Communications Security Establishment Commissioner

ANNUAL REPORT

2013-2014

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984, Station “B”
Ottawa, ON K1P 5R5

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

© Minister of Public Works and
Government Services 2014
Cat. No. D95-2014
ISSN 1206-7490

FSC
www.fsc.org
MIX
Paper from
responsible sources
FSC® C103458

Communications Security
Establishment Commissioner

The Honourable Jean-Pierre Plouffe, C.D.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, C.D.

June 2014

Minister of National Defence
MGen George R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, ON K1A 0K2

Dear Minister:

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, 2013, to March 31, 2014, for your submission to Parliament.

Yours sincerely,

Jean-Pierre Plouffe

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

TABLE OF CONTENTS

Biography of the Honourable Jean-Pierre Plouffe, C.D. /2

Commissioner's Message /3

Mandate of the Communications Security Establishment Commissioner /7

Commissioner's Office /13

Overview of the 2013–2014 Findings and Recommendations /14

Update on CSEC Efforts to Address Previous Recommendations /17

- Update on a review of CSEC assistance to the Canadian Security Intelligence Service (CSIS) under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act* /18

- Update on an ongoing review of CSEC use of metadata /20

Highlights of the Six Classified Reports Submitted to the Minister in 2013–2014 /23

1. Review of CSEC foreign signals intelligence information sharing with international partners /23

2. Review of the activities of the CSEC Office of Counter Terrorism /31

3. Study of CSEC policy compliance monitoring framework and related activities /34

4. Review of CSEC 2012–2013 foreign signals intelligence ministerial authorizations /37

5. Annual review of a sample of disclosures by CSEC of Canadian identity information to Government of Canada clients and second party partners /43

6. Annual review of incidents and procedural errors identified by CSEC in 2013 that affected or had the potential to affect the privacy of Canadians and measures taken by CSEC to address them /45

Complaints About CSEC Activities /48

Duty Under the *Security of Information Act* /48

Activities of the Commissioner's Office /48

Work Plan — Reviews Under Way and Planned /52

In Closing /53

Annex A: Excerpts from the *National Defence Act* and the *Security of Information Act* Related to the Commissioner's Mandate /55

Annex B: Commissioner's Office Review Program — Logic Model /59

Annex C: 2013–2014 Statement of Expenditures /61

BIOGRAPHY OF THE HONOURABLE JEAN-PIERRE PLOUFFE, C.D.

Couvrette/Ottawa

The Honourable Jean-Pierre Plouffe was appointed Commissioner of the Communications Security Establishment effective October 18, 2013, for a period of three years.

Mr. Plouffe was born on January 15, 1943, in Ottawa, Ontario. He obtained his law degree, as well as a master's degree in public law (constitutional and international law) from the University of Ottawa. He was called to the Quebec Bar in 1967.

Mr. Plouffe began his career at the office of the Judge Advocate General at the Department of National Defence. He retired as a Lieutenant-Colonel from the Canadian Armed Forces in 1976. He then worked in private practice with the law firm of Séguin, Ouellette, Plouffe et associés, in Gatineau, Quebec, as defence counsel and also as defending officer for courts martial. Thereafter Mr. Plouffe worked for the Legal Aid Office as defence counsel.

Mr. Plouffe was appointed a reserve force military judge in 1980, and then as a judge of the Quebec Court in 1982. He was thereafter appointed to the Superior Court of Quebec in 1990, and to the Court Martial Appeal Court of Canada in March 2013. He retired as a supernumerary judge on April 2, 2014.

COMMISSIONER'S MESSAGE

In this, my first annual report, I want to set the record straight on what the Office of the CSE Commissioner does, how we do it and the way we develop reports. Unlike what has been publicly speculated over the past year, my role as Commissioner is to ensure Communications Security Establishment Canada (CSEC) is conducting its activities in a manner compliant with the law. Indeed, that is a good part of the reason why I accepted the position of CSE Commissioner last October. I do not wish to live in a society where the state makes unjustified intrusions into its citizens' privacy. Nor, however, do I wish to live in a country where the security both of its citizens and of the nation itself is not a priority of the government, especially at this time when increasingly serious and complex challenges threaten our national interests.

My job of independent and external review is focused squarely on CSEC and whether its operational activities respect the law and the privacy of Canadians. CSEC's legislated mandate has clear provisions and limitations on its activities when it comes to protecting the privacy of Canadians.

An intense public debate was sparked by unauthorized disclosures of classified documents by Edward Snowden, a former contractor to the United States' National Security Agency (NSA), about activities of the NSA, as well as of CSEC and its other Five Eyes partners (in the United Kingdom, Australia and New Zealand). I am concerned that commentators are raising fears that are based, not on fact, but rather, on partial and sometimes incorrect information regarding certain CSEC activities. I want to reassure Canadians, especially those who are skeptical about the effectiveness of review of intelligence agencies, that I am scrupulously investigating those CSEC activities that present the greatest risks to compliance with the law and to privacy. Rest assured that I will do so with the requisite vigour and all the powers of the *Inquiries Act* necessary to arrive at comprehensive conclusions. I will make public as much information as possible about these investigations, their resulting conclusions and any recommendations. Transparency is important to maintain public trust.

I am also staying current with developments in CSEC's world, whether those developments concern technological capabilities, organizational changes or legal issues. I will inform the Minister of National Defence if I conclude that there is any law, direction or policy that I believe is not clear or effective in terms of ensuring compliance and the protection of privacy. However, it is for Parliament to determine whether the scope of CSEC activities is to be changed. I am prepared to appear before parliamentary committees and contribute to any such discussions.

The right to privacy is a fundamental tenet of a free and democratic society. The *Canadian Charter of Rights and Freedoms* guarantees that Canadians can enjoy a reasonable expectation of privacy. In a free and democratic society, however, there are certain cases where a need for a limit on the privacy of an individual can be demonstrably justified.

CSEC collects foreign signals intelligence in order to protect Canada's national interests, including against a number of foreign-based threats such as terrorism, espionage, cyber attacks, kidnappings of Canadians abroad or attacks on Canadian embassies. In collecting this intelligence, it is unavoidable that CSEC will obtain some information about Canadians. The *National Defence Act* prohibits CSEC from targeting the private communications of a Canadian. However, at the same time, it does permit CSEC to use and retain a private communication that is intercepted under a ministerial authorization if: the interception is the result of targeting a foreign entity outside of Canada; the information is essential to international affairs, defence or security; and satisfactory measures are in place to protect the privacy of Canadians. Parliament would not have introduced requirements, in the *National Defence Act*, for the protection of information about Canadians, if its intent was to prohibit CSEC from using and retaining intercepted information about Canadians. However, each particular piece of information about a Canadian is subject to a privacy interest and this is a focus of each of my reviews. I also verify that CSEC's activities do not intentionally target the private communications of Canadians or any person in Canada, which would be unlawful.

Over the years, my office has found that CSEC deletes almost all of the small number of recognized foreign signals intelligence private communications unintentionally intercepted by its collection programs. This year, to increase the assurance that I can provide to the public in this report, I directed my employees to examine all — rather than a sample — of these private communications that were used or retained by CSEC. The results of this review are described in detail in the highlights section of this report.

I welcome the engagement of Canadians in considering the role of foreign signals intelligence and cyber defence activities in an increasingly complex and interconnected world, and in reconciling the requirements of privacy on the one hand, and public safety and national security on the other. This debate is further complicated by rapid technological developments, particularly in the area of telecommunications, which have far-reaching implications for privacy, cyber defence activities, and intelligence collection. It is my goal to carry on my predecessor's work to be more informative and transparent about the activities of my office and of CSEC. To this end, we have posted additional information on the office website concerning current issues and how we go about our work. Other measures include discussions with media representatives and academics, as well as participation in a number of conferences on privacy and security to explain our work and to learn about public perspectives. As we continue our public outreach, I look forward to feedback on our efforts.

Given the increased interest of the public over this past year in the activities of my office, I want to take advantage of this opportunity to better inform Canadians. This year's report also repeats some background information, which I believe is necessary in the current context for readers to fully understand my review of CSEC.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

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

1. reviewing CSEC activities to determine whether they comply with the law;

2. undertaking any investigation I deem necessary in response to a written complaint (more information on the Commissioner's responsibilities for conducting investigations into complaints is available on the office's website); and

3. informing the Minister of National Defence (who is accountable to Parliament for CSEC) and the Attorney General of Canada of any CSEC activities that I believe may not be in compliance with the law.

Legislative basis for CSEC activities

When the *Anti-terrorism Act* came into effect on December 24, 2001, it added Part V.1 to the *National Defence Act*, and set out CSEC's three-part mandate:

- part (a) authorizes CSEC to acquire and use foreign signals 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 assistance to federal law enforcement and security agencies, including helping them obtain and understand communications collected under those agencies' own lawful authorities.

(CSEC's website provides more information on CSEC's mandate: www.cse-cst.gc.ca.)

With the emphasis on reviewing the lawfulness of CSEC activities and the protection of the privacy of Canadians, the legislation requires that the CSE Commissioner be a supernumerary or retired judge of a superior court.

