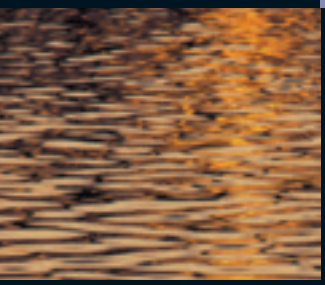
Communications Security Establishment Commissioner

Annual Report



2010-2011

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

Cat. No. D-95-2011

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 2011

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 annual report on my activities and findings for the period of April 1, 2010, to March 31, 2011, 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

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

I was appointed Commissioner of the Communications Security Establishment on June 18, 2010. I knew very little about the challenge that awaited me. I knew that I was following in the footsteps of illustrious colleagues whom I had the privilege of knowing during my career (Chief Justices Bisson and Lamer, and Judges Gonthier and Cory). I knew that I would be involved in the highly technical and fascinating, albeit sensitive field, of security and the protection of the privacy of Canadians. As a lawyer and a Federal Court of Appeal judge, I had been involved in a number of privacy and terrorism cases. However, I would never have imagined the extent of the activities of the Communications Security Establishment Canada (CSEC), nor the critical and active role played by the Office of the Commissioner.

First, I wish to acknowledge the warm welcome that I received from the Office's team. I say "team" because they are a group of people who work together in a remarkable spirit of cooperation and strength of mind and of purpose. I especially appreciated the efforts that were made as soon as I arrived to explain to me in a clear and understandable manner the mandates and roles of the Office and of CSEC respectively. In this regard, I would also like to thank CSEC and its Chief, John Adams, who took considerable time and effort to convey the full nature and scope of CSEC's work. The information sessions that they organized for me were complex and intense, and I must say, well adapted to my needs.

During the first nine months of my mandate, I was impressed by the professionalism, objectivity, and rigour of my analysts. They know they have an important mission, especially in ensuring that the unintentional interception by CSEC of the private communications of Canadians is in compliance with the law. Consequently they leave no stone unturned in their reviews, which are conducted in an impressively detailed and comprehensive manner.

I was also impressed, and I must say surprised, because I was initially sceptical in this regard, with the degree of transparency and spirit of cooperation displayed by CSEC and its Chief. There have been, and will be, of course, significant differences of opinion between my office and CSEC on certain issues. However, overall, I can say that the protection of the privacy of Canadians is, in the eyes of CSEC and its employees, a genuine concern, which is more than I would have imagined at the beginning of my mandate.

During my appearance before the House of Commons' Standing Committee on National Defence on November 18, 2010, I stated in the following terms the dilemma faced by Parliament when passing the *Anti-Terrorism Act* in December 2001:

> Within Canada, every individual has a quasi-constitutional right with respect to his or her privacy. And every person has a constitutional right with respect to security of the person. In addition, the State has an obligation to protect each of these individual rights and to ensure the country's security as well. These rights and obligations are not easy to reconcile: what in fact would the right to privacy mean – or the right to security of the person – in a society where security was no longer taken for granted or that was no longer free and democratic?

I must reconcile these rights and obligations in the very specific context of the activities in which CSEC is engaged. It should be recalled that the first mandate of CSEC is to gather intelligence from foreign entities located outside Canada. CSEC is in fact prohibited by its governing legislation from "spying" on a Canadian wherever he or she might be in the world or on any individual in Canada. It is only unintentionally — and I would add unavoidable given the complexity, pervasiveness and interconnectedness of global telecommunications networks — that private communications are intercepted by CSEC. It is precisely because of this inevitability that the *National Defence Act* provides for ministerial authorization. The number of these intercepts, I hasten to emphasize, is very small.

During my first several months as Commissioner, I took the initiative to meet with the Minister of National Defence, the Chief of CSEC, the National Security Advisor to the Prime Minister, the Security Intelligence Review Committee, the Inspector General of the Canadian Security Intelligence Service, the Privacy Commissioner, and the interim Chair of the Commission for Public Complaints against the Royal Canadian Mounted Police. These meetings enabled me to gain a better appreciation not only of the scale of review activities in Canada but also of the opportunity for greater contact among the various review agencies.

Before explaining my role, I'd like to provide the reader with a clear understanding of CSEC's mandate.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

The *Anti-Terrorism Act* came into effect in December 2001, adding Part V.1 of the *National Defence Act*, and setting out CSEC's three-part mandate:

> Part (a) authorizes CSEC to collect foreign intelligence in accordance with the Government of Canada's intelligence priorities;
>
> Part (b) authorizes CSEC to help protect electronic information and information infrastructures of importance to the Government of Canada; and
>
> Part (c) authorizes CSEC to provide technical and operational help to federal law enforcement and security agencies, including obtaining and understanding communications collected under those agencies' own authorities.

The activities listed under parts (a) and (b) of CSEC's mandate are subject to three legislative limitations aimed at protecting Canadians' privacy:

1. CSEC is prohibited by law from directing its activities at Canadians – wherever they might be in the world – or at any person in Canada;

2. In conducting foreign intelligence or information technology security activities, CSEC may unintentionally intercept a one-end Canadian communication which is a private communication as defined by the *Criminal Code*. CSEC may use and retain this information only if it is essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government computer systems or networks; and

3. To provide a formal framework for the unintentional interception of private communications, the *National Defence Act* requires express authorization by the Minister of National Defence once he or she is satisfied that specific conditions provided for in the *National Defence Act* have been met. These are known as ministerial authorizations.

