there is a need for integrated review of integrated operations among enforcement and intelligence agencies. Justice O'Connor's recommendations included "statutory gateways" to support integrated review. While cooperation among review bodies must be conducted in a manner that respects security requirements, including the *Security of Information Act*, I find no obstacles, legal or otherwise, to

such cooperation, if required. Moreover, I can, and do, review CSEC activities conducted under part (c) of its mandate — which involve requests for assistance to CSEC from the Canadian Security Intelligence Service (CSIS) and the RCMP — to ensure these activities are in compliance with the law.

The O'Connor inquiry included the examination of information sharing between agencies from different countries. This theme has been discussed by Canadian and international scholars. At the annual conference of the Canadian Association of Security and Intelligence Studies (CASIS), held in October 2008, reference was made to an "accountability gap", concerning an absence of cooperation between review bodies of different countries to review information sharing agreements among their respective intelligence agencies. This is a sensitive area but one that is of great interest to me, particularly as it relates to the potential sharing of personal information about Canadians. Within my own jurisdiction, in the coming year, I will be conducting a review of CSEC's activities in this area.

Parliamentary committee involvement

The Government of Canada has called for increased parliamentary involvement in the review of security and intelligence activities. Traditionally, a role for parliamentarians has been clearly established through the mechanism of Parliamentary committees: in the case of my office, it is the Standing Committee on National Defence, to which my public annual report is referred. Since the creation of the CSE Commissioner's office in 1996, the Commissioner has been invited to appear before this committee to discuss his activities and findings and to answer parliamentarians' questions quite infrequently.

Safeguarding privacy: Regular review of identity disclosures

Following my in-depth review of CSEC's disclosure of information about Canadians to Government of Canada clients, completed in December 2008, it was suggested by CSEC that reviews of this kind could be conducted on a regular basis. Since this CSEC activity lies at the heart of my mandate, I believe it is worthwhile to examine it regularly. As a result, my office has arranged with CSEC to begin reviews at regular intervals throughout the coming reporting year.

I believe the nature of this CSEC suggestion, and the manner in which it was presented to my office, speaks to the professional trust that has evolved in the relationship between our respective organizations. It is a positive sign, and one which I am pleased to highlight in this report.

Information about Canadians — Did you know?

When collecting foreign intelligence, CSEC may incidentally acquire information about Canadians. This information may be retained if it is assessed as essential to the understanding of the foreign intelligence. Information about Canadians may be included in foreign intelligence reporting only if it is suppressed (i.e. replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC requires federal departments and agencies to explain their authority to request and use this information under their respective mandates and to provide an operational justification of their need to know this information. Only after these conditions have been met will CSEC release the suppressed information.

Briefings from CSEC

My office is briefed regularly on CSEC operational policies and relevant administrative activities. In 2008–2009, my office was also provided with presentations and training in the areas of information management and information technology (IT) databases, on the safeguarding of IT networks of importance to the Government of Canada, and on the status of CSEC's policy framework. In addition, CSEC provided briefings specific to certain reviews prior to those reviews being undertaken.

More effective review through annual roundtables

For the past two years, my staff and CSEC officials have participated in what has become an annual roundtable meeting aimed at optimizing the review process, while minimizing any adverse impact on CSEC's legislated activities. The roundtable meeting is also an opportunity to reinforce open communication and to enhance mutual understanding and trust in the working relationship between the two organizations. These meetings have proven useful in removing obstacles to effective review and will, I am sure, enable us to make progress in the years ahead.

Strengthening lawful compliance

The objective of my review mandate is to assess whether CSEC's activities comply with the law, including the extent to which CSEC has adequate measures to protect the privacy of Canadians. While I am to report to the Minister and to the Attorney General of Canada any instances of non-compliance with the law, I also make it a point, wherever possible, to identify preventive measures that reinforce CSEC's lawful compliance.

One area in which my predecessors and I consistently called for preventive measures is improved information management practices. As we all previously noted, the absence of an adequate records management system impaired CSEC's ability to account for its activities. In response to these concerns, CSEC has taken positive steps to rectify gaps in record management practices. In fact, a new corporate records management system is expected to be fully operational during the 2009–2010 reporting period. CSEC is to be commended for its efforts in this important area.