The **Commissioner's legislative mandate** includes:

- full independence, at arm's length from government and a separate budget granted by Parliament;
- full access to all CSEC facilities, files and systems; and
- full access to CSEC personnel, including the power of subpoena to compel individuals to answer questions.

CSE Commissioner

The Commissioner is an independent statutory officer and is not subject to general direction from the Prime Minister, the Minister of National Defence (who is accountable to Parliament for CSEC) or any other minister on how to carry out his mandate. The Commissioner assists the Government of Canada in its control of CSEC by providing advice to the Minister of National Defence to support the Minister's decision making and accountability for CSEC. The Commissioner's unclassified annual report for Parliament states whether CSEC has acted lawfully and the extent to which it protected the privacy of Canadians in the conduct of its activities, as do his classified reports to the Minister.

To be effective, reviewers need specialized expertise to be able to understand the technical, legal and privacy aspects of CSEC activities. They also need security clearances at the level required to examine CSEC records and systems. They are bound by the *Security of Information Act* and cannot divulge to unauthorized persons the specific information they access.

I also have a mandate under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy if they believe it is in the public interest to release special operational information of CSEC. (More information on the Commissioner's responsibilities for public interest defence is available on the office's website.)

Annex A 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. 55).

Our approach

The purpose of my review mandate is:

- to determine whether CSEC complies with the law and, if I believe that it may not have complied, to report this to the Minister of National Defence and to the Attorney General of Canada;
- to determine whether the activities conducted by CSEC under ministerial authorization are, in fact, those authorized by the Minister of National Defence, and to verify that the conditions for authorization required by the *National Defence Act* are met;
- to verify that CSEC does not direct its foreign signals intelligence and information technology (IT) security activities at Canadians; and
- to promote the development and effective application of satisfactory measures to protect the privacy of Canadians in all the operational activities CSEC undertakes.

Protection of Canadians' privacy

CSEC is prohibited by law from directing its foreign signals intelligence collection and IT security activities at Canadians — wherever they might be in the world — or at any person in Canada. My review of CSEC activities includes determining whether CSEC takes satisfactory measures to protect every Canadian's reasonable expectation of privacy in CSEC use and retention of collected communications. I examine CSEC use, disclosure and retention of private communications. I verify that Canadian identity information is protected and only shared with authorized partners when needed for understanding the foreign signals intelligence or cyber defence information. I also verify that metadata is used to understand the global information infrastructure, obtain foreign intelligence or protect cyber systems, but *not* to obtain information about a Canadian. I am required under the *National Defence Act* to report to the Attorney General of Canada and to the Minister of National Defence any activities that I believe may not be in compliance with the law, with a particular emphasis on privacy.

Using a variety of methods, we are continuously conducting reviews of:

- selected activities based on a risk analysis, to ensure compliance at a detailed level;
- electronic systems, tools and databases;
- a cross-section of activities to verify compliance in relation to broad issues, such as privacy or metadata; and
- the content of policies, procedures and controls to identify existing or potential systemic weaknesses and to determine how they are applied by CSEC employees.

(More information on the Commissioner's risk-based and preventative approach to selecting and prioritizing reviews is available on the office's website.)

Each review includes an assessment of CSEC activities against a standard set of criteria:

- **Legal requirements:** I expect CSEC to conduct its activities in accordance with the *National Defence Act*, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code*, and any other relevant legislation, and in accordance with Justice Canada legal 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 including the protection of the privacy of Canadians. I expect CSEC employees to be knowledgeable about and comply with policies and procedures. I also expect CSEC to have an effective compliance validation framework and activities to ensure the integrity of operational activities is maintained, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

(More information on the Commissioner's review methodology and criteria is available on the office's website.)

Reporting on our findings

My classified review reports document CSEC activities, contain findings relating to the review criteria, and disclose the nature and significance of any deviations from the criteria. Where and when appropriate, I make recommendations to the Minister of National Defence aimed at improving privacy protections or correcting discrepancies between CSEC activities and my expectations.

I determine the content of my reports, which are based on facts and conclusions drawn from those facts. The reports are free of any interference by CSEC or any Minister.

The results of individual reviews are the subject of classified reports to the Minister of National Defence. Following the standard audit practice of disclosure, draft versions of review reports are presented to CSEC for confirmation of factual accuracy. This is essential to the review process given that my recommendations are based on the facts as uncovered in my reviews.

The Commissioner's annual report for Parliament is a public document. CSEC reviews the draft to verify that it does not contain any classified information according to the *Security of Information Act*. In the interest of transparency and better public understanding, I push the limits to include as much information as possible in my report. The report is provided to the Minister of National Defence who must by law table it in Parliament.

In the interest of transparency within a stringent security framework, my office publishes on our website the titles of all review reports submitted to the Minister of National Defence (with any classified information removed) — 81 to date — to demonstrate the depth and breadth of Commissioners' reviews.

The logic model in **Annex B** provides a flow chart of the review program (p. 59).

COMMISSIONER'S OFFICE

In 2013–2014, I was supported in my work by a staff of 11, together with a number of subject-matter experts, as required. My office's expenditures were $1,943,120 which is within the overall funding approved by Parliament. This was the first year the office operated in expanded physical space to accommodate an increase in the number of employees.

Annex C provides the 2013–2014 Statement of Expenditures for the Office of the CSE Commissioner (p. 61).

(Information on the history of the Office of the CSE Commissioner is available on the office's website.)

OVERVIEW OF THE 2013–2014 FINDINGS AND RECOMMENDATIONS

During the 2013–2014 reporting year, six classified reports were submitted to the Minister of National Defence on reviews and a study of CSEC activities.

These investigations 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*.

The results

Each year, I provide an overall statement on my findings about the lawfulness of CSEC activities. **All of the activities of CSEC reviewed in 2013–2014 complied with the law**. CSEC was cooperative with my office in the conduct of reviews.

This year, I made 10 recommendations to promote compliance, strengthen privacy protection and support the Minister of National Defence in his decision making and control of CSEC.

A number of reviews focused on the need for precision and accuracy of language in information exchanges with CSEC's domestic and international partners.

I examined a number of new automated processes of CSEC, with privacy protections being built into them. I verified CSEC's use of technology to diminish the possibilities of human errors or privacy violations.

Information sharing with international partners was the focus of a specific in-depth review and was an important part of three other reviews. I recommended that the Minister of National Defence issue a new directive to CSEC on information sharing activities with its second party partners in the United States, the United Kingdom, Australia and New Zealand (that is, second party partners are CSEC's counterparts in the Five Eyes alliance), to clearly set out expectations for the protection of the privacy of Canadians. I recommended that CSEC promulgate guidance to formalize and strengthen practices for addressing potential privacy concerns involving second party partners. I also recommended that CSEC record second party partners' confirmation that they have actioned CSEC requests to address any privacy incidents relating to a Canadian.

Two recommendations require CSEC to make available to the Minister of National Defence more comprehensive information regarding communications it collects and the private communications it unintentionally intercepts as part of authorized foreign signals intelligence collection, as well as information CSEC obtains from its second party partners.

Two recommendations emphasize the requirement for CSEC to immediately identify a foreign signals intelligence private communication for essentiality to international affairs, defence or security, and to regularly assess whether the retention of a private communication is strictly necessary and remains essential to international affairs, defence or security, or whether that communication should be deleted.

Three recommendations address gaps in CSEC policy related to: proper accountability and approvals for certain sensitive activities; certain metadata activity; and the specific circumstances and handling of a particular type of communication.

The recommendations are described in the section on highlights of reviews. My office and I will monitor developments.

In addition to the five reviews and one study completed this year, my predecessor sent a letter to the Minister in June 2013 to report on a follow-up review of certain CSEC activities. In this review, Commissioner Décary examined a small number of additional CSEC documents relating to certain individuals. He did not have any outstanding questions relating to compliance with the law or to the protection of the privacy of Canadians.

UPDATE ON CSEC EFFORTS TO ADDRESS PREVIOUS RECOMMENDATIONS

Since 1997, my predecessors and I have submitted to the Minister of National Defence 81 classified review reports. In total, the reports contained 148 recommendations. CSEC has accepted and implemented or is working to address 93 percent (137) of these recommendations, including all 10 recommendations this year.

Conducting investigations

Over the past five years, my officials have interviewed approximately one third of CSEC foreign signals intelligence employees involved in targeting, collection, processing, analysis and reporting activities.

Commissioners monitor how CSEC addresses recommendations and responds to negative findings as well as areas for follow-up identified in past reviews. This past year, CSEC advised my office that work had been completed in response to three past recommendations.

At the end of the 2012–2013 reporting period, the office was awaiting former Minister MacKay's response to two recommendations relating to my predecessor's review of certain foreign signals intelligence activities. Subsequently, the former Minister agreed with CSEC's management response and accepted the recommendations. Respecting the first recommendation, CSEC has promulgated updated policy guidance respecting how to clearly and consistently communicate with its partners about what entity its activities are being directed at. CSEC also provided training and awareness sessions to managers and analysts on the need for clarity of language in communications. With respect to the second recommendation, CSEC has taken a number of actions to ensure analysts have complete knowledge of existing policy guidance on their responsibilities for determining the foreign status of an entity and the justification for directing an activity at that entity, as well as actions for CSEC managers to verify that analysts follow this guidance. These actions include: specific policy guidance introduced since the period

under review that provides clear instructions to analysts on targeting; policy compliance monitoring by a dedicated team; as well as mandatory classroom training, on-the-job training and a compulsory on-line test on protecting privacy.