CSEC is prohibited from directing its activities at Canadians – wherever they might be in the world – or at any person in Canada.

In providing assistance under part (c) of its mandate, CSEC is subject to the same laws and limitations that govern the agencies it is assisting.

Annex A contains text of relevant sections of the *National Defence Act* relating to the role and mandate of CSEC. (p. 33)

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

My mandate under the *National Defence Act* consists of three key functions:

1. **reviewing** CSEC activities to ensure they comply with the law;

2. **conducting** any investigations I deem necessary in response to complaints about CSEC; and

3. **informing** the Minister of National Defence and the Attorney General of Canada of any CSEC activities that I believe may not be in compliance with the law.

I also have a mandate under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to release special operational information on the grounds that it is in the public interest. To date, no such matters have been reported to a Commissioner.

Within the context of CSEC's mandate, the purpose of my reviews is:

- to ensure that activities conducted by CSEC under ministerial authorization are those authorized by the Minister of National Defence;
- to ensure that CSEC complies with the law and only directs its activities at foreign entities located outside Canada;
- to ensure that, in all the activities CSEC undertakes, it effectively applies satisfactory measures to protect the privacy of Canadians; and
- to report the results of my reviews to the Minister of National Defence, who is responsible for CSEC.

Additionally, each year I am required to submit a report to the Minister of National Defence on my activities, which the Minister must then table in Parliament.

My office is an autonomous agency with its own appropriation from Parliament.

While I am mandated to report to the Minister, my office is independent and separate from the Department of National Defence. My strong review mandate reflects the powers I have under the *Inquiries Act* as well as the independent nature of my office, which is an autonomous agency with its own appropriation from Parliament.

Annex B contains the text of the relevant sections of the *National Defence Act* and the *Security of Information Act* relating to my role and mandate as CSE Commissioner (p. 35) and **Annex C** describes the history of the Office of the CSE Commissioner. (p. 37)

COMMISSIONER'S OFFICE

I am supported in my work by a staff of eight, together with a number of subject-matter experts, under contract, as required. In 2010–2011, my office's expenditures were $1,605,422, which is within the allocated appropriation from Parliament.

Annex D provides the 2010-2011 Statement of Expenditures for the Office of the Communications Security Establishment Commissioner. (p. 39)

Objective of Review

The objective of my office's rigorous review process is to enable me to provide to the Minister of National Defence, and indeed to all Canadians, assurance that CSEC is complying with the law and protecting the privacy of Canadians. If I find an instance where CSEC has not complied with the law, I am obliged to inform the Minister of National Defence and the Attorney General of Canada.

> *Rigorous review enables me to provide the Minister assurance that CSEC is complying with the law.*

Selection of activities for review

CSEC activities are selected for review and prioritized using a set of detailed criteria to help determine where risk is greatest for potential non-compliance with the law and for risks to privacy.

Selection and prioritization of subjects for review are documented in my three-year work plan, which is updated regularly as part of an ongoing process of assessing risk.

Risk is assessed by considering, among other factors:

- the controls placed on the activity to ensure compliance with legal, ministerial and policy requirements;
- whether the activity involves private communications or information about Canadians;
- whether the activity is new or how much time has passed since the last in-depth review of an activity;
- whether there have been significant changes to the authorities or technologies relating to the activity;
- whether Commissioners have made findings or recommendations relating to the activity which require follow-up; and
- issues arising in the public domain.

Review methodology and criteria

My staff test the contents of CSEC's databases.

In conducting a review, my staff examine CSEC's written and electronic records, including CSEC's policies and procedures and legal advice received from Justice Canada. My staff request briefings and demonstrations of specific activities, interview managers and employees and observe firsthand CSEC operators and analysts to verify how they conduct their work. My staff test information obtained against the contents of systems and databases. The work of CSEC's internal auditors and evaluators may also inform reviews.

Each review includes an assessment of CSEC's activities against a standard set of criteria, described below, consisting of legal requirements, ministerial requirements, and policies and procedures. Other criteria may be added, as appropriate.

Legal requirements: I expect CSEC to conduct its activities in accordance with the *National Defence Act*, the *Privacy Act*, the *Criminal Code*, the *Canadian Charter of Rights and Freedoms* and any other relevant legislation, and in accordance with Justice Canada advice.

Ministerial requirements: I expect CSEC to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

Policies and procedures: I expect CSEC to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements and the protection of Canadians' privacy. I expect employees to be knowledgeable about and comply with policies and procedures. I also expect CSEC to employ an effective management control framework to ensure that the integrity and lawful compliance of its activities is maintained. This includes appropriate accounting for decisions taken and for information relating to compliance and the protection of the privacy of Canadians.

My review reports contain findings that confirm whether the above-noted criteria have been satisfactorily met by CSEC. These reports may also disclose the nature and significance of deviations from these criteria. In some cases, I make recommendations to the Minister which are aimed at correcting discrepancies between CSEC's activities and the expectations established by the review criteria. I monitor CSEC's efforts to address recommendations and respond to negative findings. As well, I monitor areas for follow-up identified in past reviews.

The Logic Model in **Annex E** provides a flow chart of our comprehensive review program. (p. 41)

Recommendations

Since 1997, my predecessors and I have submitted to the Minister of National Defence a total of 61 classified review reports and studies. In total, the reports contain 133 recommendations. CSEC has accepted and implemented or is working to address 95 percent (122 out of 129) of these recommendations. I am awaiting the Minister's response to the four recommendations I made in 2010-2011. This past year, CSEC completed work in response to three past recommendations and I am monitoring 18 recommendations that CSEC is working to address.