A comprehensive review process

In its reviews, my office sometimes goes into great depth, observing CSEC operators and analysts first hand to gain better knowledge of their work. This knowledge is particularly important when my staff examine an area in which I have made a recommendation with which CSEC disagrees.

This year, in one such case, which I describe in the section on Review Highlights, I revisited a recommendation relating to privacy, which was made last year. Following completion of a second, focussed review, I retracted that recommendation because I was satisfied that the risk to privacy was minimal and that CSEC had appropriate safeguards in place. I believe this retraction results from a rigourous but fair review approach which, in this instance, recognized the professional manner in which these particular analysts strive to conduct their work.

Implementing recommendations — Did you know?

Since 1997, my office has submitted 52 reports to the Minister, many of which have contained substantial recommendations. CSEC has accepted and implemented and/or is working to address over 90 percent of these recommendations, which speaks to the effectiveness of the review process.

METHODOLOGY

Identifying risks to lawfulness and privacy

A key ingredient in developing a sound review selection process is the identification of activities, practices or procedures that may pose a risk to CSEC's compliance with the law. For example, these can be potential risks identified by my staff from previous or current reviews of CSEC activities, or from briefing sessions given to my staff by CSEC. CSEC may itself also identify potential risks.

In assessing topics for possible review, I instruct my staff to consider questions such as: to what extent is CSEC exposed to risk of unlawful activity in this area, and what is the likelihood that this could occur?; and if it occurs, what is the potential adverse impact?

In addition, my staff developed more detailed criteria in 2008–2009 to help determine the priority in which the identified areas of potential risk will be reviewed. These criteria, which continue to be refined, include: significant changes to authorities; changes to technology; any area that has never been reviewed in-depth, or has not been reviewed in the past four years; a follow-up to a particular recommendation I made previously; and issues arising in the public domain.

Attributes of a good review

In conducting a review, my staff examine all relevant written and electronic records, files, correspondence and other documentation. My staff conduct interviews with CSEC managers and staff involved in the activities being reviewed and visit CSEC facilities to conduct checks, including CSEC databases. The results of reviews are shared with CSEC and, in most instances, CSEC takes action to strengthen compliance with the law or policy.

One of my primary concerns in the review of CSEC activities is ensuring that each review is based upon appropriate evidence to support all findings, conclusions and recommendations. This means that all evidence gathered must be directly *relevant, replicable* and *valid.*

Review evidence — Did you know?

Evidence is information and data that are collected and used to provide a factual basis for developing findings and recommendations against review criteria.

Relevant: refers to the extent to which the information bears a clear and logical relationship to the review objective(s) and criteria. If information is not relevant, it cannot be evidence. *Replicable:* concerns the likelihood of coming up with the same findings if all steps of the review were reproduced. *Valid:* refers to whether the information actually is what it purports to be in relation to the content, origin and timing. As a general principle, the quantity of evidence is sufficient when there is enough to persuade a reasonable person that the review findings and conclusions are valid and the recommendations are appropriate. In order to decide if the collective weight of the evidence is sufficient, I must consider the quality of the evidence gathered, and the cost of obtaining more evidence relative to its likely benefits.

Developing review findings and recommendations

The comparison of evidence gathered against previously established review criteria results in the development of usable findings and recommendations. Review findings confirm whether criteria have been satisfactorily met, or disclose the level, nature and significance of deviations from them. The process of assessing the evidence gathered against criteria is focussed on questions such as: does a deficiency exist between findings and expectations and as established by the review criteria? what is the cause of the deficiency? what are its likely impacts? and can the deficiency be corrected?

2008–2009 REVIEW HIGHLIGHTS

During the 2008–2009 reporting period, my office completed seven reviews on different aspects of CSEC activities. The reviews were carried out under my authority as articulated in paragraph 273.63(2)(a) and subsection 273.65(8) of the *NDA*.

The primary objective of the reviews, consistent with my mandate, was to assess whether the activities complied with the law, including the extent to which CSEC has adequate measures in place to protect the privacy of Canadians. I am able to report that the activities examined in 2008–2009 complied with the law.