CSEC implemented a third past recommendation by providing specific policy guidance for targeting for a particular method of foreign signals intelligence collection.

In addition, my office and I are monitoring 13 active recommendations that CSEC is working to address — three outstanding recommendations from previous years and 10 from this year.

Update on a review of CSEC assistance to the Canadian Security Intelligence Service (CSIS) under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*

In last year's annual report, my predecessor reported on his findings and recommendations respecting his review of *CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the CSIS Act*. Commissioner Décary examined CSEC assistance to CSIS following an October 2009 Federal Court order that authorized CSIS, with the assistance of CSEC, to obtain a warrant to collect intelligence on Canadians located outside Canada provided that the interception of the communications or seizure of information occurred from within Canada. One of Commissioner Décary's recommendations, implemented by CSEC, was that CSEC advise CSIS to provide the Court with certain additional evidence about the nature and extent of the assistance CSEC may provide to CSIS, namely respecting CSEC seeking assistance from and sharing information about the Canadian subjects of the warrants with its second party partners. Commissioner Décary shared with the Security Intelligence Review Committee (SIRC) certain general points relating to CSIS that arose out of the two recommendations, for SIRC to follow up on as it deemed appropriate. (SIRC also conducted a review on this subject, which was summarized in its 2012–2013 annual report.)

Subsequent to the tabling in August 2013 of Commissioner Décary's annual report, the Honourable Mr. Justice Mosley issued an order in September requiring that counsel for CSEC and CSIS appear before the Federal Court to speak to the matter raised in the report.

In November 2013, Justice Mosley delivered *Redacted Amended Further Reasons for Order* in this matter. He recognized "the hazards related to the lack of control over intelligence information once it has been shared" with foreign agencies that were highlighted in Commissioner Décary's and SIRC's reports (paragraph 115). Justice Mosley concluded that the Federal Court's "jurisdiction does not extend to the authority to empower the Service [CSIS] to request that foreign agencies intercept the communications of Canadian persons travelling abroad either directly or through the agency of CSEC under its assistance mandate" (paragraph 119). Justice Mosley also indicated: "[t]he failure to disclose that information [that CSIS would request assistance of the Second Parties through CSEC] was the result of a deliberate decision to keep the Court in the dark about the scope and extent of the foreign collection efforts that would flow from the Court's issuance of a warrant. This was a breach of the duty of candour owed by the Service [CSIS] and their legal advisors to the Court" (paragraphs 117 and 118).

Some have suggested that this matter points to a failure of the review bodies to help control the intelligence agencies. On the contrary, these events demonstrate how review works, as Justice Mosley was alerted to this following Commissioner Décary's recommendations. It also demonstrates how review bodies — in this case the Commissioner's office and SIRC — can cooperate and share information within existing legislative mandates.

Update on an ongoing review of CSEC use of metadata

The issue of metadata has served as the focal point for public discussion about CSEC, its activities and my review of those activities. In June 2013, in response to greater public demand for information in the wake of unauthorized disclosures of classified information on foreign signals intelligence, my predecessor issued a statement explaining CSEC use of metadata, the measures in place to protect the privacy of Canadians, the role of the office and past reviews. This statement was unprecedented and significant in that it contained information previously considered highly classified by government and had therefore never been released.

In January of this year, I confirmed that my office was aware of a particular metadata activity that was the subject of media reports alleging that CSEC illegally tracked the movements and on-line activities of persons at a Canadian airport. I stated that this activity did not involve "mass surveillance" or tracking of Canadians or persons in Canada as purported in some stories. (The statements are available on the office's website.)

What is metadata? Metadata is information associated with a communication that is used to identify, describe, manage or route that communication. It includes, but is not limited to, a telephone number, an e-mail or an IP (Internet protocol) address, and network and location information. Metadata excludes the content of a communication. CSEC is allowed to use metadata only to understand the global information infrastructure, to provide foreign intelligence on foreign entities located outside Canada or to protect computer systems of importance to the Government of Canada.

Under the *National Defence Act*, the **global information infrastructure** includes electromagnetic emissions, communications systems, IT systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems or networks.

Paragraphs 273.64(1)(*a*) and (*b*) of the *National Defence Act* authorize CSEC to collect, use, share and retain metadata. A ministerial directive provides additional guidance and places limits on CSEC metadata activities. Thus far, I have confirmed that metadata remains fundamental to CSEC's mandated activities. CSEC uses metadata, for example, to determine the location of a communication, to target the communications of foreign entities outside Canada, and to avoid targeting a Canadian or a person in Canada.

As with any of its activities, CSEC is prohibited from directing its metadata activities at a Canadian or at any person in Canada. However, some metadata collected by CSEC is information about Canadians and CSEC must take measures to protect privacy in the use of that metadata. The Minister of National Defence has provided direction to the Chief of CSEC on metadata activities, including on the protection of the privacy of Canadians. The Chief has further elaborated and provided guidance to CSEC employees, through various internal policies, regarding the procedures and practices that must be followed for activities that may use metadata.

My office's first focused review on metadata began in 2006. Over the years, it has continued to examine and monitor CSEC use of metadata and Commissioners have made a number of recommendations relating to metadata. For example, in 2008, CSEC suspended certain activities involving information about Canadians and made significant changes to policies and practices before restarting those activities.

Planning for another comprehensive review of metadata was under way prior to the unauthorized disclosures by Edward Snowden last June. In light of the significant public interest in this issue, this ongoing review is a high priority. It provides an opportunity to once again examine CSEC's metadata activities, to assess changes to the activities and to determine compliance with the law and whether CSEC protects the privacy of Canadians. It will also follow up on observations of past Commissioners. For the first time, this review includes an in depth examination of how CSEC uses metadata to identify cyber attacks and

threats to Canada's critical information infrastructure. My review has identified some important questions, which I will continue to examine in the coming year, including: what are the vulnerabilities and risks to the privacy of Canadians imposed by new technologies that CSEC uses to collect and analyze metadata? How and to what extent can privacy protections be built directly into the technologies and processes used by CSEC for metadata collection and analysis? I will report on the results in my next public annual report.

About metadata

CSEC metadata analysis activities, which CSEC conducts to understand global communications networks, have been the subject of my office's reviews for the past eight years. When the media suggested that CSEC had illegally tracked the movements and on-line activities of persons at a Canadian airport, we were briefed by CSEC. We questioned the CSEC employees involved and examined results of the activity. Based on our investigation and on our accumulated knowledge, I concluded that this CSEC activity did not involve "mass surveillance" or tracking of Canadians or persons in Canada; no CSEC activity was directed at Canadians or persons in Canada. Even with this finding, I recognize that metadata collection deserves persistent scrutiny. Before the news reports surfaced, my office had already started another in-depth review focused exclusively on metadata, in addition to many other reviews that involve analyzing some aspect of metadata activities.

(More details on CSEC's metadata activities can be found in the testimony of the Chief of CSEC on February 3, 2014, before the Senate Committee on National Security and Defence.)

HIGHLIGHTS OF THE SIX CLASSIFIED REPORTS SUBMITTED TO THE MINISTER IN 2013–2014

1. Review of CSEC foreign signals intelligence information sharing with international partners

Background

CSEC's ability to fulfill its foreign signals intelligence collection and IT security mandates rests, in part, on building and maintaining productive relations with its foreign counterparts. CSEC's long-standing relationships with its closest allies — the U.S. National Security Agency, the U.K. Government Communications Headquarters, the Australian Signals Directorate and the New Zealand Government Communications Security Bureau — continue to benefit CSEC, and, in turn, the Government of Canada. This cooperative alliance may be more valuable to Canada now than at any other time, in the context of increasingly complex technological challenges added to dynamic international affairs and threat environments. Canada is a net importer of intelligence; the amount of foreign signals intelligence CSEC receives from the Second Parties is extensive.

The global nature of today's threats requires security and intelligence agencies to cooperate and share information with one another. The Government of Canada's response to the report of the Standing Committee on Public Safety and National Security, *Review of the Findings and Recommendations Arising from the Iacobucci and O'Connor Inquiries*, recognized that:

> the exchange of information with foreign partners raises unique challenges — policy, legal and operational — that are examined on a case-by-case basis in the context of Canada's national security environment. The 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. (p. 4)

The need for information sharing is vital. However, information must be exchanged in compliance with the law, including the *Charter*, and must include sufficient measures to protect the privacy of Canadians.

The Five Eyes foreign signals intelligence alliance evolved from collaboration during the Second World War. Long-standing agreements and present-day resolutions provide the foundation for CSEC foreign signals intelligence information sharing with the Second Parties. Although these cooperative arrangements include a commitment by the partners to respect the privacy of each other's citizens, it is recognized that each partner is an agency of a sovereign nation that may derogate from the agreements and resolutions, if it is judged necessary for their respective national interests.

