COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

ANNUAL REPORT 2014-2015

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1474, Station “B”
Ottawa ON K1P 5P6

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

Catalogue No. D95E-PDF
ISSN 1700-0874

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 2015

Minister of National Defence
MGen G.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, 2014, to March 31, 2015, for your submission to Parliament.

Yours sincerely,

Jean-Pierre Plouffe

P.O. Box/C.P. 1474, Station "B"/Succursale « B »
Ottawa ON Canada K1P 5P6
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

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

The last year has been marked by vigorous debate about the activities of the Communications Security Establishment (CSE) and of my office in reviewing those activities. Fuelled by continuing unauthorized disclosures of documents from Edward Snowden and legislative proposals in reaction to the murder of two Canadian soldiers on Canadian soil, an important part of the discussion has been the question of control over intelligence and security agencies. Canadians deserve reassurance that the activities of these agencies — including any additional authorities they may be granted — do not unreasonably infringe on the privacy of Canadians. At the core of this debate is my mandate, as well as the mandates of my review colleagues at the Security Intelligence Review Committee and at the Civilian Review and Complaints Commission for the RCMP.

In this charged environment, I need to maintain perspective. In my role as CSE Commissioner, I draw on my many years as a judge to examine facts dispassionately, to ask questions objectively and to view through the lens of the law instead of emotion. But I remain keenly aware that the work of CSE sparks powerful reactions when Canadians feel that their privacy could be violated and when the necessary shroud of secrecy distorts their perception of what CSE does — and therefore also of what my office does.

I continue to be concerned about public discussion that draws conclusions or forms opinions based on partial information. Without full context, which cannot be revealed to those outside the "security fence," partial information can be misleading and misinterpreted. The nature of its mandate compels CSE to operate largely in secret. But my office has full access to CSE, granted by the *Inquiries Act*, which allows me and my staff to look deep inside the organization to know and understand what is going on. The role of my office is to represent the public interest in CSE's accountability, but in a way that does not compromise the important work that CSE does, under legislation, to protect Canada's national interests, and that Canadians expect it to do. This is what legislators intended.

Parliamentarians could not, however, have been able to predict how technology was going to reshape society. The Internet and communications technologies have blurred international borders and shifted social boundaries. This context and the current threat environment require cooperation among Canada's intelligence and security agencies. Indeed, many of the reviews my office conducted this year reflect the theme of cooperation, whether between CSE and the Canadian Security Intelligence Service or other government institutions, whether among CSE and its counterparts in Australia, New Zealand, the United Kingdom and the United States, or whether among intelligence review bodies.

With the government and Canadians searching for the best way for intelligence and security agencies to work together, while at the same time ensuring adequate controls and adequate protection of the privacy of Canadians, some commentators take issue with the increased authorities proposed in Bill C-51, the *Anti-terrorism Act, 2015*. As for the potential effect of this legislation on CSE, we cannot know at this time precisely how its measures will affect the work of CSE.

There is a need to ensure that operational requirements do not eclipse the privacy protection of Canadians, and this can be counter-balanced by strengthening review. As I wrote to the House of Commons committee examining Bill C-51 in March 2015, existing legislative mandates provide for a limited amount of cooperation among the review bodies. However, an explicit authority for the review bodies to cooperate and share operational information would strengthen review capacity and effectiveness, which is that much more critical in the context of increasing cooperation and sharing of information among and with intelligence and security agencies.

The issue of cooperation among review bodies is a long-standing one. In fact, in his 2006 Arar inquiry report, Justice Dennis O'Connor recommended that statutory gateways be enacted to achieve four goals: "exchange of information, referral of investigations, joint investigations and coordination in the preparations of reports." My predecessor and I have already engaged in the first of these goals, with our referrals of information to the Security Intelligence Review Committee, and have begun to act on the last one — all under existing authorities.

Throughout the past year, CSE has dealt with my office in a forthright manner. Its transparency with me is a testament to the seriousness and confidence with which CSE approaches its legislated mandate.

Transparency continues to be an important element of my approach, which is important to maintain public trust. Part of my role is to inform Parliament and Canadians about CSE's activities, and I believe it is important to support my findings with as much explanation as possible, within the restrictions of the *Security of Information Act*. As an independent and external body, my office can challenge, and has challenged, CSE to justify why certain information needs to be considered classified. Indeed, last year I included statistics related to unintentionally intercepted private communications collected through CSE's foreign signals intelligence activities; this year's report contains more statistics. I see these as important steps in helping to demystify the work of CSE and contributing to better-informed public discussion.

I would like to express my appreciation to John Forster, whose leadership of CSE ended in January 2015. Mr. Forster was open and candid with me when there were potentially contentious issues to be discussed. As I welcome the new Chief of CSE, Greta Bossenmaier, I look forward to continuing a frank and professional relationship with her. And I will continue to demonstrate that spirit of openness in my reporting to Canadians on CSE activities.

Finally, in one of my reviews this year I point to a section of Part V.1 of the *National Defence Act* that needs to be amended. This adds to the calls by all my predecessors to amend Part V.1 to eliminate ambiguities. One must remember that Part V.1 of the *National Defence Act* was drafted and enacted quickly in 2001, following the events of September 11. Given the circumstances and the clear threat to security that existed at the time, Parliament had no choice but to act quickly. Amendments would clarify the law and are not, in my considered opinion, controversial. I am disappointed in the missed opportunities to address this significant issue.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

My mandate under the *National Defence Act* is:

1. to review activities of CSE to determine whether they comply with the law;

2. to undertake any investigation I deem necessary in response to a written complaint (more information is available on the office's website); and

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

Under the *Security of Information Act*, I also have a mandate 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 CSE. (More information is available on the office's website.)