With respect to the first three of the reviews listed below, in which I have reviewed different foreign intelligence collection activities conducted under ministerial authorizations, I reiterate that, pending amendments to clarify the *NDA*, these reviews are based on legal interpretation provided to CSEC by Justice Canada.

Reviews of foreign intelligence activities under ministerial authorizations — Common elements

Paragraph 273.64(1)(a) of the *NDA* authorizes CSEC to collect foreign intelligence in accordance with the Government of Canada's intelligence priorities. In the case of each of the CSEC foreign intelligence collection activities reviewed by my office in 2008–2009, CSEC obtained the ministerial authorization pursuant to subsections 273.65(1) and (2) of the *NDA* because, in carrying out the activities, it was possible that CSEC might intercept communications that either originated or terminated in Canada, and which constituted "private communications", as defined in the *Criminal Code*.

The *NDA* requires that foreign intelligence collection activities not be directed at Canadians or any person in Canada (paragraph 273.64(2)(a)), and that they be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information (paragraph 273.64(2)(b)).

Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1)

Background

This review examined certain CSEC foreign intelligence collection activities conducted under three successive ministerial authorizations in effect between 2004 and 2007. Two previous reviews of these same activities conducted by my office in 1999 and 2005 respectively were taken into consideration.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements, and its operational policies and procedures.

However, the review found that additional information should be recorded and reported to the Minister in order to enhance accountability. This additional information concerns the foreign intelligence CSEC collects under this ministerial authorization and which it shares with its principal partners outside Canada. The sharing of information about Canadians is an area that my office will continue to examine.

The review also found that a memorandum of understanding between CSEC and a federal department respecting these activities should be updated to reflect current practices. In the meantime, CSEC agreed to continue to follow the terms of the existing agreement and to document any new understandings.

In addition, my staff identified certain deficiencies in CSEC policies and procedures related to the activities reviewed.

Recommendations

As a result of these findings, I recommended that CSEC adopt and publish additional written guidance respecting the process its analysts are to follow when making targeting decisions. I also recommended that CSEC amend its policy respecting the deletion of private communications recognized by analysts and found to have no foreign intelligence value. The *NDA* requires that an intercepted private communication shall be used or retained only if it is essential to international affairs, defence or security (paragraph 273.65(2)(d)).

I am pleased to note that CSEC accepted the recommendations, and is making improvements in areas where deficiencies were identified, including making changes to its systems.

Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2)

Background

This review examined certain other CSEC foreign intelligence collection activities conducted under four ministerial authorizations in effect from 2004 to 2007. The review included an examination of CSEC's reporting of the foreign intelligence to its partners in Canada and abroad.

Findings

Based on the information reviewed and interviews conducted, I found that the activities were authorized and complied with the law and with CSEC operational policies and procedures. Personnel responsible for the collection and management of intelligence activities were interviewed and found to be knowledgeable about the legislative authorities, policies and procedures that govern CSEC's collection.

However, the review also found that CSEC did not meet two of the expectations set out in the ministerial authorizations. In one instance, it was noted that CSEC did not meet a requirement to report in a timely manner to the Minister of National Defence following the expiration of the ministerial authorization. My staff found that the report was not received by the Minister's office until almost one year later.

Secondly, it was noted that in one instance CSEC did not report to the Minister an important increase in the number of private communications it inadvertently intercepted. CSEC subsequently provided my office with an explanation for this omission. Nevertheless, in reviewing this issue, I assessed that the information should have been reported in order to meet the ministerial expectation.

My report to the Minister of National Defence also suggested that CSEC introduce a greater degree of rigour in methodology applied to assessing the value of foreign intelligence reporting.

Recommendation

In addressing the expectation regarding private communications, I recommended that CSEC make an explicit statement to address each ministerial expectation separately in future reports to the Minister. I am pleased to note that CSEC accepted this recommendation.

Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3)

Background

This review examined a third type of CSEC foreign intelligence collection activity conducted under three successive ministerial authorizations in effect from 2004 to 2007. In addition, the review examined CSEC's compliance with the expectations set out in a related ministerial directive, issued pursuant to subsection 273.62(3) of the *NDA*.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were authorized and complied with the law. I did, however, set out specific findings and made recommendations that I believe would strengthen CSEC's practices and compliance with its policies and procedures.