This was the first review focused exclusively on CSEC foreign signals intelligence information sharing activities with the Second Parties. In the first part of the review, which was summarized in his 2011–2012 public annual report, former Commissioner Décary found that CSEC has substantial controls and measures in place to help ensure that its foreign signals intelligence information sharing with the Second Parties is lawful and protects the privacy of Canadians.

The second part of the review focused on two questions:

1. How does CSEC assure itself that its international partners follow the long-standing agreements and practices that provide a foundation for CSEC's foreign signals intelligence information sharing?
2. How many private communications and what volume of information about Canadians does CSEC share with and receive from the Second Parties?

Commissioner Décary assessed CSEC activities in the context of the limitations in the *National Defence Act* for the protection of the privacy of Canadians, that is, CSEC foreign signals intelligence

activities "shall not be directed at Canadians or any person in Canada" (paragraph 273.64(2)(*a*) of the *National Defence Act*) and "shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information" (paragraph 273.64(2)(*b*) of the Act). He examined the legislative framework for CSEC's provision to and receipt from the Second Parties of intercepted communications and other foreign signals intelligence information, particularly private communications and information about Canadians. He also examined CSEC's due diligence respecting its sharing activities, for example, to see whether CSEC takes all reasonable steps to confirm that the Second Parties treat Canadians' privacy consistent with the laws of Canada and the privacy protections applied by CSEC.

Findings and recommendations

Commissioner Décary's review resulted in two recommendations to support the Minister of National Defence in his accountability for CSEC and to provide additional measures to protect the privacy of Canadians.

The first recommendation related to the first question about how CSEC assures itself that its second party partners follow the long-standing agreements and practices, including the protection of the privacy of Canadians.

The allies recognize each other's sovereignty and respect each other's laws by pledging not to target one another's communications. Consequently, CSEC policies and procedures state that collection activities are not to be directed at second party nationals located anywhere, or against anyone located in second party territory. Document review, discussions in interviews and written answers suggest that CSEC conducts its foreign signals intelligence activities in a manner that is consistent with the agreements it has with its second party partners to respect the privacy of the partners' citizens, and to follow the partners' policies in this regard.

CSEC trusts that its second party partners will follow the general statements found in the agreements signed among the Second Parties and similarly not direct activities at Canadians or persons in Canada. However, Commissioner Décary was unable to assess the extent to which CSEC's second party partners follow the agreements and protect the private communications and information about Canadians in what CSEC shares with the partners. CSEC does not as a matter of general practice seek evidence to demonstrate that these principles are in fact being followed.

While CSEC uses indicators that it believes provide sufficient assurance that the Second Parties are honouring their arrangements, it did not initially demonstrate knowledge or provide evidence of how its second party partners treat information relating to Canadians. During the conduct of this review, CSEC declined to provide the Commissioner's office with a description of or a copy of relevant extracts of second party policies on the handling of this information. CSEC also declined at that time to identify for the Commissioner's office any specific differences — large or small — between respective partners' laws, policies and practices and how this may affect the partners' protection of the privacy of Canadians. CSEC suggested at that time that review of second party authorities and activities pertain to the Second Parties and not to the lawfulness of CSEC activities and these questions were therefore outside of the Commissioner's mandate.

As a result, **Commissioner Décary recommended** that the Minister of National Defence issue a new ministerial directive to provide general direction to CSEC on foreign signals intelligence information sharing activities and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities. Commissioner Décary recommended that the drafting of this new directive be informed by an in-depth analysis of the potential impact of respective national differences in legal and policy authorities on CSEC compliance with the law and the protection of the privacy of Canadians, that is, a risk assessment. He recognized that such a risk assessment is not a trivial undertaking, would take time, and would require the cooperation of the Second Parties.

Subsequent to Commissioner Décary sending his classified report to the Minister of National Defence, the new Chief of CSEC, Mr. John Forster, re-examined CSEC's initial position, sought permission from second party partners, and provided the Commissioner's office with detailed documentation relating to respective second party policies and procedures on the treatment of information about Canadians. This is one example of Chief Forster's positive leadership to promote increased transparency of CSEC activities and to support review by my office. The second party policies contain comprehensive guidance directing their respective employees to protect and treat information about Canadians in a manner comparable to CSEC's approach.

However, in light of recent controversies in some second party countries, including about alleged domestic spying by their foreign signals intelligence agencies, I remain in agreement with Commissioner Décary that a risk assessment is essential. My office and I continue to follow developments in second party countries closely.

To formalize and strengthen practices for addressing potential privacy concerns involving second party partners, the new ministerial directive should explicitly acknowledge the risks associated with the fact that the information CSE shares with the Second Parties may include the communications of Canadians and information about Canadians, and that CSEC cannot demand, for reasons of sovereignty, that its second party partners account for any use of such information.

Commissioner Décary went beyond the basic scope of this review and recommended that the new directive address IT security information sharing with the Second Parties, as well as foreign signals intelligence information sharing.

Commissioner Décary's second recommendation related to private communications and the volume of information about Canadians CSEC shares with and receives from the Second Parties.

The unintentional interception of a private communication by CSEC is a different situation than the unintentional acquisition by CSEC from a second party source of a one-end Canadian communication.

Ministerial authorizations

The *National Defence Act* allows the Minister of National Defence to give CSEC written ministerial authorization to not be held criminally responsible if, during an authorized act of collecting foreign signals intelligence, private communications are unintentionally intercepted. The law specifies the conditions under which a ministerial authorization can be issued. Without the ministerial authorization regime, CSEC would be prohibited under the *Criminal Code* from intercepting the communications of a targeted foreign entity located outside Canada that was in contact with a Canadian or person in Canada.

The 2001 amendments to the *National Defence Act* established the ministerial authorizations regime. Ministerial authorizations allow CSEC to direct its activities at foreign entities abroad, for the sole purpose of providing foreign signals intelligence in accordance with the Government of Canada's intelligence priorities, even if doing so risks the unintentional interception of private communications of Canadians. By means of a ministerial authorization, the Minister of National Defence may authorize CSEC to conduct activities that risk the interception of private communications, as long as CSEC has met relevant criteria outlined in the *National Defence Act* (for example, by directing collection at foreign entities located outside Canada and implementing measures to protect the privacy of Canadians with respect to the use or retention of private communications unintentionally intercepted). Foreign signals interception activities conducted under a ministerial authorization must satisfy conditions stated in subsection 273.65(2) of the *National Defence Act*, and may also be subject to additional measures that the Minister of National Defence considers advisable. For example, to protect the privacy of Canadians, pursuant to

subsection 273.65(5) of the Act, a ministerial authorization may require CSEC to report certain information to the Minister.

The requirements in ministerial authorizations apply only to interceptions conducted by CSEC under CSEC authorities using CSEC's own capabilities. The ministerial authorization regime is a Canadian instrument and applies to CSEC; it has no application to the Second Parties or to their respective sovereign regimes, since those parties treat information according to their own domestic authorities. Ministerial authorizations cover CSEC's unintentional interception of private communications, not CSEC's acquisition of foreign signals intelligence from second party sources. Such sharing is implicitly authorized under part (a) of CSEC's mandate [paragraph 273.64(1)(*a*) of the *National Defence Act*].

International collaboration

CSEC is prohibited from requesting an international partner to undertake activities that CSEC itself is legally prohibited from conducting. My reviews examine CSEC cooperation with its allies to ensure compliance with the law.

As a result, CSEC has not reported to the Minister of National Defence details, for example, regarding communications involving Canadians or information about Canadians that have been shared by its second party partners. Therefore, to support the Minister of National Defence in his accountability for CSEC and as an additional measure to protect the privacy of Canadians, **Commissioner Décary recommended** that CSEC report such details to the Minister on an annual basis.

Strong arguments can be made that a Canadian's expectation of privacy in her or his communications would be at least the same if not greater whether the communications are unintentionally intercepted and recognized by CSEC itself or are unintentionally acquired by a second party partner and shared with CSEC.

Regularly reporting to the Minister of National Defence a wider range of statistical information relating to information shared with the Second Parties, in a manner similar to the existing ministerial authorization statistics, would support the Minister in his accountability for CSEC. This would make the Minister aware of the extent of such information relating to Canadians and thereby supplement existing measures to protect the privacy of Canadians.

Conclusion

Information sharing with CSEC's second party partners is an essential component of CSEC's foreign signals intelligence collection and other activities. It is also a fact that each of the Second Parties, as a sovereign nation, can derogate from agreements made with CSEC as dictated by their own national interests. Attempting to prescribe in agreements or policies all details and to anticipate all eventualities respecting CSEC foreign signals intelligence information sharing with the Second Parties is not reasonable.

However, CSEC foreign signals intelligence information sharing activities with the Second Parties has the potential to directly affect the privacy and security of a Canadian when private communications or identity information is shared. Precision and accuracy of language in exchanges of information can be critical and affect outcomes, including how individuals are treated. That is why this review resulted in two recommendations to support the Minister of National Defence in his accountability for CSEC and to provide additional measures to protect the privacy of Canadians. The Minister of National Defence accepted and CSEC is working to address the two recommendations on a new ministerial directive on sharing and on reporting details to the Minister regarding communications involving Canadians or information about Canadians that have been shared by its Second Party partners. My office and I will monitor developments.