On occasion, CSEC may reject one of my recommendations. In this instance, I assess the reasons provided, in order to determine whether to accept them or to pursue the issue.

See **Annex F** for a complete list of the 61 classified review reports and studies submitted to the Minister of National Defence. (p. 43)

OVERVIEW OF 2010–2011 FINDINGS AND RECOMMENDATIONS

During the 2010–2011 reporting year, I submitted six reports to the Minister of National Defence on my review of CSEC activities.

These reviews were conducted under two areas of my mandate:

- ensuring CSEC activities are in compliance with the law — as set out in paragraph 273.63(2)(*a*) of the *National Defence Act*; and
- ensuring CSEC activities under a ministerial authorization are authorized — as set out in subsection 273.65(8) of the *National Defence Act*.

One review, which is now being done on an annual basis, related to disclosures of information about Canadians to Government of Canada departments and agencies. This review permits me to closely monitor CSEC activities involving Canadian identity information. Performing this review yearly allows me to verify that CSEC complies with the law and maintains measures to protect the privacy of Canadians.

Two reviews were conducted of CSEC information technology security activities conducted under ministerial authorizations.

Three reviews related to foreign signals intelligence activities, and included a review of how CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act*.

The results

Overall, I am able to report that the activities of CSEC examined this year complied with the law.

My reviews in 2010-2011 also demonstrate that:

- CSEC takes seriously and acts on the Commissioner's recommendations. Over the past year CSEC addressed a number of deficiencies identified in previous reviews. My follow-up of these recommendations determined that CSEC addressed these deficiencies;

The activities of CSEC examined this year complied with the law.

- CSEC continued important work to incorporate information management practices into its core programs and has made it part of its employees' daily activities. This is important in enabling CSEC to demonstrate accountability for its activities and decisions; and
- CSEC has mature management, governance and internal oversight structures to guide and direct its operational activities.

In total this past year, I made four recommendations, two of which relate to reporting information to the Minister of National Defence with the objective of providing the Minister with a more complete picture of communications CSEC unintentionally intercepts and involving Canadians or persons in Canada. The other two recommendations strengthen policy guidance for certain foreign signals intelligence activities.

CSEC takes seriously and acts on the Commissioner's recommendations.

Past reviews of CSEC activities under ministerial authorizations have consistently demonstrated that the proportion of private communications that CSEC unintentionally intercepts is very small. Nevertheless, should there be an instance of non-compliance involving private communications, the potential impact on the privacy of Canadians could be significant, which is why I continue to focus my attention on this particular activity.

The proportion of private communications that CSEC unintentionally intercepts is very small.

See **Annex G** for information on legislative safeguards for private communications and information about Canadians. (p. 47)

HIGHLIGHTS OF THE SIX REVIEW REPORTS SUBMITTED TO THE MINISTER IN 2010-2011

1. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 1)

Background

The *National Defence Act* mandates CSEC 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.

This review examined certain information technology security activities conducted by CSEC under ministerial authorization in 2008–2009 at two Government of Canada departments. The activities examined help protect computer systems by detecting, analyzing, and mitigating sophisticated cyber attacks aimed at covertly accessing sensitive government computer networks.

My review followed-up on an operational issue that came to light in late 2006 and which had the potential for non-compliance. The Commissioner's 2007–2008 Annual Report commended the Chief of CSEC for his handling of this issue and for keeping the Commissioner informed of corrective steps.

The review also included an examination of CSEC's responses to the findings and recommendations of a previous review of information technology security activities at a specific Government of Canada department. These previous findings and recommendations related to ambiguities in policy, corporate record keeping and CSEC employees' awareness of their responsibilities for the activities. My review included examining a 2007 CSEC internal audit report relating to these activities.

Review rationale

Specific controls are placed on these information technology security activities to ensure they comply with legal, ministerial and policy requirements. Major changes to certain practices and to CSEC's policies and procedures relating to these activities recently occurred. This is the first review since CSEC restructured these activities. Past Commissioners have also made findings and recommendations on these activities.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements, and CSEC's policies and procedures.
- CSEC's use and retention of unintentionally intercepted private communications and information about Canadians complied with the law and CSEC policies.
- I am pleased to note that, in 2008–2009, CSEC made significant changes to the policies and procedures and to the accountability framework for these activities. I found the new policies and procedures to be comprehensive, containing satisfactory measures to protect the privacy of Canadians.
- CSEC also introduced processes that strengthen employee understanding of the compliance framework, policies and procedures. CSEC monitored the conduct of the activities to verify compliance with legal, ministerial and policy requirements, and retained a complete record of these activities.
- I am confident that the significant changes made to these information technology security activities address the previous findings and recommendations made in the Commissioner's 2006 review.

- Finally, this review included a follow-up examination of a principal CSEC information technology security software tool and database. I confirmed an observation made last year in this office's study of CSEC's information technology security activities not conducted under ministerial authorization: that a software tool used by CSEC has adequate functionality to restrict access to information in the system, to meet security and confidentiality requirements, and to protect the privacy of Canadians.

Recommendations

I made no recommendations.

2. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 2)

Background

This review examined other information technology security activities, conducted for two Government of Canada departments in 2007–2008 and 2008–2009, under ministerial authorizations pursuant to the *National Defence Act*.