The review also found that CSEC did not meet one expectation set out in the ministerial directive. However, practices at the working level resulted in the fulfilment of the intention of that expectation.

Rigorous business practices at the working level throughout the development, approval and execution of these activities give a high level of assurance that the activities are conducted as approved. The review did not find the same level of clarity, rigour and record keeping in some parts of the program management processes. As a consequence, I made three recommendations.

Recommendations

With respect to CSEC not meeting one expectation of the ministerial directive, and to ensure continuity of practice through time and any staff turnover, I recommended that CSEC include certain measures in its policies or procedures.

Second, while CSEC personnel demonstrated a clear understanding of associated policies and procedures, and there was no suggestion of non-compliance, I recommended that written guidelines be put in place to address certain deficiencies in policies and procedures.

Finally, the record of specific activities is comprehensively documented. In contrast, however, the record of decision related to the management of the program is incomplete. I recommended that both components be subject to the proper application of sound records management processes. As I observed previously, CSEC has been implementing a new records management system and is keeping my office informed of progress, which I am following with interest. I am pleased to note that CSEC has accepted these recommendations and is taking measures to address each of them.

Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians

Background

My office reviewed CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians, in accordance with subsection 273.64(2) of the *NDA*.

Two types of technologies were studied in this review: a foreign intelligence acquisition system and an analytical tool. The foreign intelligence acquisition system is used to acquire, process and collect information from the global information infrastructure. The analytical tool is used to support CSEC's collection of foreign intelligence and to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada (IT security). My staff observed demonstrations of the two technologies and queried CSEC operators on various aspects of their use.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were carried out in accordance with the law. CSEC uses these two technologies to fulfill its legislated mandate and demonstrated that it would modify its technologies, if required, to comply with its statutory obligations to protect the privacy of Canadians. The acquisition, implementation and use of these technologies helps CSEC protect the privacy of Canadians by identifying potential private communications as well as personal information about Canadians.

The review found that special attention should be brought to the development of IT security policy instruments so as to ensure that CSEC's guidance in this regard is up-to-date and formalized at the highest level. There was a difference in practices between CSEC's two business-lines (IT security and foreign intelligence collection) with regard to accounting for personal information identified through analysis. CSEC provided a reasonable explanation for this difference.

Recommendation

I made one recommendation regarding requests for foreign intelligence ministerial authorizations. Since there is a risk of intercepting private communications when using the foreign intelligence acquisition system reviewed, a ministerial authorization was required. I recommended that CSEC re-evaluate how it describes foreign intelligence activities in its requests for ministerial authorizations so as to be more precise about the activities the Minister of National Defence is authorizing. I am pleased to note that CSEC accepted the recommendation.

Review of disclosure of information about Canadians to Government of Canada clients

Background

As part of its mandate to provide foreign intelligence in accordance with Government of Canada intelligence priorities, CSEC disseminates classified reports to federal government departments and agencies that have demonstrated requirements for the information, based on their respective mandates. These reports are authored by CSEC as well as allied agencies and may contain suppressed information about Canadians if it is essential to the understanding of the report (see: *Information about Canadians — Did you know?*).

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities complied with the law and with its operational policies and procedures. I made no recommendations.

Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive

Background

Last year, I reported on certain activities undertaken by CSEC under a ministerial directive and in support of its foreign intelligence collection mandate. As indicated in my 2007–2008 Annual Report, I suggested that CSEC re-examine its practice that only those private communications recognized by certain staff be accounted for. I recommended that other staff who observe and handle private communications should also be responsible for accounting for them. CSEC did not accept this recommendation, and, as a result, I directed my staff to conduct a follow-up review of these activities.

This second, focussed review, with direction to probe this matter as deeply as necessary, aimed to acquire greater knowledge about this activity, to examine the risk to privacy, and to determine if CSEC's measures to protect the privacy of Canadians were sufficient in this instance.

The goal of this review was ultimately to determine whether my recommendation of 2007–2008 should be maintained, amended or retracted. Review methodology included first-hand observation of the activities of CSEC front-line personnel conducting this activity.

Findings

The review, based on detailed knowledge and understanding of activities observed by my staff, found that CSEC conducts these activities in accordance with the law and ministerial requirements, and in accordance with operational policies and procedures.

