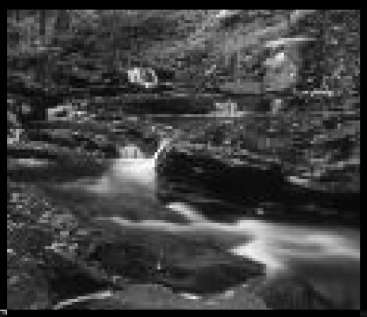
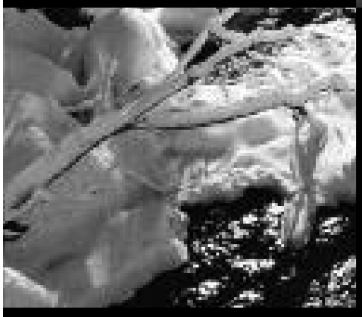
COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

Annual Report





2009-2010

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 978-1-100-51826-8
Cat. No. D95-2010

Cover photos: Malak

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

June 2010

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 the annual report for the period of April 1, 2009, to March 31, 2010, on the activities and findings of my two predecessors, the Honourable Peter deC. Cory and the late Honourable Charles D. Gonthier, for your submission to Parliament.

Yours sincerely,

Robert Décary

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

This report is dedicated to the memory of

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

1928–2009

TABLE OF CONTENTS

INTRODUCTION

By the Honourable Peter deC. Cory, C.C., C.D.

I was pleased to accept the appointment of Communications Security Establishment Commissioner, effective December 14, 2009. The office had been without a Commissioner since the untimely death last July of my predecessor, and former colleague on the Supreme Court of Canada, the late Honourable Charles D. Gonthier.

Upon my arrival at the office last December, what impressed me immediately was the professionalism and dedication of the staff. Despite the fact that there had been no Commissioner in place between the passing of Mr. Gonthier and my appointment, the work of the office continued, with staff carrying on review of the Communications Security Establishment Canada (CSEC) activities. The only work that did not proceed was the forwarding of review reports to the Minister, a task which is the sole responsibility of the Commissioner.

I was also struck by the professionalism and dedication of CSEC personnel. One area of activity in 2009–2010 which stands out is CSEC's important, and at times life-saving, work in support of Canadian Forces in Afghanistan, as a priority established by the Government of Canada.

During the time between my appointment and the end of this reporting period, I was thoroughly apprised of CSEC's activities through a comprehensive briefing from the Chief of CSEC as well as briefings and discussions with my staff pertaining to the review of CSEC's activities to assess compliance with relevant legislation.

I know from past reports that those CSEC activities that were reviewed complied with the law. The opportunity I had for discussions with the Chief and with my staff demonstrated to me that there is consistency in the way in which CSEC fulfills its mandate. Those activities about which I submitted reports to the Minister of National Defence also complied with the law. This is a reflection of a culture of compliance that exists within CSEC.

This is not to say that there are not certain issues about which there are or may be disagreements. These disagreements can be worked through more effectively, however, when there is a fundamental understanding of the law by CSEC staff and a practical appreciation of how it applies to their work.

As a final word, let me state that subsequent to my appointment in late 2009, a number of factors intervened to lead me to limit my time as Commissioner. These are circumstances that I sincerely regret, since the process of selection must take time. However, life sometimes sets before us circumstances that do not always work out the way we would have thought or preferred. I am grateful for the opportunity I had to work with the able and conscientious staff at the Commissioner's office. I am assured as well that my successor has a sound base on which to carry forward the important, independent role of the Commissioner in ensuring that CSEC complies with the law and protects the privacy of Canadians while fulfilling its legislated mandate.

REVIEW ENVIRONMENT

Proposed amendments to the *National Defence Act*

The *National Defence Act* (*NDA*) prohibits CSEC from directing its foreign intelligence and information technology security activities at a Canadian or any person in Canada. It also requires CSEC to take measures to protect the privacy of Canadians in the use and retention of intercepted information.

However, due to the manner in which communications are transmitted, CSEC may, while conducting its mandated foreign intelligence collection or information technology security activities, unintentionally intercept communications of Canadians or persons in Canada, which constitute "private communications" as per section 183 of the *Criminal Code*.