I will continue to examine the controls in place and measures taken by CSEC to help ensure that its foreign signals intelligence information sharing with the Second Parties is lawful and protects the privacy of Canadians in the conduct of future reviews.

In addition, this review provided the Commissioner's office with background information on CSEC disclosures of Canadian identity information to second party partners. Starting this year, I included disclosures of Canadian identities to second party partners in an expanded annual review (see summary of the annual review of a sample of disclosures of Canadian identity information, pages 43–45).

I will also continue to include privacy incidents involving the second party partners in my annual review of the incidents identified by CSEC (see summary of the annual review of privacy incidents and procedural errors identified by CSEC in 2013 that affected and had the potential to affect the privacy of Canadians and measures taken by CSEC to address them, pages 45–47).

In the coming months, I will explore options to cooperate with review bodies of second party countries to examine information sharing activities among respective intelligence agencies and to verify the application of respective policies. A number of Canadian and international academics have referred to an accountability gap concerning an absence of international cooperation among review bodies. These researchers suggest that growing international intelligence cooperation should be matched by growing international cooperation between review bodies. I will examine opportunities for cooperation.

2. Review of the activities of the CSEC Office of Counter Terrorism

Background

This review was started by my predecessor and completed under my authority. The purpose of the review was to acquire detailed knowledge of CSEC's Office of Counter Terrorism (OCT) and to assess any changes to its activities since the last in-depth review was completed in 2007. I examined a sample of recent OCT activities to determine whether the activities complied with the law and the extent to which CSEC protected the privacy of Canadians.

Another specific objective was to follow up on matters raised in a review of certain foreign signals intelligence activities, summarized in Commissioner Décary's report of last year. The purpose of this aspect of the review was to determine whether developments in CSEC policies and procedures since the period previously under review have resulted in an improvement in the clarity of language in CSEC information exchanges with partners, and CSIS in particular.

The OCT was established in October 2001, in the aftermath of the events of September 11, to centralize CSEC foreign signals intelligence efforts relating to international terrorism threats. OCT operational activities involve acquiring and using information from the global information infrastructure for the purpose of providing foreign intelligence relating to terrorism, and providing technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties to investigate terrorism. The OCT collaborates closely with CSIS and the Royal Canadian Mounted Police and with CSEC's second party partners. The OCT may also support the government's response to critical incidents such as a Canadian being taken hostage abroad.

Findings and recommendations

OCT activities are subject to the same legal requirements to protect the privacy of Canadians that apply to all CSEC activities. CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its OCT activities at a Canadian wherever he or she may be or at any person in Canada. OCT employees demonstrated knowledge of policy and practices aimed at ensuring compliance with the law and privacy protection, and managers routinely monitored the activities for compliance.

I found that a sample of metadata activities involving information about Canadians conducted by the OCT was generally conducted in compliance with operational policy. I did, however, find that parts of CSEC policy related to this metadata activity did not reflect standard practices. **I recommended** that CSEC modify its policy for these

activities to reflect its current practices, specifically for record keeping. I will pursue examination of this issue as part of my ongoing review of CSEC foreign signals intelligence and IT security activities that may use metadata.

I also recommended that CSEC promulgate written guidance to formalize and strengthen existing practices for addressing potential privacy concerns with Second Party partners. Although CSEC cooperative arrangements include a commitment by the partners to respect the privacy of each other's citizens, it is recognized that each partner is an agency of a sovereign nation that may derogate from the arrangements, if it is judged necessary for their respective national interests.

Since the 2007 review of the OCT, CSEC has promulgated new guidance and introduced a new process for recording information exchanges between itself and federal law enforcement and security agencies. This procedural change is significant and will promote clarity of language in such information exchanges. As a result, I concluded that CSEC addressed the recommendation in my predecessor's review of certain foreign signals intelligence activities respecting clarity of language. The OCT materials reviewed raised no concerns such as those encountered in my predecessor's review reported last year; the information exchanges were clear and unambiguous.

Conclusion

While I made two recommendations to the Minister of National Defence to strengthen CSEC policy, I found that the OCT activities were conducted in compliance with the law and ministerial direction. The Minister of National Defence accepted and CSEC is working to address the two recommendations by promulgating new and updated operational policy guidance to address the issues identified in the recommendations. My office and I will monitor developments.

3. Study of CSEC policy compliance monitoring framework and related activities

Background

This study was started by my predecessor and completed under my authority. Policy compliance monitoring is a long-standing program internal to CSEC that assists it in ensuring and demonstrating that its foreign signals intelligence and IT security operational activities comply with the law, ministerial requirements and policy, including protecting the privacy of Canadians. Policy compliance monitoring may identify areas of possible concern, but also has an educational role within CSEC. This was the first comprehensive study of CSEC policy compliance monitoring activities since a 2009 audit by CSEC internal auditors resulted in CSEC changing a number of its related policy framework and activities. A central finding of the 2009 audit was that some supervisors in operational areas believed the direction in CSEC policy was not sufficiently clear.

Records of CSEC monitoring activities inform my reviews by demonstrating CSEC efforts to ensure compliance. Commissioners have emphasized the importance of a robust policy compliance monitoring framework and activities. For example, in his February 25, 2011, *Review of CSEC's Activities Under Foreign Intelligence Ministerial Authorizations*, Commissioner Décary recommended that "given the importance to helping to ensure compliance and the protection of privacy, CSEC should accelerate the timeline for implementation of an improved foreign signals intelligence Active Monitoring Program."

The objectives of the study were:

- to acquire detailed knowledge of and to document CSEC's new monitoring framework and how related activities contribute to CSEC compliance and privacy protection;
- to observe the level of awareness among foreign signals intelligence and IT security operational managers and employees of the policy framework and activities;

- to use the knowledge gleaned to inform my standard criteria and methodology used for reviews, namely how to assess whether CSEC has an effective management control system; and
- to identify any issues that may require follow-up.

Findings

Since the 2009 audit, CSEC has promulgated comprehensive policy and procedures that clearly define the roles and responsibilities for those involved in policy compliance monitoring. The new guidance contains detailed and specific requirements and activities for monitoring under seven themes: data handling; reporting; retention and disposition; collection management; information management; conditions of ministerial authorizations; and dissemination.

I found a rigorous approach to policy compliance monitoring based on document reviews, interviews with CSEC operational managers and employees, and with those employees in the foreign signals intelligence and IT security program areas that are dedicated and responsible for compliance and oversight of operational activities. The direction on monitoring is clear and comprehensive and is being followed. Monitoring activities are now part of CSEC's day-to-day activities. Both the foreign signals intelligence and IT security program areas have incorporated mandatory policy awareness and policy knowledge tests for employees into their compliance monitoring programs. In addition, requirements for policy compliance monitoring are being built into new or updated CSEC tools and systems.

One area that I identified for improvement is the establishment of consistent naming conventions for policy compliance monitoring records within CSEC's system of corporate records. This would help ensure the timely availability of these records to demonstrate CSEC efforts to ensure compliance with the law, ministerial requirements and policy.

Conclusion

Since the 2009 audit, CSEC foreign signals intelligence and IT security have taken significant measures to strengthen compliance by implementing a new framework for policy compliance monitoring and detailed operational instructions, training and testing, as well as a number of new related activities.

I will continue to assess and verify CSEC policy compliance monitoring activities in the conduct of reviews.

Why gather foreign signals intelligence?

CSEC collects foreign signals intelligence to help protect the security of Canada and of Canadians against, for example, foreign-based terrorism, foreign espionage, cyber attacks and kidnappings of Canadians abroad, as well as to support government decision making by providing a better understanding of global events. With the potential for invasion of the privacy of Canadians, are the risks involved in collecting foreign signals intelligence worth it? Parliamentarians thought so in 2001 when they passed amendments to the *National Defence Act* that provided a legislative basis for CSEC. But Parliamentarians also foresaw the danger of potential misuse of signals intelligence and explicitly required CSEC to target only foreign entities, not Canadians or individuals in Canada, and not Canadians abroad. Further, in drafting CSEC's governing legislation, Parliamentarians required CSEC to put in place measures to protect the privacy of Canadians, in particular, in the use and retention of intercepted information. Human error and overzealousness present other risks; Parliament chose to manage these risks by entrenching the office of the CSE Commissioner in the legislation to review CSEC activities to ensure that they are in compliance with the law, including the protection of the privacy of Canadians.

4. Review of CSEC 2012–2013 foreign signals intelligence ministerial authorizations

Background

The *National Defence Act* allows the Minister of National Defence to give CSEC written ministerial authorization to conduct activities that risk the unintentional interception of private communications while collecting foreign signals intelligence. The law specifies the conditions under which a ministerial authorization can be issued. Ministerial authorizations relate to an "activity or class of activities" specified in the authorizations. This term is interpreted by Justice Canada as meaning a specific method of acquiring foreign signals intelligence (the how). The authorizations do not relate to a specific individual or subject (the whom or the what). (More information on ministerial authorizations as well as on the authorities for and limitations on CSEC activities are available on the office's website and CSEC website.)