Based on the current practices, as observed in detail on two separate occasions, I assessed that the activities examined in this review involve only a low risk to privacy. CSEC staff conducting the activities have a different and lesser potential of affecting the privacy of Canadians than other staff conducting different activities and who are already required to account for private communications.

In addition, I assessed that CSEC has sufficient measures in place to protect the privacy of Canadians during its conduct of these activities. Personnel were aware of and followed operational policies and procedures that provide direction with respect to the protection of the privacy of Canadians.

I am pleased to note that CSEC recently revised its operational policy on this subject to include additional guidance respecting the protection of the privacy of Canadians. Managers routinely and closely monitor compliance with applicable policies and procedures. The people with whom my staff spoke were forthcoming and demonstrated a professional approach.

Therefore, in view of these findings, I retracted my previous recommendation and informed CSEC that I have no expectation of corrective action in regard to these activities.

Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate

Background

The specific objective of this review was to acquire knowledge of CSEC's activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate. I examined CSEC's compliance with the expectations set out in the ministerial directive and associated policies and procedures. These expectations are administrative in nature and relate primarily to security and risk management.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were consistent with the foreign intelligence priorities of the Government of Canada, and were carried out in accordance with the law and with CSEC operational policies and procedures. CSEC had also taken specific measures to protect the privacy of Canadians. I also found that, for the most part, CSEC conducted the activities in accordance with expectations set out in the ministerial directive and with associated policies and procedures.

Recommendations

I recommended, however, that CSEC reconcile certain discrepancies between ministerial expectations and its own practices. I also recommended that CSEC review, update and finalize certain key documents respecting these activities, and that it clarify certain terms used in the documents. I believe this will strengthen CSEC's ability to meet the ministerial expectations and therefore enhance accountability. I am awaiting CSEC's response to these recommendations.

REVIEWS UNDERWAY AND PLANNED

I am pleased to note that of the reviews I indicated were underway in my report last year, all were completed, though the results of the comprehensive study of CSEC's information technology security activities will be submitted to the Minister early in the next reporting year. In addition, the examination of certain common practices of CSEC related to its mandated activities, has been split into several reviews to permit more detailed examination. The first of these, on disclosure of information about Canadians, was completed and submitted to the Minister in this reporting year.

Other reviews that are underway or planned for the next reporting year include: CSEC's foreign intelligence sharing with international partners; activities conducted under foreign intelligence ministerial authorizations; activities conducted under IT security ministerial authorizations; the process by which CSEC determines that targets of foreign intelligence interest are indeed foreign entities located outside Canada, as required by law; and CSEC's assistance (under part (c) of its mandate) to the Canadian Security Intelligence Service under section 16 of the *CSIS Act*.

Some of these reviews may carry over into the 2010–2011 reporting year. There may also be a certain area or activity that, as a result of various factors, I determine to be a priority, resulting in it being reviewed sooner rather than later. This situation is part of the ongoing process of assessing where risks to lawful compliance or privacy are greatest.

COMPLAINTS ABOUT CSEC'S ACTIVITIES

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

This year my office received one complaint warranting investigation. While I cannot speak to the substance of the complaint, I am able to report that the investigation found no unlawful activity on the part of CSEC.

DUTIES UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy and seek to defend the release of classified information about CSEC on the grounds that it is in the public interest. No such matters were reported to my office in the 2008–2009 reporting period.

THE COMMISSIONER'S OFFICE

During 2008–2009, I met periodically with the Chief of CSEC to discuss issues of mutual interest. These collaborative meetings reflect a productive working relationship which, I believe, contributes to the overall efficiency and effectiveness of the review process.

I had occasion during the reporting period to meet the Prime Minister's newly appointed National Security Advisor, whose duties include accountability for CSEC policy and operational direction. I also met with several federal court judges and other senior government officials.

My office's new status

As I observed in my last report, a decision was taken in the autumn of 2007 that would sever my office's long-standing relationship with the Privy Council Office for the provision of administrative and other support activities and transfer these responsibilities to the Department of National Defence.