Recognizing this possibility, the *NDA* allows the Minister of National Defence to authorize CSEC to intercept private communications. Prior to granting this authorization, however, the Minister must be satisfied that certain conditions set out in the *NDA* are met. There are four conditions for foreign intelligence collection ministerial authorizations (subsection 273.65(2)) and five conditions for information technology security ministerial authorizations (subsection 273.65(4)).

CSEC's activities conducted under a ministerial authorization must be undertaken in accordance with:

- relevant legislation, namely the *NDA*, *Canadian Charter of Rights and Freedoms*, *Privacy Act*, *Criminal Code*, as well as Justice Canada advice;
- requirements set out by the Minister of National Defence in the authorization or in a ministerial directive, for example, for accountability, to record and report to the Minister certain information after the expiration of the ministerial authorization; and
- CSEC policies and procedures.

Part of the Commissioner's legislated mandate is to examine CSEC's activities under ministerial authorizations to ensure they were authorized and conducted in compliance with the law. Reviews by past Commissioners have never identified an instance in which CSEC targeted the communications of a Canadian or a person in Canada.

Private communications and information about Canadians

Reviews of CSEC activities under ministerial authorizations have consistently demonstrated that the proportion of private communications of Canadians that CSEC unintentionally intercepts is very small.

CSEC's classified foreign intelligence reports may contain information about Canadian citizens, permanent residents or Canadian corporations (as defined in section 273.61 of the *NDA*), if such information is deemed essential to the understanding of the reports. However, this information must be suppressed, that is replaced by a generic reference such as "a Canadian person".

CSEC's foreign intelligence ministerial authorizations are broadly written and apply to methods of collecting foreign intelligence rather than to individuals. However, Commissioners have been of the view that it is not clear that the *NDA* supports such an approach. Commissioners have stated that amendments to the *NDA* are necessary to clarify ambiguities relating to foreign intelligence ministerial authorizations. Former Commissioner Gonthier also emphasized last year that "the length of time that has passed without producing amended legislation puts at risk the integrity of the review process."

Commissioner Gonthier was informed by the Minister of National Defence that clarification of ambiguities and other amendments to the *NDA* are a legislative priority. Pending amendments, Commissioners have continued to use the interim solution of applying a qualified opinion, that is, reviewing CSEC foreign intelligence collection activities under ministerial authorization on the basis of the *NDA* as it is interpreted by Justice Canada. However, past Commissioners have noted they disagree in certain important respects with that interpretation, which highlights the need for amendments to the *NDA*.

CSEC assistance to CSIS under part (*c*) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*

National security matters are increasingly the subject of court and other public proceedings. In his October 5, 2009 decision in the matter of an application for a warrant pursuant to sections 12 and 21 of the *CSIS Act*, the Honourable Mr. Justice Mosley of the Federal Court authorized CSIS, with the technical assistance of CSEC, to intercept from *within* Canada communications pertaining to threat-related activities in which it was believed two persons would engage while travelling *outside* of Canada. Justice Mosley distinguished the application from a similar one heard and denied in October 2007 by the Honourable Mr. Justice Blanchard, also of the Federal Court.

In the reasons for his decision, Justice Mosley emphasized that "[i]n authorizing CSIS, with the technical assistance of CSE[C], to collect information ... intercepted in Canada, I am not authorizing CSE[C] to overstep its legislative mandate under the *National Defence Act*. [...] CSE[C] will not be directing its activities at Canadian citizens to acquire information for its purposes but assisting CSIS".

CSEC's mandate to assist federal law enforcement and security agencies

Paragraph 273.64(1)(*c*) of the *National Defence Act* permits CSEC to provide technical and operational assistance to federal law enforcement and security agencies. CSEC is subject to any limitations imposed by law on the agency to which CSEC is providing assistance — for example, conditions imposed by a judge in a warrant.

In 2010–2011, the Commissioner's office will conduct a review of CSEC's assistance to CSIS involving the interception in Canada of communications of Canadians located outside of Canada and subject to a warrant under sections 12 and 21 of the *CSIS Act*, such as those authorized by Justice Mosley's decision.