The activities at the two departments involved CSEC efforts to penetrate the departments' computer systems (under controlled circumstances) to demonstrate potential vulnerabilities and to test the departments' reactions to such attacks.

My examination included changes to the scope of these activities and to the technology used by CSEC. I assessed these changes in terms of their potential impact on the risk to compliance with the law and on the risk to privacy.

Review rationale

Major changes to certain practices, technologies and CSEC policies and procedures relating to these activities have recently occurred. Specific controls are placed on these activities to ensure compliance with legal, ministerial and policy requirements, while protecting the privacy of Canadians. Past Commissioners had also made findings and recommendations concerning these activities. This is the first review since CSEC restructured these activities.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements and CSEC policies and procedures.
- I found that the new policies and procedures were comprehensive and contained satisfactory measures to protect the privacy of Canadians.
- The record of the activities demonstrated that CSEC's new management control framework provides strong monitoring and compliance validation tools, which help ensure compliance with the law and the protection of Canadians' privacy.
- Changes to the technology and its application by CSEC did not impact on the risk to compliance with the law or on the risk to privacy.

Recommendations

I made no recommendations.

3. Combined annual review of CSEC foreign signals intelligence collection activities conducted under ministerial authorizations

Background

This was the first combined annual review of all foreign signals intelligence collection programs. I am required by the *National Defence Act* to review activities under ministerial authorization. The 2009–2010 Annual Report that I submitted to the Minister describes the recent introduction of the office's horizontal review approach, which involves a thorough examination of processes common to all CSEC foreign intelligence collection activities under ministerial authorization. For example, common to all collection methods are the processes by which CSEC: identifies, selects and directs its activities at entities of foreign intelligence interest; uses, shares, reports, retains or disposes of intercepted information; and takes measures to protect private communications and information about Canadians. My review included examining a CSEC internal audit report relating to these activities.

Review rationale

The horizontal review approach led to a re-assessment of how my office reviews ministerial authorizations. Given that common processes are examined in horizontal reviews, it was determined that this combined annual review of foreign signals intelligence ministerial authorizations would focus on any significant changes and on any private communications unintentionally intercepted by CSEC.

I looked for changes to the authorities and scope of the programs, to the technology used by CSEC, and to the associated management control frameworks. I assessed any changes in terms of their impact on the risk to compliance with the law and on the risk to privacy.

I examined certain metrics relating to interception and the privacy of Canadians. The purpose was to establish a baseline of key information, to examine trends and to allow identification of any significant changes over time. These metrics will also inform the risk assessment process and the development of my review work plan.

Another objective of this review was to examine a sample of private communications intercepted by CSEC under foreign intelligence ministerial authorizations but which had not been used in CSEC reporting. The purpose was to assess whether this sample contained foreign intelligence essential to international affairs, defence or security, as required by the *National Defence Act*.

Findings

The extent to which I assessed CSEC's compliance with the law was determined by this review's focus on identifying and understanding significant changes to the foreign signals intelligence collection programs.

- Within this context, and based on information reviewed and interviews conducted, I found that the activities were authorized under the *National Defence Act* and there was no indication of unlawful activity by CSEC. CSEC met ministerial requirements, and has effective policies and procedures in place to guide its activities.
- There are positive trends in policy development and in the clarity and consistency of the requests for ministerial authorizations. Within the overall amount of communications intercepted by CSEC, I found that the proportion of recognized private communications that had been unintentionally intercepted remained very small.

> ***CSEC retained only those private communications essential to Canada's international affairs, defence, or security.***

- Overall, the foreign signals intelligence collection programs did not change significantly, and as a result, I determined that it is not necessary at this time to conduct an in-depth review of any of these programs.
- With regard to the sample of private communications, based on the information reviewed and interviews conducted, I found that CSEC retained only those private communications essential to Canada's international affairs, defence, or security, as required by law.

Recommendations

I made three recommendations. Two of the recommendations dealt with reporting to the Minister of National Defence certain information relating to privacy, and including in the ministerial authorizations a requirement to report this information. This information is necessary to provide the Minister with a complete picture of CSEC's collection activities and to support the Minister in his accountability for CSEC, including for the measures CSEC takes to protect the privacy of Canadians.

I also recommended that, given the importance of ensuring legal compliance and the protection of Canadians' privacy, CSEC should accelerate the timeline for implementation of an improved policy for the active monitoring of activities under foreign signals intelligence ministerial authorizations.

As of the end of the 2010-2011 reporting period, March 31, 2011, I am awaiting the Minister's response to these recommendations and will note them in next year's annual report.

4. Review of CSEC activities carried out under a ministerial directive and used by CSEC to identify new foreign entities believed to be of foreign intelligence interest

Background

The *National Defence Act* mandates CSEC 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.

CSEC conducts a number of activities for the purposes of locating new sources of foreign intelligence. When other means have been exhausted, CSEC may use information about Canadians when it has reasonable

grounds to believe that using this information may assist in identifying and obtaining foreign intelligence. CSEC conducts these activities infrequently, but they can be a valuable tool in meeting Government of Canada intelligence priorities. CSEC does not require a ministerial authorization to conduct these activities because they do not involve interception of private communications. However, a ministerial directive provides guidance on the conduct of these activities.