The law also directs the CSE Commissioner to review activities carried out under a ministerial authorization and to report annually to the Minister of National Defence on the review. An annual combined review of the foreign signals intelligence ministerial authorizations is one way that I fulfill this part of my mandate. This year, I examined the three foreign signals intelligence ministerial authorizations in effect from December 1, 2012, to November 30, 2013, relating to three activities or classes of activities.

The purpose of this review was to: ensure that the activities conducted under the ministerial authorizations were authorized; identify any significant changes — for the year under review, compared with previous years — to the authorization documents themselves and to CSEC activities or class of activities described in the authorizations; assess the impact, if any, of the changes on the risk to non-compliance and on the risk to privacy, and, as a result, identify any subjects requiring follow-up review; and examine private communications unintentionally intercepted by CSEC under these authorizations, for compliance with the law and the protection of the privacy of Canadians.

In past years as part of this annual review, Commissioners examined samples of unintentionally intercepted private communications. This year, I examined all of the 66 private communications unintentionally acquired by CSEC in the conduct of its foreign signals intelligence activities that CSEC used in reports or retained at the end of the 2012–2013 ministerial authorization period for use in future reporting. I examined all reports produced by CSEC in 2012–2013 containing information derived from private communications. For these 66 private communications, my employees tested the contents of CSEC systems and databases and listened to the intercepted voice recordings, read the written contents, or examined the associated transcripts of the communications. I also examined key metrics relating to interception, private communications and the privacy of Canadians.

Findings and recommendations

The 2012–2013 foreign signals intelligence ministerial authorizations were authorized, that is, they met the four conditions for authorization set out in the *National Defence Act*.

Conditions for authorization of foreign signals intelligence ministerial authorizations

The Minister of National Defence may only issue a [foreign signals intelligence] ministerial authorization […] if satisfied that

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

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

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

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

CSEC made significant changes to the format of its foreign signals intelligence ministerial authorizations in 2012–2013. As a result, collection that was formerly authorized under six ministerial authorizations in 2011–2012 was authorized under three ministerial authorizations in 2012–2013. I examined the changes to the documents, carefully comparing the contents to previous documents and evaluating CSEC's justification for the changes made to the documents. I had no questions about the changes. The new format resulted in documents that are more properly aligned with the purpose of the ministerial authorizations — that is, to shield CSEC from potential liability under Part VI of the *Criminal Code* in the event that CSEC unintentionally intercepts private communications as part of authorized foreign signals intelligence collection — and that are clear and comprehensive. It is important to note that reporting requirements to the Minister of National Defence did not change under the new ministerial authorizations.

I also examined changes to CSEC operational policies relating to the conduct of the activities under foreign signals intelligence ministerial authorizations. To ensure proper accountability for certain sensitive activities, **I recommended** that CSEC promulgate detailed guidance regarding the additional approvals required for these particular activities. I had no concerns about the other changes made by CSEC to its operational policies.

In 2012–2013, CSEC made some changes to the technology used for some of its foreign signals intelligence collection activities. I had no concerns about the changes and will examine any impact of the changes in subsequent in-depth reviews of the activities.

During the period under review, CSEC finalized and launched one tool (referred to in my predecessor's report of last year), and implemented another tool, both of which will assist CSEC analysts in correctly identifying and marking collected communications that might be private communications or contain information about Canadians. These markings are important because they determine how CSEC systems and

databases treat, retain or delete the communications. The new tools should reduce the potential for human error. It remains, however, the analysts' responsibility to validate the results of these automated tools.

While CSEC made a significant change to how it counts the "collected communications" that it reports to the Minister of National Defence, CSEC is also continuing to use the same method as in previous years to count and report recognized private communications. This ensures the ability to make year-over-year comparisons of the overall number of collected communications and the number of unintentionally intercepted private communications.

Recognized private communications

Overall, in 2012–2013, the volume of communications collected through CSEC's foreign signals intelligence activities increased. However, the number of recognized private communications unintentionally intercepted and retained by CSEC was small enough that I could review each of them individually. At the end of the 2012–2013 ministerial authorization period, CSEC retained 66 of the recognized private communications that it collected. Of these, 41 private communications were used in CSEC reports (with any Canadian identities suppressed in the reports) and 25 were retained by CSEC for future use. All other recognized private communications unintentionally intercepted by CSEC were destroyed.

I found that all CSEC reports based on private communications contained foreign intelligence relating to international affairs, defence or security.

However, during my review I found instances where procedures relating to the identification of private communications were not followed correctly by CSEC employees. In one instance, a private communication was recognized but, contrary to policy, that communication was incorrectly marked for retention even though it had not been assessed as essential to international affairs, defence or security. In another situation, CSEC identified several private communications, but did not mark them for retention or deletion until several weeks after they were identified.

In addition, there were other instances of analysts retaining foreign intelligence private communications — in some cases, for several months — that had been, but no longer were, essential to international affairs, defence or security. In these cases, CSEC reminders to delete these communications were not actioned in a timely manner. However, these private communications were ultimately deleted prior to the end of the ministerial authorization period, on which reporting to the Minister of National Defence is based.

As a result of these examples, I made three recommendations. First, **I recommended** that CSEC analysts immediately identify recognized private communications for essentiality to international affairs, defence or security, as required by the *National Defence Act*, or, if not essential, for deletion. Second, **I recommended** that CSEC analysts regularly assess, at a minimum quarterly, whether the ongoing retention of a recognized private communication not yet used in a report is strictly necessary and remains essential to international affairs, defence or security or whether that private communication should be deleted. Third, **I recommended** that CSEC make available to the Minister of National Defence more comprehensive information regarding the number of collected communications and intercepted private communications that it acquires and retains throughout the period that a ministerial authorization remains in effect.

As a result of another example in which an analyst retained for some time private communications pending further guidance, **I recommended** that CSEC promulgate policy on the specific circumstances and handling of a particular type of communication.

Finally, I found that CSEC made further progress in implementing a recommendation from the 2010–2011 annual review of foreign signals intelligence ministerial authorizations to report to the Minister of National Defence certain information relating to privacy. My office and I will continue to monitor developments.

Conclusion

I found that all private communications that were recognized by CSEC were intercepted unintentionally. There was no intention on CSEC's part in collecting these communications with a Canadian end; the Canadian end was in all cases incidental to CSEC's intentional targeting of a foreign entity outside Canada (the foreign end).

The Minister of National Defence accepted and CSEC is working to address the five recommendations I made to promote compliance, strengthen privacy protection and support the Minister in his accountability for CSEC. CSEC has committed to issuing guidance for the approval of certain sensitive activities. CSEC indicated it will include more information in its 2013–2014 ministerial authorizations annual report on the number of private communications retained throughout the reporting year. CSEC has committed to enforcing the roles and responsibilities of analysts as identified in existing operational policies and procedures respecting the identification of private communications. CSEC has also committed to ensuring that all analysts review their retained private communications quarterly to assess whether the communications remain essential and should be retained or whether the communications should be deleted. Finally, CSEC has committed to developing and promulgating policy guidance on the specific circumstances and handling of a particular type of communication. My office and I will monitor developments.

Information about Canadians: any personal information (as defined in the *Privacy Act*) about a Canadian, or business information about a Canadian corporation.

5. Annual review of a sample of disclosures by CSEC of Canadian identity information to Government of Canada clients and second party partners

Background

This is the fourth annual review of disclosures by CSEC of Canadian identity information from foreign signals intelligence reports to Government of Canada clients. For the first time, this review included a sample of disclosures to CSEC's second party partners, as well as disclosures through a Government of Canada client or second party partner to non-Five Eyes recipients. The review encompassed the period of July 1, 2012, to June 30, 2013.

The *National Defence Act* and the *Privacy Act* require CSEC to take measures to protect the privacy of Canadians, including personal information. Canadian identity information may be included in CSEC foreign signals intelligence reports if it is essential to understanding the intelligence. However, with some limited exceptions that are stated in CSEC policy, any information that identifies a Canadian must be suppressed in the reports — that is, replaced by a generic reference such as "a named Canadian." When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting Government of Canada client or second party partner has both the authority and operational justification for obtaining the Canadian identity information. Only then may CSEC provide that information.

Findings

My office selected and examined a sample of approximately 20 percent of disclosure requests received by CSEC from all clients and partners during the period under review, associated end-product reports, and any associated disclosures of Canadian identity information. Denial of disclosures to Government of Canada clients and international partners were also examined.

I found that CSEC's disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients and second party partners complied with the law and with ministerial direction concerning the protection of the privacy of Canadians. CSEC effectively applied satisfactory measures to protect personal information and the privacy of Canadians in its disclosures.

Investigation by my office identified two privacy incidents pertaining to two Canadians mentioned in four reports. It appears that a second party partner unintentionally included Canadian identity information in the reports, that is, Canadian identity information was not initially suppressed in those reports as required by CSEC and second party policies. This is not to suggest that there was any deliberate non-compliance on the part of CSEC or of any of its partners; at that time, it was unknown that the individuals were Canadians. CSEC recorded the incidents in its Privacy Incidents File. I will be examining CSEC's responses to these incidents.