Findings and recommendations arising from the Iacobucci and O'Connor inquiries

In June 2009, the House of Commons Standing Committee on Public Safety and National Security issued a report of its review of the findings and recommendations arising from the *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Iacobucci inquiry) and the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (O'Connor inquiry). The Standing Committee urged the government to implement all of the recommendations from these inquiries.

In October 2009, the government responded to the Standing Committee's report with a commitment "…to modernize and strengthen the national security review framework". Specifically, the response stated: "[t]he Government's objective is to strengthen national security structures that are already in place..." and "[m]uch work has also been done to advance policy analysis on Canada's national security review framework " including "...providing a mechanism to facilitate inter-agency review of national security activities".

Regarding the latter point, former Commissioner Gonthier stated that there are no obstacles, legal or otherwise, to cooperation among national security review agencies. Much can be done by way of joint or parallel reviews, research or other collaborative work.

Respecting the role of parliamentarians, and in the context of the development of an enhanced national security framework, the government's response indicated that due consideration will be given to the Standing Committee's fifth recommendation: that Bill C-81, introduced in the 38th Parliament, *An Act to Establish the National Security Committee of Parliamentarians*, or a variation of it, be introduced in Parliament at the earliest opportunity. Past Commissioners have raised questions about the composition of such a committee and its access to classified national security information.

The O'Connor and Iacobucci inquiries also identified a number of issues respecting Canadian security and intelligence agencies' sharing of information with foreign agencies. The government's response indicated that "[t]he cumulative result of successive commissions of inquiry, reports and lessons learned has been the refinement of policies and practices surrounding the exchange of information between foreign partners and Canada's national security and intelligence and law enforcement communities". Information sharing is an essential component of CSEC's foreign intelligence program. The Commissioner's office is currently completing a review of this activity.

In its response to the recommendations of the O'Connor and Iacobucci inquiries, the government indicated that it will continue to consider the advice of stakeholders. The Commissioner's office remains willing to discuss such matters.

YEAR IN REVIEW

The last reporting year was a unique one for the Commissioner's office. As noted in the introduction, there was no Commissioner for a period of five months following the passing of Commissioner Gonthier. Nevertheless, the work of the office continued. Reviews and classified reports were completed, and others that had been approved by former Commissioner Gonthier were continued, or begun, as planned.

The primary objective of reviews is to assess whether CSEC's activities comply with the law, including the extent to which adequate measures are in place to protect the privacy of Canadians. Three classified reports were submitted to the Minister during the past year. One was a comprehensive study relating to CSEC information technology security activities and two were reviews relating to foreign intelligence activities.

The two reviews found that CSEC complied with the law and ministerial requirements and protected the privacy of Canadians. CSEC accepted the recommendations made in the reviews and is taking action to address them. CSEC is also addressing findings in order to improve its policies or practices.

Implementing recommendations

Since 1997, Commissioners have submitted to the Minister of National Defence 55 classified review reports and studies. In total, these reports have contained 129 recommendations. CSEC has accepted and implemented or is working to address 94 percent (121) of these recommendations. The few recommendations that were not accepted or implemented may have been in areas surpassed by events or circumstances. In an instance where CSEC rejects a recommendation, the Commissioner reviews the reasons provided by CSEC, then assesses whether to accept these reasons or to pursue the issue, possibly by examining it in even greater depth.

Regular review of disclosures of information about Canadians

The Commissioner's 2008–2009 annual report noted that the Commissioner's office would conduct regular reviews of CSEC's disclosure of information about Canadians to Government of Canada clients. For a period of six months last year, the Commissioner's office conducted monthly reviews of all disclosures and found them to comply with the law, and with CSEC policies and procedures. Given these positive results as well as the positive result of a more comprehensive review of disclosures reported in the 2008–2009 annual report, it was determined that monthly reviews were not necessary. However, given also that this activity lies at the heart of the Commissioner's mandate, as noted by former Commissioner Gonthier last year, an annual review will still be conducted.

Timeliness of CSEC's responses to information requests

CSEC's operations in 2009–2010 were affected by a number of extraordinary factors and external pressures such as responding to international special events. While Commissioners respect that operations must be CSEC's priority, the length of time CSEC took to respond to requests for information from the Commissioner's office this past year was at times too long. CSEC is examining ways to better support the Commissioner's review requirements.