Subsequently, it was determined that positioning my office within the same portfolio as CSEC did not have the appearance of propriety and autonomy that ought to exist between an agency and its review body. As a result, and effective April 1, 2009, my office was granted its own parliamentary appropriation. While the reporting relationship to the Minister of National Defence remains intact, as set out in the *NDA*, my office is separate from, and is not part of, that department.

These changes have, by necessity, given rise to additional expenditures for support services, with a corresponding increase in the budget which appears at Annex C. Still, I view this new status as another indication of the maturation of my office and further reinforcement of its independence.

Canadian Association of Security and Intelligence Studies 2008 Conference

My office's participation in the annual CASIS conference in October 2008 afforded an excellent opportunity to exchange perspectives on security and intelligence issues, including review, with leading experts, scholars, policy makers and practitioners from across the country. My office was also pleased to mentor two Canadian graduate students in security and intelligence studies in conference events and discussions.

International Intelligence Review Agencies Conference

I attended the International Intelligence Review Agencies Conference in Auckland, New Zealand in October 2008 to make a presentation to a conference panel on developing trust between a review body and the agency being reviewed, while retaining independence. In my remarks, I emphasized that building and maintaining CSEC's trust in my office, while safeguarding my office's independence, requires constant management and accommodation of interests at all levels.

I also emphasized that CSEC's trust in the Commissioner's office depends significantly on the demonstrable quality of its review work. As a result, my office has placed considerable emphasis on developing, documenting and implementing sound methodologies, based on accepted standards of review and informed by years of practical experience. I added that my office has developed operational policies and procedures that, among other things, provide guidance to staff in carrying out reviews, ensure a large measure of transparency and consistency in my office's work when seen from CSEC's perspective, and provide a basis for assessing and improving CSEC's own performance in implementing its mandate.

British Intelligence and Security Committee of Parliamentarians

I met with the British Intelligence and Security Committee of Parliamentarians during the Committee's visit to Ottawa in March 2009. Committee members and my staff and I participated in a useful exchange of information and opinions on security and intelligence review issues of mutual interest and concern.

IN CLOSING

As I conclude my first term as CSE Commissioner and prepare to embark upon a second term in August 2009 for one year, I do so with satisfaction in current achievements and a sense of optimism going forward. Over the past three years I am pleased to have established a productive working relationship with the Chief of CSEC. I look forward to building on this relationship as I continue to review CSEC's activities in accordance with my mandate. For me, comprehensive review of these activities remains both a challenging and rewarding task, and one which I am greatly honoured to carry out on behalf of Canadians.

ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

National Defence Act – **Part V.1**

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

(2) The duties of the Commissioner are

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

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

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

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

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

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

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

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

[...]

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

Security of Information Act

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

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

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

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

ANNEX B: CLASSIFIED REPORTS, 1996–2009

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – June 11, 2008 (TOP SECRET/COMINT/CEO)

47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – June 11, 2008 (TOP SECRET/ COMINT/CEO)

48. Review of disclosure of information about Canadians to Government of Canada clients – November 19, 2008 (TOP SECRET/COMINT/CEO)

49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – January 13, 2009 (TOP SECRET/ COMINT/CEO)

50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – February 26, 2009 (TOP SECRET/COMINT/CEO)

51. Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – March 12, 2009 (TOP SECRET/ COMINT Codeword/CEO)

52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – March 12, 2009 (TOP SECRET/ COMINT/CEO)

ANNEX C: STATEMENT OF EXPENDITURES 2008–2009

Standard Object Summary

Salaries and Wages	$782,686
Transportation and Telecommunications	43,337
Information	16,303
Professional and Special Services	258,294
Rentals	157,371
Purchased Repair and Maintenance	1,913
Materials and Supplies	7,822
Acquisition of Machinery and Equipment	23,595
Other Expenditures	0
Total	**$1,291,321**

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

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

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

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

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

In autumn 2007, a decision was taken that would sever OCSEC's long-standing arrangements with the Privy Council Office for administrative and other support activities. Effective April 1, 2009, OCSEC was granted its own parliamentary appropriation. While the Commissioner continues to provide the Minister of National Defence with his reports, OCSEC is separate from, and not part of, the department.