My office also identified and discussed with CSEC a number of minor instances where records of the disclosures were not in accordance with best practices. I will monitor these issues as part of future annual reviews of disclosures.

CSEC has comprehensive policies and procedures that guide its disclosure of Canadian identity information from foreign signals intelligence reports to Government of Canada clients. It is a positive development that CSEC is amending its policy guidance to provide further direction regarding disclosures to second party partners.

CSEC employees interviewed were fully knowledgeable about and complied with the policies and procedures, and CSEC managers routinely and closely monitored disclosures to ensure compliance and privacy protection.

It is a positive development that CSEC continues to give priority to the completion of the full automation of its information and records management processes for the disclosure of Canadian identity information from foreign signals intelligence reports.

Conclusion

My review did not result in any recommendations. CSEC conducted its activities in a thorough manner; all of the requests reviewed were authorized and justified.

Should there be an instance of non-compliance in CSEC disclosure of Canadian identity information, the potential impact on the privacy of Canadians could be significant. It is for this reason that I intend to continue to conduct an annual review of disclosures.

6. Annual review of incidents and procedural errors identified by CSEC in 2013 that affected or had the potential to affect the privacy of Canadians and measures taken by CSEC to address them

Background

CSEC requires its foreign signals intelligence and IT security employees to report and document privacy incidents in order to demonstrate compliance with legal and ministerial requirements and CSEC policies, and to prevent further incidents. Incidents are documented in one of two files, depending on the severity. The Privacy Incidents File (PIF) is a record of CSEC incidents where privacy was breached. The Minor Procedural Errors Report (MPER) contains operational errors that occurred in connection with information relating to Canadians but that did not result in that information leaving the control of CSEC, or in that information being exposed to external recipients who ought not to have received it. The PIF and MPER are voluntary CSEC initiatives to record what CSEC defines as privacy incidents.

Every review I conduct of CSEC activities generally includes an examination of any privacy incident relating to the subject of the review. The annual review of the entire PIF and MPER focuses on incidents not examined in detail in the course of my other reviews. This is done to assure myself that CSEC took appropriate corrective actions for all privacy incidents it identified.

The objectives of this review were: to acquire knowledge of the incidents, procedural errors and subsequent CSEC actions to correct the incidents or mitigate the consequences; to inform development of my work plan by determining what privacy incidents, procedural errors and related activities, if any, may raise issues about compliance or the protection of the privacy of Canadians, and therefore should be subject to follow-up review; and to assist me in evaluating CSEC's policy compliance monitoring framework and related activities.

Findings and recommendation

Based on my review of CSEC records, CSEC answers during interviews and in response to written questions, as well as independent verification by my office of reports in a CSEC database, I am satisfied that CSEC took appropriate corrective actions in response to the procedural errors and privacy incidents it identified and recorded during 2013.

I found that the procedural errors were minor and none involved a breach of privacy.

Where privacy was breached, CSEC did not discover any adverse impact on the Canadian subjects.

CSEC has implemented or is working on certain remedial actions to prevent future privacy incidents similar to those identified. For example, CSEC created new guidance and is clarifying other policy to help prevent the unintentional naming of Canadians in CSEC reports. I will monitor the impact of the changes in future reviews.

One privacy incident resulted from the sharing of information between CSEC and CSIS. In his 2012–2013 review of certain foreign signals intelligence activities, my predecessor made a recommendation respecting clarity of language for when CSEC is sharing information with its Government of Canada partners. In my *Review of the Activities of the CSEC Office of Counter Terrorism* of this year, I discuss the implementation of a process introduced by CSEC that has helped prevent the use of imprecise and inconsistent language in CSEC exchanges of information with its Government of Canada partners. I accept CSEC's explanation of why a technical issue at the time of the privacy incident resulted in this particular exchange being made outside of the new process. My office and I will continue to monitor CSEC information exchanges with partners to ensure proper processes are followed and that there is clarity of language to avoid any ambiguous situations that might raise questions about compliance.

I also found that CSEC generally takes appropriate measures to protect the privacy of Canadians when a privacy incident arises from activities of a Second Party. However, because of the enhanced potential of the violation of the privacy of a Canadian when a privacy incident involves a Second Party, **I recommended** that CSEC request that its second party partners confirm that CSEC requests to address any privacy incidents relating to a Canadian have been actioned by the partners, and that CSEC record the responses in the PIF.

Conclusion

My review did not reveal any systemic deficiencies or issues that require follow-up review.

I intend to continue to conduct an annual review of CSEC's PIF and MPER.

The Minister of National Defence accepted the recommendation. My office and I will monitor developments with regard to the findings and recommendation I have made in this review.

COMPLAINTS ABOUT CSEC ACTIVITIES

Anyone, including an employee of CSEC, can write to me to complain about CSEC activities, for example, to express concerns that CSEC is engaging in unlawful activity or is not taking sufficient measures to protect the privacy of Canadians. In 2013–2014, I was contacted by a growing number of individuals who were seeking information or expressing concern about CSEC activities. My office or I replied to many of the inquiries. Other inquiries were assessed as outside of the Commissioner's mandate or as lacking credibility. No complaints about CSEC activities warranted investigation. (More information on the complaints process is available on the office's website.)

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 — such as certain information relating to CSEC activities — on the grounds that it is in the public interest. No such matters were reported to me in 2013–2014. (More information on the Commissioner's responsibilities under the *Security of Information Act* is available on the office's website.)

ACTIVITIES OF THE COMMISSIONER'S OFFICE

At the beginning of my term as Commissioner, my office provided me a series of briefings to introduce the overall operations and activities that are conducted under the Commissioner's authority. CSEC subsequently provided me with numerous detailed information sessions on legal, operational, technical and administrative issues respecting its activities. I want to thank Chief Forster and his team for these important briefings, during which I also had the opportunity to meet many CSEC senior managers and personnel.

During the past year, CSEC also provided a number of detailed briefings to employees of my office as part of the conduct of reviews. As well, CSEC provided an annual overview briefing on recent and important operational, policy and organizational changes and issues. Several of my employees sat in as observers on CSEC training courses on foreign signals intelligence and on IT security activities.

Transparency and communications

During the past year, following disclosures of classified documents by former U.S. NSA contractor Edward Snowden, my office and I responded to a dramatic increase in the number of requests by the media and academics for information about my role and activities. In the past, it was difficult for the Commissioner and the office to gain the attention of more than a handful of journalists and academics with specialized interests. General public awareness was minimal. Times have changed. Now, aside from the increase in requests for information, my office and I have been receiving more requests for participation in various conferences and meetings.

In November 2013, as part of the Canadian Association of Security and Intelligence Studies symposium in Ottawa, the Executive Director of my office participated in a panel discussion on "Intelligence Collection and Accountability: Getting the Balance Right." Also participating in the panel were a senator and a number of academics with expertise in national security law and privacy. The Executive Director explained the Commissioner's mandate, powers and activities, as well as the impact of review, and corrected certain misconceptions, for example, related to the Commissioner's independence and capacity, and to CSEC authorities, judicial warrants and ministerial authorizations.

As a result of the various issues raised publicly during this past year, and questions about the Commissioner's role and office, we added information to the office website in a question-and-answer format. The purpose was to clarify the issues, to dispel some misconceptions and to correct inaccuracies.

In December 2013, the Executive Director and I appeared before the Senate Committee on National Security and Defence. I welcomed this opportunity so early in my mandate to discuss the *raison d'être* of my position as Commissioner and to provide the committee with concrete examples of the impact of my work as an independent entity within the Canadian security and intelligence community. I would welcome additional invitations from the Senate or from a House of Commons committee to discuss my role, activities and any issues of concern.

In February 2014, the Executive Director participated in the 15th Annual Privacy & Security Conference, "Harnessing the Power of the Digital Storm: Can We Have It All?," in Victoria, British Columbia. In a panel session entitled "Privacy and Security: A False Dichotomy?" that also included the SIRC Executive Director and a law professor from the University of Alberta, the Executive Director addressed questions about the Commissioner's mandate and topics of current media attention. (A copy of the Executive Director's opening remarks can be found on the office's website.)

Also in February, the Executive Director joined a lawyer from the British Columbia Civil Liberties Association and a University of Ottawa law professor specializing in national security in a debate organized by *The Globe and Mail* and published both in print and on-line. The session, "Privacy or national security: Have spy agencies gone too far?," included discussion of metadata, the role of the Commissioner and the impact of review.

To contribute further to informing the public, detailed information on our activities was added to the office's website, as noted, to clarify misconceptions and to address issues raised about the role and work of the Commissioner. The website is still being enhanced, with more detail to come about how my office and I review the operational activities of CSEC. My aim is to help reassure the public that I, as Commissioner, have full access to CSEC, its personnel, facilities and systems, and that the review process and my investigations are probing, rigorous and as detailed as necessary to allow me to determine whether CSEC has complied with the law and has adequately protected the privacy of Canadians.