Enabling a higher level of assurance

During the past year, CSEC provided a number of detailed briefings to staff of the Commissioner's office. Some of the briefings were general in nature with the objective of keeping the office informed of operational, policy and organizational issues. Other briefings provided information on specific CSEC activities prior to establishing terms of reference for a review or during a review underway.

Several briefings described CSEC's tools, systems and databases, including those used to ensure that CSEC complies with statutory requirements for targeting foreign entities outside of Canada.

The briefings, along with direct access to CSEC systems and front-line employees, enhanced the depth of review by the Commissioner's office in 2009–2010. All of this enables a Commissioner to provide a higher level of assurance to the Minister of National Defence that CSEC is complying with the law and protecting the privacy of Canadians.

Strengthening accountability and compliance

Commissioners look to reinforce good practices that maintain or strengthen CSEC's compliance with the law and the protection of the privacy of Canadians. CSEC has continued to make significant improvements to its information management practices and has continued to expand the use of its corporate records management system, issues that were subjects of past recommendations by Commissioners. These enhancements are critical to CSEC accountability and compliance.

CSEC is also to be commended for a new initiative to increase employee awareness and knowledge of the authorities, policies and procedures governing its activities. This initiative makes policies which are specifically relevant to an employee's position readily available on the employee's computer. This initiative is expected to strengthen CSEC's compliance framework and the protection of the privacy of Canadians.

REVIEW METHODOLOGY

In the conduct of a review, the Commissioner's staff examine relevant written and electronic records, files, correspondence and other documentation, including policies, procedures and legal advice. CSEC provides briefings and demonstrations of its activities as well as detailed answers in response to written questions from the Commissioner's office.

Commissioner's staff may test the information obtained against the contents of CSEC systems and databases. In addition, Commissioner's staff interview CSEC managers and other personnel involved in activities under review and observe firsthand CSEC operators and analysts to learn exactly how they are conducting their work.

The Commissioner's office may also refer to the work of CSEC's internal auditors and evaluators. In some cases, this may lead to identifying an activity for review.

Review criteria

Reviews conducted by the Commissioner's office include an assessment of CSEC's activities against a standard set of criteria respecting legal requirements, ministerial requirements, and CSEC policies and procedures. Other criteria may be added to each review, as appropriate.

Legal requirements: The Commissioner expects CSEC to conduct an activity in accordance with the *NDA*, the *Canadian Charter of Rights and Freedoms*, *Privacy Act*, *Criminal Code*, any other relevant legislation and Justice Canada advice.

Ministerial requirements: The Commissioner expects CSEC to conduct an activity in a manner that is in accordance with ministerial direction, namely any requirements and limitations set out in a ministerial authorization or directive.

Policies and Procedures: The Commissioner expects CSEC to have appropriate policies and procedures in place to guide an activity and to provide sufficient direction respecting legal and ministerial requirements and the protection of the privacy of Canadians. The Commissioner expects CSEC employees to be aware of and comply with policies and procedures. The Commissioner also expects CSEC to utilize an effective management control framework to ensure that the integrity and lawful compliance of an activity is maintained on a routine basis. This includes appropriate accounting for decisions taken and for information relating to compliance and the protection of the privacy of Canadians.

A new approach to reviewing foreign intelligence activities

CSEC's foreign intelligence collection activities conducted under ministerial authorization involve a number of distinct methods of acquiring information from the global information infrastructure. Nevertheless, there are a number of common processes and associated tools, as well as common systems and databases, which support these collection methods and which CSEC uses to deal with the information obtained. For example, common to all of the collection methods are the processes by which CSEC: selects foreign entities located outside Canada that are of foreign intelligence interest; shares reports and information with its clients and international partners; and retains or disposes of intercepted communications.

Rather than examine thoroughly individual ministerial authorizations, it was assessed as more effective to examine thoroughly each process common to CSEC's foreign intelligence collection activities under ministerial authorization. This new approach, which cuts across the collection methods, is referred to as *horizontal review*.

Why horizontal review?