In recent years, three reviews have involved some degree of examination of these activities: a Review of CSEC's foreign intelligence collection in support of the Royal Canadian Mounted Police (RCMP) (Phase II) (2006); a Review of CSEC's activities carried out under a (different) ministerial directive (2008); and a Review of CSEC's support to the Canadian Security Intelligence Service (CSIS) (2008).

In his 2006–2007 Annual Report, the late Commissioner Gonthier questioned whether the foreign signals intelligence part of CSEC's mandate (part (a) of its mandate) was the appropriate authority in all instances for CSEC to provide support to the RCMP in the pursuit of its domestic criminal investigations. In his 2007–2008 Annual Report, Commissioner Gonthier stated that pending a re-examination of the legal issues raised, no assessment would be made of the lawfulness of CSEC's activities in support of the RCMP under the foreign signals intelligence part of CSEC's mandate. He also noted that CSEC's support to CSIS raised similar issues. Commissioner Gonthier emphasized that although he was in agreement with the advice that the Department of Justice had provided to CSEC, he questioned which part of CSEC's mandate — part (a) or part (c), the assistance part of CSEC's mandate — should be used as the proper authority for conducting the activities.

Subsequent to these reviews and statements in the annual reports, the Chief of CSEC suspended these activities. CSEC then made significant changes to related policies, procedures and practices.

Review rationale

These activities involve CSEC's use and analysis of information about Canadians for foreign intelligence purposes. Specific controls are placed on these activities to ensure compliance with legal, ministerial and policy requirements. Major changes to certain policies, procedures and practices have recently occurred. This was the first review of these activities since the Chief of CSEC allowed their resumption under new policies and procedures. There were also related issues, findings and recommendations highlighted by my predecessors that required follow-up.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements and CSEC's policies and procedures.
- I found that the new policies and procedures were comprehensive and contained satisfactory measures to protect the privacy of Canadians.
- Because of the significant changes made by CSEC to these activities and the positive results of this review, I am of the view that CSEC has addressed the previous findings and recommendations.
- I assessed that the new processes put in place by CSEC were consistent with part (a) of its mandate. I had no questions similar to those raised in previous years as to whether such activities would be more appropriately authorized under part (c) of CSEC's mandate.
- CSEC's new policies, guidelines and forms address findings and recommendations made by past Commissioners. CSEC managers and officials were knowledgeable about and complied with policies and procedures. CSEC managers routinely and closely monitored these activities to ensure they complied with the governing authorities.

Recommendations

I made no recommendations. However, given that these activities involve CSEC's use and analysis of information about Canadians, and therefore have the potential to affect their privacy, I have directed my office to monitor these activities to ensure they continue to be conducted in accordance with the law, ministerial requirements and CSEC's policies and procedures.

5. Review of the process by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act*

Background

CSEC must also be able to identify those one-end Canadian private communications it can lawfully intercept under a ministerial authorization on the basis that the acquisition of these communications is unintentional and the interception is directed at a foreign entity located outside Canada. This process must contain measures to protect the privacy of Canadians.

For the period of September 2008 to December 2010, I examined and tested the process and practices by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada.

Review rationale

These activities are the foundation of CSEC's foreign signals intelligence collection programs. Specific controls are placed on these activities to ensure they meet the legal, ministerial and policy requirements which are crucial to protecting Canadians' privacy.

Past Commissioners made findings and recommendations on these activities, which required follow-up. In addition, major changes to certain technologies and policies and procedures relating to these activities have recently occurred and others are in progress. This is one of the first in-depth horizontal reviews of a CSEC process common to all foreign intelligence collection methods.

Findings

- Based on information reviewed and interviews conducted, I found that the process by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada is in accordance with the law, ministerial requirements, and CSEC's policies and procedures.
- CSEC has sufficient policies and processes to satisfy the legal requirement not to direct foreign signals intelligence interception activities at a Canadian (anywhere) or at any person in Canada.
- CSEC employees who were interviewed and observed in their work were knowledgeable about relevant policies and procedures and were applying them in the conduct of the activities. CSEC managers routinely and closely monitor the activities to ensure they comply with governing authorities.

CSEC takes measures in the design of its systems to promote compliance with the law and the protection of Canadians' privacy.

- CSEC takes measures in the design of associated systems and databases to promote compliance with the law and the protection of Canadians' privacy. I found that recent enhancements to these systems and databases assist in ensuring compliance with the law, ministerial requirements and policy. Additional planned enhancements will further improve compliance.
- I did find, however, certain deficiencies in some of the associated management systems and databases. I am pleased to note that CSEC is taking measures to address these deficiencies. I will monitor CSEC's efforts in this regard.

Recommendations

CSEC's policies and procedures generally provide sufficient direction to CSEC employees in protecting Canadians' privacy while determining that entities of foreign intelligence interest are foreign entities located outside of Canada. However, policies and procedures applicable to a certain foreign signals intelligence collection program provide only limited direction on the process and practices for such activities. I therefore recommended that CSEC provide specific guidance for these activities.

As of the end of the reporting period, March 31, 2011, I am awaiting the Minister's response to this recommendation and will note it in next year's annual report.

6. Annual review of CSEC disclosures of information about Canadians to Government of Canada clients

Background

This review fulfills a commitment in the 2009–2010 Annual Report to conduct an annual review of a sample of disclosures of information about Canadians to Government of Canada departments and agencies. The purpose is to verify that CSEC complies with the law and maintains measures to protect the privacy of Canadians.