Finally, this past year, my office made a total of seven presentations to new CSEC employees attending a course that is mandatory for them to take in order to work at CSEC. The presentations consist of an overview of my office, the type of work we do and what to expect if the activity or area they are involved in is subject to review by my office.

Review bodies working cooperatively

In December 2013, the Review Agencies Forum, which consists of employees of the Commission for Public Complaints Against the RCMP, SIRC, the Office of the Privacy Commissioner and my office, met to discuss issues of common interest and compare best practices in review methodology. A senior manager from the Privy Council Office provided a brief on national security issues. Officials also discussed cooperation among review bodies.

My office also organized a one-day training workshop, held in November, for new employees of the review bodies, in order to enhance the effectiveness of independent review.

This year, my office and I will continue to work with Review Agencies Forum partners to explore opportunities for the conduct of coordinated or joint reviews under existing legislation.

During the past year, my predecessor, and then myself, met with the former Privacy Commissioner of Canada and I met with the Interim Privacy Commissioner to discuss issues of mutual concern. The Office of the Privacy Commissioner oversees the entire public service as well as federally regulated businesses for compliance with, respectively, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. My position as CSE Commissioner was created specifically to review CSEC for compliance, including for the protection of the privacy of Canadians. The Privacy Commissioner and I will continue to cooperate on shared priorities.

WORK PLAN — REVIEWS UNDER WAY AND PLANNED

Commissioners use a risk-based and preventative approach to reviews. A three-year work plan is updated twice a year. Developing the work plan draws on many sources. An important one consists of regular briefings from CSEC on new activities and changes to existing activities. Another is the classified annual report to the Minister of National Defence from the Chief of CSEC on CSEC's priorities and its legal, policy and management issues of significance.

The results of several reviews currently under way are expected to be reported to the Minister of National Defence in the coming year and included in my 2014–2015 annual report. The subjects of these reviews include: another focused review on metadata; a review of particular foreign signals intelligence activities conducted under ministerial authorizations; a review of CSEC IT security activities conducted under ministerial authorizations in support of Government of Canada efforts to address cyber threats; a follow-up review of certain CSEC activities with the Canadian Armed Forces; and a review of CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 16 and 21 of the *CSIS Act*.

Some of the reviews planned for 2014–2015, which may carry over to the next year, are: a review of particular foreign signals intelligence activities conducted under ministerial authorizations; and foreign signals intelligence and IT security activities conducted using exceptional procedures.

In addition, I plan to continue the annual reviews of: (1) foreign signals intelligence ministerial authorizations; (2) CSEC disclosures of Canadian identity information; and (3) privacy incidents and procedural errors identified by CSEC and the measures subsequently taken by CSEC to address them.

IN CLOSING

Six months after my appointment, as I write this first public annual report — the 18th report by a Commissioner — I am continuing to learn about and to question the activities of CSEC. I appreciate the support and professionalism of my office team.

I have read and heard questions raised about the independence of the Commissioner. There is no question that the scope of the powers that I have is sufficient to fully investigate CSEC. Also, the size of my budget and office are sufficient to conduct an adequate amount of meaningful review. As I continue to learn, however, I will also continue to assess whether I have adequate resources.

Alongside fulfilling my mandate, transparency will remain a priority focus for the coming year. While my mandate is to review CSEC activities to determine compliance with law — that is, making sure CSEC is doing things right — I am prepared to contribute to any public policy debate before Parliament as to whether CSEC is doing the right things, particularly relating to the protection of the privacy of Canadians. I am also following with interest the ongoing civil claim in the Supreme Court of British Columbia about whether CSEC activities infringe individuals' *Charter* rights.

Like my predecessors, I remain confident that Chief Forster and CSEC take very seriously their responsibilities to comply with the law and protect the privacy of Canadians. It is my job to investigate and verify that CSEC continues to do so and I take my job equally seriously. I encourage the strengthening of a culture of compliance within CSEC, which is the best assurance for employees doing the right thing and against breaches of privacy.

One last issue gives me cause for concern because of the time that has elapsed from when it was first identified. Since the enactment of Part V.1 of the *National Defence Act* in December 2001, all CSE Commissioners have voiced concerns that certain fundamental provisions in the legislation lack clarity. In 2007, the government committed to amending the legislation to clarify these ambiguities. It is hoped that this can be resolved in the near future.

ANNEX A: EXCERPTS FROM THE *NATIONAL DEFENCE ACT* AND THE *SECURITY OF INFORMATION ACT* RELATED TO THE COMMISSIONER'S MANDATE

National Defence Act — Part V.1

Appointment of Commissioner

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.

Duties

(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.

Annual report

(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.

Powers of investigation

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

Employment of legal counsel, advisers, etc.

(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.

Directions

(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.

[...]

Review of authorizations

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.

Public interest defence

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.

[...]

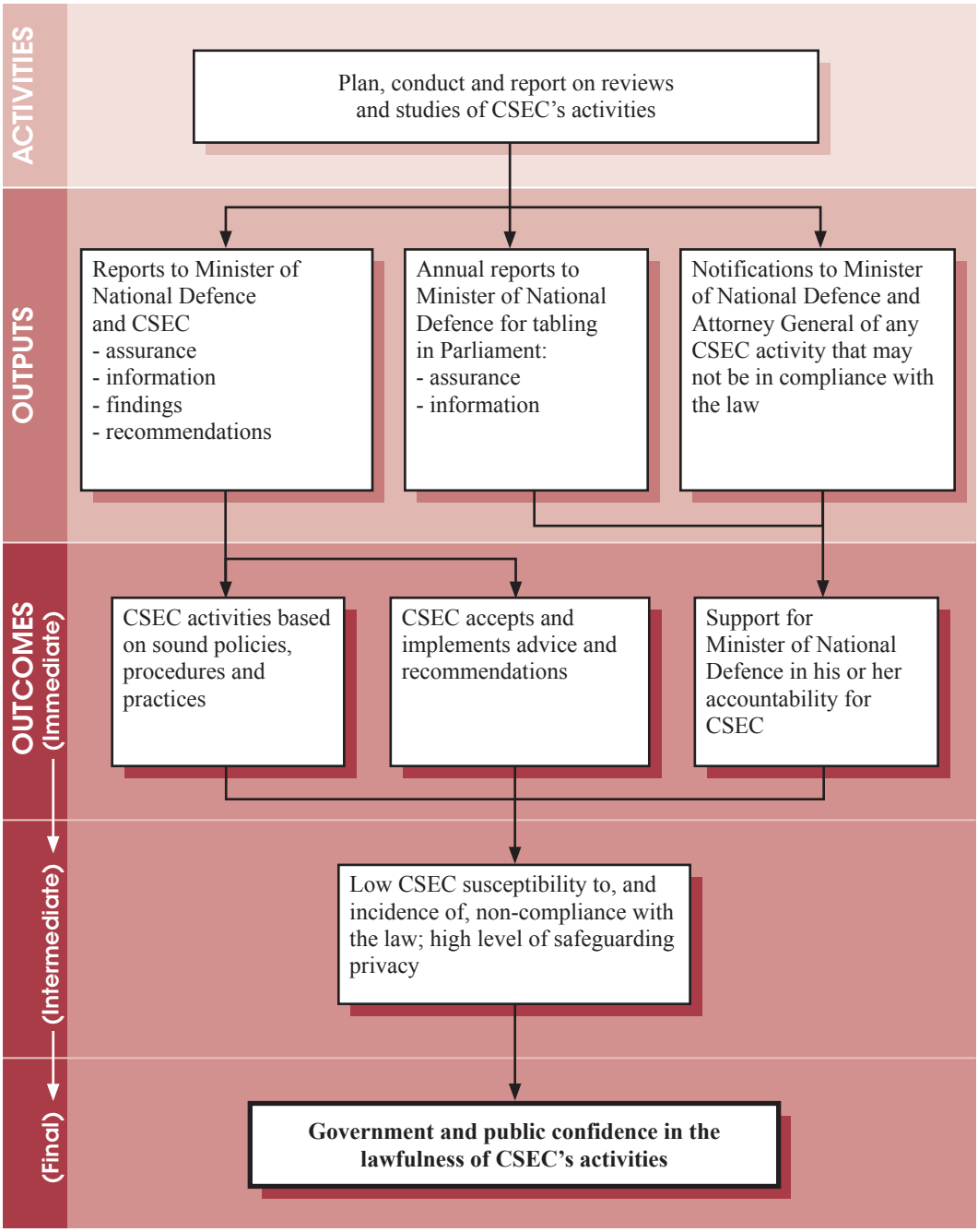
Prior disclosure to authorities necessary

(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: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL



ANNEX C: 2013–2014 STATEMENT OF EXPENDITURES

Standard Object Summary ($)

Salaries and Benefits	1,158,827
Transportation and Telecommunications	16,331
Information	13,040
Professional and Special Services	351,481
Rentals	328,892
Repairs and Maintenance	2,638
Material and Supplies	16,509
Machinery and Equipment	10,491
Capital Assets, Including Leasehold Improvements	44,911
Total	**1,943,120**