The horizontal review approach, born of years of accumulated review experience on the part of the Commissioner's office, is designed to provide the Commissioner's staff with an even more comprehensive understanding of how CSEC conducts its activities. Ultimately, its objective is to increase the degree of assurance the Commissioner can provide to the Minister of National Defence that CSEC is complying with the law and protecting the privacy of Canadians.

In addition to the horizontal review approach, the Commissioner's office now reviews all foreign intelligence ministerial authorizations together, on an annual basis. This review will identify any significant changes to the activities covered by the ministerial authorizations or in the authorizations themselves. Any significant changes will be assessed in terms of their impact on risks of non-compliance and risks to the privacy of Canadians. If appropriate, a detailed review will be conducted. This annual review of foreign intelligence ministerial authorizations will also examine used and retained intercepted private communications to ensure they are communications essential to international affairs, defence or the security of Canada, as required by paragraph 273.65(2)(*d*) of the *NDA*.

The Commissioner provides classified reports containing findings and recommendations to the Minister of National Defence, with copies going to the Chief of CSEC, to the National Security Advisor to the Prime Minister, who is accountable for CSEC operations and policy, and to the Deputy Minister of National Defence, who is accountable for administrative matters pertaining to CSEC. Prior to finalizing a report, the Commissioner's office seeks CSEC's comments respecting the report's factual accuracy.

Study of CSEC information technology security activities not conducted under ministerial authorization

Background

This study was initiated and conducted under the authority of former Commissioner Gonthier, as articulated in paragraph 273.63(2)(*a*) of the *NDA*. It examined CSEC information technology (IT) security activities not conducted under ministerial authorization. A previous review of IT security activities was conducted in 2000. However, because of significant changes and developments in this area since that time, a comprehensive study was undertaken of all IT security activities not conducted under ministerial authorization. Other IT security activities that CSEC conducts under ministerial authorizations are reviewed annually.

CSEC's principal authority for IT security is derived from paragraph 273.64 (1)(*b*) of the *NDA*: "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". CSEC's IT security activities focus on preventing and responding to sophisticated IT threats and cyber attacks that attempt to covertly access sensitive government computer systems. Among its IT security activities, CSEC promotes sound security practices to help government departments reduce IT vulnerabilities and manage IT security risks. This may involve

the provision of monitoring and countermeasures to prevent, detect and respond to IT threats and cyber attacks.

The objectives of the study were to acquire knowledge of CSEC IT security activities and to conduct a risk assessment to determine which of these activities, if any, may raise issues about compliance with the law, ministerial requirements, CSEC policy and procedures, or the protection of the privacy of Canadians — and should therefore be subject to follow-up review. Particular attention was paid to activities that may involve private communications or information about Canadians.

Some of the areas included in the scope of this study were: the government's cryptographic program; relationships with industry; research, analysis and reporting respecting cyber vulnerabilities and sophisticated IT threats and attacks; assistance in identifying and responding to vulnerabilities and incidents affecting information infrastructures of importance to the government; and associated relationships with key Canadian government and international partners.

Findings and conclusions

The study found that CSEC IT security activities not conducted under ministerial authorization generally present a low risk of possible non-compliance with Part V.1 of the *NDA* and a low risk to the privacy of Canadians. One quarter of the areas included in the study were identified for follow-up review and have been incorporated into the Commissioner's three-year work plan.

In only a few cases, CSEC's IT security activities not conducted under ministerial authorization involve access to a small amount of information about Canadians. Most of this information relates to the identity of a Canadian company, or consists of information voluntarily provided by CSEC's government clients as part of cyber protection activities or ongoing Crown business.

There are, however, other IT security activities not conducted under ministerial authorization that may present risks to the privacy of Canadians. These activities are conducted under the *Criminal Code* and the *Financial Administration Act* authorities of other government entities and may involve CSEC access to private communications and information about Canadians. In respect of these activities, the study found that CSEC takes measures to protect the privacy of Canadians. For example, private communications and information about Canadians are disclosed only to those officials involved in protecting computer systems. Nevertheless, the potential risks to privacy presented by these activities cannot be discounted. Therefore, the Commissioner's office will conduct in-depth reviews of these activities to verify CSEC's compliance, and to assess the extent to which it protects the privacy of Canadians in carrying out these activities.