Information about Canadians may be included in CSEC's reports if it is essential to understanding foreign intelligence. However, any information that identifies a Canadian must be suppressed in reports disseminated to government departments and agencies ─ that is, replaced by a generic reference such as "a named Canadian".

See **Annex G** for more detailed information on legislative safeguards for private communications and measures to protect information about Canadians. (p. 47)

When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting government department or agency has both the authority and operational justification for obtaining such information. Only then may CSEC provide this information.

This review encompassed a sample of approximately 20 percent of requests received by CSEC for disclosure of suppressed information about Canadians contained in foreign intelligence reports, from April to September 2010. The sample included disclosures made to all of the Government of Canada departments and agencies that requested, and were provided with, information about Canadians.

My office examined the forms that CSEC used to document the departments' and agencies' authorities and justifications of their need for information about Canadians, as well as the associated foreign intelligence reports.

Review rationale

CSEC's disclosure activities involve the sharing of information about Canadians. Should there be an instance of non-compliance while CSEC conducts these activities, the potential impact on the privacy of Canadians could be significant.

In addition, I assessed CSEC's activities in response to two recommendations in a February 2010 review report of my predecessor relating to: (a) providing tools to support the tracking of clients' requests for, and any associated disclosures of, suppressed information about Canadians; and, (b) improving the consistency and accuracy of CSEC reports to the Minister of National Defence about these activities.

Findings

- Based on information reviewed and interviews conducted, I found that CSEC's disclosure of suppressed information about Canadians to Government of Canada clients was conducted in compliance with the law.

- Policies and procedures were in place to provide sufficient direction to CSEC employees on the protection of the privacy of Canadians.
- CSEC employees were knowledgeable about, and acted in accordance with, policies and procedures. CSEC managers monitored activities to ensure CSEC employees complied with governing authorities.
- I am satisfied that CSEC's practices and the planned implementation of a new system will address previous recommendations and permit CSEC to better track and produce accurate and consistent metrics on these activities.

Recommendations

I made no recommendations but will continue to conduct an annual review of these activities to verify that CSEC continues to comply with the law and maintains measures to protect the privacy of Canadians. I will also monitor CSEC efforts to implement the new system.

COMPLAINTS ABOUT CSEC'S ACTIVITIES

My mandate includes undertaking any investigation I deem necessary in response to a complaint — for example to determine whether CSEC has engaged, or is engaging, in unlawful activity or is not taking sufficient measures to protect the privacy of Canadians.

In 2010–2011, there were no complaints that warranted investigation.

DUTY 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 seeking to defend the release of special operational information on the grounds that it is in the public interest. No such matters were reported in 2010–2011.

ACTIVITIES OF THE COMMISSIONER'S OFFICE

Appearance before the Standing Committee on National Defence

As I mentioned in my introduction, in November 2010 I appeared for the first time before the House of Commons Standing Committee on National Defence, which examined my nomination. I was thankful for the opportunity to meet with the Committee so early in my mandate, to describe my experiences, and to provide an overview of the legislative framework for CSEC and my role and activities. My remarks to the Committee are available on my office's website at www.ocsec-bccst.gc.ca. I look forward to other opportunities to appear before this or other committees of Parliament to discuss my activities and findings or to discuss the importance of review generally.

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 2011. Committee members and my officials and I exchanged information on challenges and best practices in review methodologies and compared differences in respective models for the review of security and intelligence agencies.

Review Agencies Forum

Since 2005, the Review Agencies Forum has brought together officials from my office, the Security and Intelligence Review Committee (SIRC), the Office of the Inspector General of the Canadian Security Intelligence Service, the Commission for Public Complaints against the Royal Canadian Mounted Police (CPC) and the Office of the Privacy Commissioner. The Forum met in January 2011 to discuss issues of common interest.

Training

During 2010, my office developed, and in November delivered, a review workshop for personnel of organizations dedicated to the review of law enforcement and security and intelligence agencies. This workshop contributed to training individuals in these review bodies. The purpose is to enhance the effectiveness of independent review. Another workshop will be held in the fall of 2011.

> *My office developed and delivered a review workshop.*

Several of my staff received training from CSEC in the use of a specific CSEC foreign intelligence database. I would like to express appreciation to CSEC for this training.

Other activities

In October 2010, my office participated in the annual Canadian Association of Security and Intelligence Studies conference in Ottawa. The theme of the conference was Understanding National Security. Leading experts from Canada and abroad provided perspectives on issues of importance to the security and intelligence and review communities.

In December 2010, my office's Executive Director and I met with the Privacy Commissioner of Canada and the Assistant Privacy Commissioner to discuss our respective roles and responsibilities. The Executive Director also participated in a workshop and provided input into the development of an Office of the Privacy Commissioner reference guide for government policy makers.

In March 2011, my office's Executive Director, along with the former Chair of the CPC and the Executive Director of SIRC, participated in a training day for Justice Canada counsel working in the field of national security. The panel made presentations on the importance of review of law enforcement and security and intelligence agencies, including discussion of the findings and recommendations made in the inquiries led by the Honourable Justices O'Connor, Iacobucci and Major.

WORK PLAN — REVIEWS UNDERWAY AND PLANNED

The results of several reviews currently underway are expected to be reported on to the Minister of National Defence in the coming year and will be included in my 2011–2012 Annual Report.