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

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

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

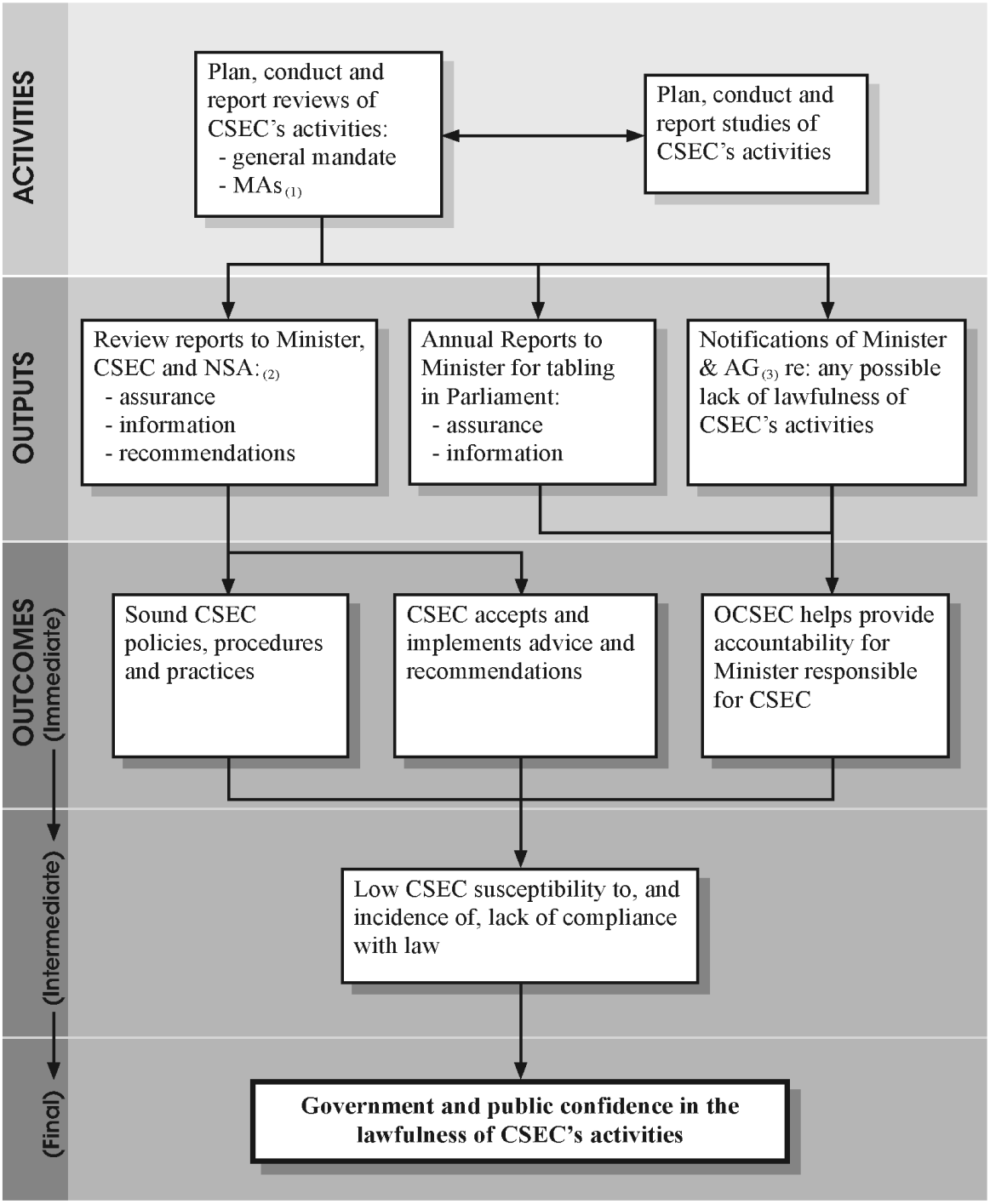
CSEC's information technology security products and services enable its clients (government departments and agencies) to effectively secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications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

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

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

ANNEX F: OCSEC REVIEW PROGRAM — LOGIC MODEL

The following logic model provides a graphic description of how the review program functions.



(1) Ministerial authorizations (2) National Security Advisor to the Prime Minister (3) Attorney General of Canada