Intrusion detection system monitoring

Paragraph 184(2)(e) of the *Criminal Code* permits in part the interception of a private communication by a person in control of a computer system in order to protect the computer system from any act that would be an offence under subsections 342.1(1) ("unauthorized use of computer") or 430(1.1) ("mischief in relation to data") of the *Criminal Code*. This provision permits the use of an intrusion detection system to protect against a cyber attack and allows for the use or retention of a private communication where it is essential to identify, isolate or prevent harm to the computer system.

Section 161 of the *Financial Administration Act* provides authority for a government entity to take reasonable measures to protect a computer system, including the interception of a private communication in circumstances specified in paragraph 184(2)(*e*) of the *Criminal Code*.

The study also included the examination of a principal CSEC IT security software tool and information repository. Former Commissioner Gonthier concluded that the CSEC IT security software tool has adequate functionality to restrict access to information held in the system, to meet security and confidentiality requirements, and to protect the privacy of Canadians. To confirm this, the Commissioner's office examined CSEC's use of the system in the context of a review of certain IT security activities conducted under ministerial authorization. The results of this review will be included in the 2010–2011 annual report.

Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan

Background

This review was initiated and conducted under the authority of former Commissioner Gonthier, as articulated in subsection 273.65(8) of the *NDA*. The report was reviewed and submitted to the Minister of National Defence by former Commissioner Cory. The review examined activities conducted under two ministerial authorizations in effect in 2006–2007 and 2007–2008 and in support of Canadian Forces military operations and other government efforts relating to Afghanistan. CSEC obtained the ministerial authorizations pursuant to subsections 273.65(1) and (2) of the *NDA* because, in carrying out the activities, it was possible that CSEC might intercept a communication that either originated or terminated in Canada, constituting a private communication, as defined in the *Criminal Code*.

Pending amendments to clarify the *NDA*, this review was based on the legal interpretation of the foreign intelligence ministerial authorization provisions in the *NDA* provided to CSEC by Justice Canada.

As this was the first review of these activities, the objectives were to acquire detailed knowledge of these activities, to assess whether these activities were authorized and complied with the law, and to assess the extent to which CSEC protected the privacy of Canadians in carrying out these activities.

Findings

It is clear that CSEC's activities under ministerial authorization and relating to Afghanistan provide important access to valuable foreign intelligence that supports both military and broader government intelligence priorities.

The activities were found to have involved access to a minimal number of private communications and information about Canadians. They were therefore assessed as presenting a low risk to the privacy of Canadians.

Based on information reviewed and interviews conducted, CSEC activities from 2006–2008 under ministerial authorization and relating to Afghanistan were found to have been appropriately authorized and conducted in accordance with the law and Justice Canada advice. These activities were also found to have been conducted in accordance with requirements in the ministerial authorizations and with ministerial direction. CSEC recorded and reported information to the Minister in accordance with the requirements of the authorizations.

Recommendations

No information or documentation was found to indicate that CSEC employees contravened operational policies and procedures applicable to these foreign intelligence collection activities. However, former Commissioner Gonthier recommended that CSEC amend its policy for these activities to clarify certain obligations. It is a positive development that CSEC acted on this recommendation and, as a result, has strengthened its ability to meet legal and ministerial requirements. The Commissioner's office will also monitor CSEC efforts to address gaps related to CSEC's dealings with the Canadian Forces, as identified by CSEC internal evaluators.

In addition, this review noted two CSEC enhancements related to foreign intelligence collection reporting that should be recognized. First, CSEC took action to centrally manage a certain type of reporting to enhance accountability for such reporting. Second, CSEC addressed a recommendation by former Commissioner Gonthier that additional information respecting foreign intelligence collection activities be recorded and reported to the Minister of National Defence to strengthen accountability.

Regular review of CSEC disclosure of information about Canadians to Government of Canada clients

Background

This review was initiated and conducted under the authority of former Commissioner Gonthier, as articulated in paragraph 273.63(2)(*a*) of the *NDA*. The report was reviewed and submitted to the Minister of National Defence by former Commissioner Cory.

When receiving a request for disclosure of the details of suppressed information about a Canadian in a report, CSEC requires its clients to explain their authority to obtain and use this information, and to provide an operational justification of their need for such information. Only after these conditions have been met will CSEC release the suppressed information.