The subjects of these reviews include: an annual review of occurrences identified by CSEC in 2010 that affected or had the potential to affect the privacy of a Canadian, and the measures taken by CSEC to address them; CSEC's foreign intelligence sharing with international partners; assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*; and CSEC's retention and disposal of intercepted information, and, in particular, of private communications and information about Canadians.

Other reviews planned for 2011–2012 include: CSEC information technology security activities conducted under Government of Canada departments' *Criminal Code* and *Financial Administration Act* authorities; activities conducted under CSEC information technology security ministerial authorizations; and particular activities of CSEC's operations centre. Some reviews may carry over into 2012–2013.

In addition, I will continue the annual reviews of foreign intelligence ministerial authorizations, of CSEC disclosures of information about Canadians to government clients, and of occurrences identified by CSEC that affected or had the potential to affect the privacy of a Canadian and the measures taken by CSEC to address them.

In addition to briefings on activities that we plan to review, the Commissioner's office requests briefings from CSEC to assist in determining risk and work plan development. We receive regular briefs on changes to the management and administration of CSEC operational-related programs, including changes to policies and procedures.

THE UPCOMING YEAR

I am beginning the second year of my mandate with optimism and realism. On the one hand, I am optimistic because of the quality of the team that assists me, the rigour of the review process established by the office, and the professionalism underlying relations between CSEC and my office. On the other hand, I am realistic given the constantly changing technological environment and an equally dynamic international environment, to which I and my team, as well as CSEC, must adapt. In this context, I want to ensure that CSEC maintains and reinforces the measures taken to protect the privacy of Canadians.

Our free and democratic society will always be subject to internal and external threats. Each technological development, for example, may have both positive and negative effects. The need to reconcile the right of everyone to a free and democratic society and the right of each person to the protection of his or her privacy demands rigorous and ongoing efforts on the part of those who, like us, have a mandate to ensure that the activities of agencies which operate in the greatest secrecy comply with the law and protect the privacy of Canadians.

The need to reconcile the right of everyone to a free and democratic society and the right of each person to the protection of his or her privacy demands rigorous and ongoing efforts.

My office will carry out several reviews during the upcoming year. I plan to pay special attention to those activities of CSEC which concern me the most and where the risks to privacy are the greatest. I want to ensure that CSEC does not use or retain any private communications that are not related to international affairs, defence, or security, which is a legal requirement. I also want to ensure that the identity of a Canadian is revealed only when it is strictly necessary. The risk to individual privacy is heightened when information is shared, particularly with international partners, and I will report next year on the review under way on this issue.

The part of CSEC's mandate dealing with the protection of information and the information infrastructures of importance to the Government of Canada has gained in prominence; recent incidents have reminded us to what degree our computer systems may be vulnerable. In this context, I have requested my officials to examine in-depth these CSEC activities of growing prominence to ensure that they comply with the law and protect the privacy of Canadians.

A final word on an issue that persists year after year: the need for legislative amendments that will eliminate the ambiguities noted by my predecessors and myself in the *National Defence Act*. I know that the work is under way. It is my hope that the new government elected on May 2nd 2011 will act quickly and that all Members of Parliament will support the elimination of these ambiguities. These legislative amendments, in my opinion, should not provoke any controversy.

ANNEX A: MANDATE OF THE CSEC — EXCERPTS FROM THE *NATIONAL DEFENSE ACT*

The Communications Security Establishment Canada (CSEC) is the 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 aquire 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.

CSEC's website is: www.cse-cst.gc.ca.

ANNEX B: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER — EXCERPTS FROM THE *NATIONAL DEFENSE ACT* AND THE *SECURITY OF INFORMATION ACT*

***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 C: 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. On June 18, 2010, the Honourable Robert Décary, Q.C., a former Justice of the Federal Court of Appeal, was appointed Commissioner.

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.

The omnibus *Anti-terrorism Act,* which came into force on December 24, 2001, 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.