The Commissioner's 2008–2009 annual report contained a summary of a comprehensive review of disclosure of information about Canadians to Government of Canada clients. The review found that CSEC activities complied with law, and with CSEC policies and procedures. Subsequently, CSEC suggested that reviews of this activity could be conducted at regular intervals. Recognizing that this CSEC activity is important to privacy protection, former Commissioner Gonthier agreed with CSEC's suggestion and monthly reviews of all CSEC disclosures to Government of Canada clients were conducted from January to June 2009.

Findings

The monthly reviews found that CSEC's disclosure of information about Canadians in foreign intelligence reports to Government of Canada clients complied with the law and with CSEC operational policies and procedures. Given these positive results, it was determined that monthly reviews were not necessary and not the most effective use of resources for either party. However, given the privacy implications of this activity, commencing in 2010–2011, the Commissioner will conduct an annual review of a random sample of disclosures to verify that CSEC continues to comply with the law and maintains measures that protect the privacy of Canadians.

Recommendations

Notwithstanding the positive findings, former Commissioner Gonthier made two recommendations respecting reporting to the Minister of National Defence on the volume of information about Canadians released to CSEC's clients. The recommendations relate to providing tools to support the tracking of such information and to improving the consistency and accuracy of the reporting. CSEC has accepted and is implementing the recommendations.

WORK PLAN — REVIEWS UNDERWAY AND PLANNED

CSEC activities selected for review are prioritized using a set of detailed criteria. For example, the ongoing review of CSEC's foreign intelligence sharing with international partners was identified as a high-priority review topic. This is because: there have been changes to the authorities and technologies relating to these activities; the amount of foreign intelligence CSEC provides to and receives from its international partners is significant; these activities could directly and adversely affect a Canadian; specific and important controls are placed on the activities to ensure compliance with legal, ministerial and policy requirements, and these controls should be examined; and, finally, in past reviews relating to these activities, Commissioners have made findings and recommendations which require follow-up.

Decisions respecting the selection and prioritization of subjects for review are documented in the Commissioner's three-year work plan, which is updated regularly as part of an ongoing process of assessing risk.

Current reviews

The results of several reviews currently underway are expected to be reported on to the Minister of National Defence in the coming year and included in the Commissioner's 2010–2011 public annual report.

The subjects of these reviews include: CSEC's foreign intelligence sharing with international partners; activities conducted under IT security ministerial authorizations; the process by which CSEC determines that targets of foreign intelligence interest are foreign entities located outside of Canada, as required by the *NDA*; a method used by CSEC to identify new entities believed to be of foreign intelligence interest; and an annual review of foreign intelligence ministerial authorizations, including a sample of associated private communications.

Upcoming reviews

Other reviews planned for 2010–2011 include: assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*; an annual review of CSEC disclosures of information about Canadians to government clients and international partners; CSEC's retention and disposal of information, and, in particular, of private communications and information about Canadians; and CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 16 and 21 of the *CSIS Act*. Some reviews may carry over into the 2011–2012 fiscal year.

COMPLAINTS ABOUT CSEC'S ACTIVITIES

The Commissioner's mandate includes undertaking any investigation deemed to be necessary in response to a complaint in order to determine whether CSEC has engaged, or is engaging, in unlawful activity.

In 2009–2010, correspondence was received concerning CSEC activities but none warranted investigation.

DUTIES UNDER THE SECURITY OF *INFORMATION ACT*

The Commissioner has a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information on the grounds that it is in the public interest. No such matters were reported to the Commissioner in the 2009–2010 reporting period.

THE COMMISSIONER'S OFFICE

Last year, the Commissioner's office was granted its own appropriation from Parliament, strengthening the Commissioner's independence. As a result of the independence, there were additional administrative requirements. The Commissioner's office then requested and received additional funding from the Treasury Board to meet these administrative requirements as well as to provide additional operational support for fulfilling the Commissioner's mandate.

Comparative study of CSEC and international partners

During the summer of 2009 the Commissioner's office was fortunate to welcome a master's student from Carleton University who completed a comparative study of publicly available information respecting CSEC and some of its international partners, their authorities, activities and oversight and review mechanisms. The study informs work such as the ongoing classified review of CSEC's foreign intelligence sharing with international partners.