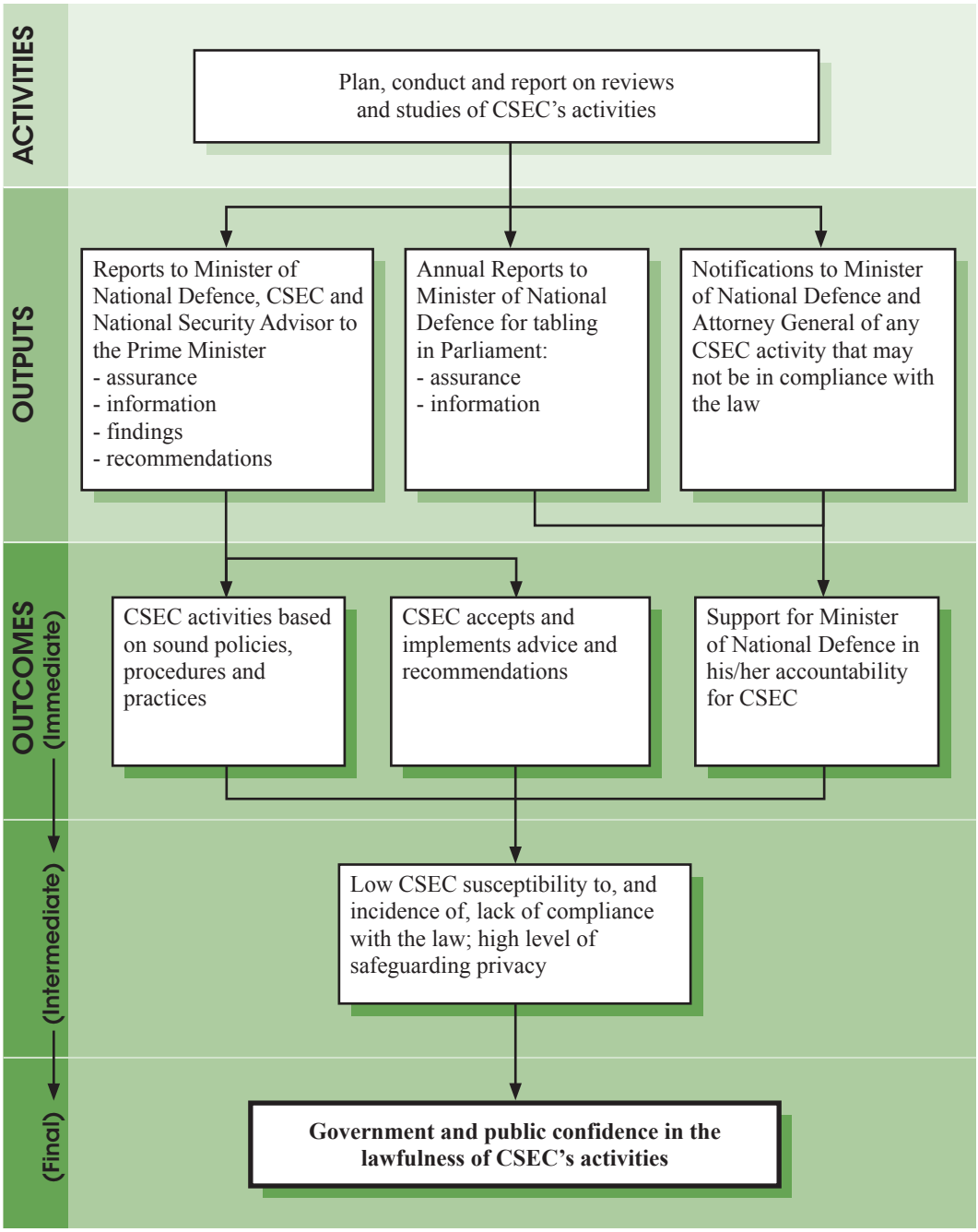
On April 1, 2009, the Commissioner's office was granted its own parliamentary appropriation. While the Commissioner continues to provide the Minister of National Defence with his reports, the Commissioner's office is separate from, and not part of, the Department of National Defence.

ANNEX D: STATEMENT OF EXPENDITURES 2010–2011

Standard Object Summary

Salaries and Wages	$ 890,939
Transportation and Telecommunications	12,995
Information	21,125
Professional and Special Services	457,655
Rentals	170,707
Purchased Repairs and Maintenance	1,249
Material and Supplies	33,252
Machinery and Equipment	17,500
Total	**$ 1,605,422**

ANNEX E: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL



ANNEX F: 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)

56. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 1) – October 18, 2010 (TOP SECRET/COMINT/CEO)

57. Review of CSEC activities carried out under a ministerial directive and used by CSEC to identify new foreign entities believed to be of foreign intelligence interest – December 16, 2010 (TOP SECRET/COMINT/CEO)

58. Review of CSEC information technology security activities conducted under ministerial authorization (Activity 2) – February 14, 2011 (SECRET)

59. Annual review of CSEC disclosures of information about Canadians to Government of Canada clients – February 21, 2011 (CONFIDENTIAL)

60. Combined annual review of CSEC foreign signals intelligence collection activities conducted under ministerial authorizations – February 25, 2011 (TOP SECRET/COMINT/CEO)

61. Review of the process by which CSEC determines that entities of foreign intelligence interest are foreign entities located outside of Canada, as required by the *National Defence Act* – March 15, 2011 (TOP SECRET/COMINT/CEO)

ANNEX G: LEGISLATIVE SAFEGUARDS FOR PRIVATE COMMUNICATIONS AND MEASURES TO PROTECT INFORMATION ABOUT CANADIANS

In the execution of its foreign intelligence and information technology security mandates, CSEC is expressly prohibited pursuant to paragraph 273.64(2)(*a*) of the *National Defence Act* from directing its activities at Canadian citizens, permanent residents or corporations, regardless of their location. CSEC is also prohibited from directing its activities at any person in Canada, regardless of their nationality.

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

Recognizing this possibility, the *National Defence Act* 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 *National Defence Act* are met. There are four conditions for foreign signals intelligence ministerial authorizations (subsection 273.65(2)) and five conditions for information technology security ministerial authorizations (subsection 273.65(4)).

CSEC's foreign signals intelligence and information technology security reports may contain information about Canadians (as defined in section 273.61 of the *National Defence Act*) 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 named Canadian" person or company. When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting government department or agency has both the authority and operational justification for obtaining such information. Only then may CSEC provide this information.

The provision of assistance to federal law enforcement and security agencies under paragraph 273.64(1)(*c*) of the *National Defence Act* is not subject to the statutory prohibition contained in paragraph 273.64(2)(*a*) of the *National Defence Act* against directing activities at Canadians located anywhere or at persons located in Canada, provided that the assisted agency has the lawful authority. CSEC is also subject pursuant to subsection 273.64(3) of the *National Defence Act* to any limitations imposed by law on the assisted agency in the performance of its duties.

CSE Commissioner Annual Report 2010-2011

Commissaire du CST Rapport annuel 2010-2011