Canadian Association of Security and Intelligence Studies (CASIS) conference

In October 2009 staff of the Commissioner's office participated in the annual CASIS conference, held in Ottawa. The theme of the conference was *Terrorism, Cyberspies and a New 'Cold' War: Emerging Challenges for Security and Intelligence*. The conference attracted many leading experts, scholars, policy makers, practitioners and academics from within Canada and internationally. Lectures and panels provided new perspectives on the ever broadening challenges facing the security and intelligence community.

International Intelligence Review Agencies Conference (IIRAC)

In March 2010, the Executive Director of the Commissioner's office attended the IIRAC in Sydney, Australia, leading a discussion on effective review, with a description of the Commissioner's office's approach in areas such as staff recruitment and development, review targeting and plans, and performance measurement and indicators.

The objectives of the bi-annual IIRAC are to share ideas and best practices and build capacity in the review and oversight functions of participating organizations. Participants are from countries that share basic principles of rule of law and democratic control over security and intelligence agencies. Participating organizations represent many different models of review and oversight, adding to the richness of exchanges of information and experience.

IN CLOSING

(by the Honourable Peter deC. Cory)

I would like to take this opportunity to say a word about Joanne Weeks, who stepped down recently as Executive Director of the Commissioner's office. She had directed the day-to-day business of the office since the appointment of the first Commissioner, the Honourable Claude Bisson, in 1996. Joanne oversaw an important evolution of the office when a legislative framework was provided for both the Commissioner's office and CSEC in the omnibus *Anti-terrorism Act,* following the terrorist attacks of September 11, 2001. For the relatively short time that I worked with Joanne, I came to appreciate her clear devotion to public service and saw her as a generous, warm-hearted individual. Joanne knew the important role that review plays and strove to ensure that she had the most capable staff to carry out the work. As her retirement approaches, I would like to express my sincere appreciation and thanks to Joanne for her dedication, not just to the Office of the CSE Commissioner but, more importantly, to Canada. Her work provides an outstanding example to all in the public service.

A TRIBUTE TO THE HONOURABLE CHARLES DOHERTY GONTHIER, C.C., Q.C.

(by the Honourable Peter deC. Cory)

The Honourable Charles Doherty Gonthier passed away on July 17, 2009, while still Commissioner of the Communications Security Establishment Canada. Active to the end in service to his country, and applying his intellect with customary vigour, he contributed significantly in many areas of the law. His interest and work in later years dealt with sustainable development, demonstrating a great social conscience and sympathy for vulnerable members of society.

Charles and I were appointed to the Supreme Court of Canada on the same day in 1989. A greatly respected colleague and a close friend, he will be sorely missed. Fortunately, he leaves a rich legacy which will inspire all of us for the rest of our days.

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 TO THE MINISTER

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 CSEC'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)

53. Study of CSEC information technology security activities not conducted under ministerial authorization – June 11, 2009 (TOP SECRET/COMINT/CEO)

54. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan – January 18, 2010 (TOP SECRET/COMINT/CEO)

55. Regular review of CSEC disclosure of information about Canadians to Government of Canada clients – February 16, 2010 (TOP SECRET/COMINT/CEO)

Standard Object Summary

Salaries and Wages	$930,329
Transportation and Telecommunications	35,893
Information	19,319
Professional and Special Services	378,465
Rentals	157,068
Purchased Repairs and Maintenance	457
Materials and Supplies	11,042
Total	**$1,532,573**

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

The Office of the Communications Security Establishment Commissioner 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, a position he held until his death in July 2009. The Honourable Peter deC. Cory, C.C., C.D., a former Justice of the Supreme Court of Canada, served as Commissioner from December 14, 2009 to March 31, 2010.

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 the Commissioner's office and CSEC. It gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization. The legislation also continued the Commissioner's powers under the *Inquiries Act*.

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.

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

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

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency, providing the Government of Canada with two key services, foreign signals intelligence and information technology security. 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 government departments and agencies to 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's three-part mandate is set out in subsection 273.64(1) of the *National Defence Act*:

(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: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL

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