CSE's mandate

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

- part (*a*) authorizes CSE to acquire and use foreign signals intelligence in accordance with the Government of Canada's intelligence priorities;
- part (*b*) authorizes CSE to help protect electronic information and information infrastructures of importance to the Government of Canada; and
- part (*c*) authorizes CSE 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.

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

To carry out my mandate, the *National Defence Act* provides me:

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

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

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. 61).

Our approach

The purpose of my review mandate is:

- to determine whether CSE 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 CSE 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 CSE 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 CSE undertakes.

Protection of Canadians' privacy

By law, CSE is prohibited 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 CSE activities includes determining whether CSE, in its use and retention of collected information, takes satisfactory measures to protect every Canadian's reasonable expectation of privacy. I examine CSE 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 foreign signals intelligence or IT security information. I also verify that metadata is used only to understand the global information infrastructure, to obtain foreign intelligence or to protect cyber systems, but *not* to obtain information about a Canadian.

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 determine how they are applied by CSE employees and to identify existing or potential systemic weaknesses.

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

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

Legal requirements: I expect CSE 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.

Ministerial requirements: I expect CSE 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 CSE 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 CSE employees to be knowledgeable about and comply with policies and procedures. I also expect CSE to have an effective compliance validation framework 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 findings

The results of individual reviews are the subject of classified reports to the Minister of National Defence. My classified review reports document CSE 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 CSE activities and my expectations, based on standard criteria.

The reports are free of any interference by CSE or any Minister. I determine the content of my reports, which are based on facts and conclusions drawn from those facts. Following the standard audit practice of disclosure, I present draft versions of review reports to CSE 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. CSE reviews the draft to verify that it does not contain any classified information that may contravene 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.

As a further step toward openness 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) — 90 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. 65).

COMMISSIONER'S OFFICE

In 2014–2015, 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 $2,043,560, which is within the overall funding approved by Parliament.

Annex C provides the 2014–2015 Statement of Expenditures for the Office of the CSE Commissioner (p. 67).

UPDATE ON CSE EFFORTS TO ADDRESS PREVIOUS RECOMMENDATIONS

Since 1997, my predecessors and I have submitted 90 classified review reports to the Minister of National Defence who is responsible for CSE. In total, the reports contained 156 recommendations. CSE has accepted and implemented or is working to address 93 percent (145) of these recommendations, including all eight recommendations this year.

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

Last year I reported on former Commissioner Décary's review of CSE foreign signals intelligence information sharing with international partners. I explained that the ministerial authorization regime is a Canadian instrument and applies to CSE; 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. As a result, CSE does not report to the Minister of National Defence details, for example, regarding communications involving Canadians or information about Canadians that Second Party partners have shared with CSE. Therefore, to support the Minister of National Defence in his accountability for CSE and as an additional measure to protect the privacy of Canadians, Commissioner Décary recommended that CSE report such details to the Minister on an annual basis. CSE has advised my office that the Chief of CSE's 2013–2014 Annual Report to the Minister of National Defence included statistics on communications CSE acquires from its Second Party partners.

CSE's Five Eyes partners

The Five Eyes partners are CSE and its main international partner agencies in the Five Eyes countries: the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Signals Directorate and New Zealand's Government Communications Security Bureau. They are also known to each other as Second Party partners.

In my review of the activities of the CSE Office of Counter Terrorism last year, I found that a sample of metadata activities involving information about Canadians was generally conducted in compliance with operational policy. I did, however, find that parts of CSE policy related to this metadata activity did not reflect standard practices. I recommended that CSE modify its policy for these activities to reflect its current practices, specifically for record-keeping. I pursued my examination of this issue as part of my review of CSE foreign signals intelligence metadata activities and found that CSE has halted some metadata analysis activities that were the subject of the recommendation and is consequently updating its policy framework.

CSE also took action on three of the five recommendations from my review of CSE's 2012–2013 foreign signals intelligence ministerial authorizations. CSE informed my office that it has improved policy in order to respond to my recommendation that CSE promulgate detailed guidance regarding additional approvals required for certain sensitive activities. The other two recommendations CSE implemented related to private communications. First, I had recommended that CSE 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 had recommended that CSE 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. In order to address these

recommendations, CSE has developed policy as well as an automated notification system where analysts receive notification when a private communication that has been marked for retention has not been used within a specific timeframe. The notification service allows the analysts to review the need to retain the private communications or otherwise they are automatically deleted.

Finally, in my annual review of privacy incidents and procedural errors identified by CSE in 2013 that affected or had the potential to affect the privacy of Canadians, I recommended that CSE request that its Second Party partners confirm that they have acted on CSE requests to address any privacy incidents relating to a Canadian, and that CSE record the responses in its privacy incident file. CSE accepted this recommendation and is working on updating its procedures to respond to my recommendation.

In addition, my office and I are monitoring 15 active recommendations that CSE is working to address — seven outstanding recommendations from previous years and eight from this year.

OVERVIEW OF 2014–2015 FINDINGS AND RECOMMENDATIONS

During the 2014–2015 reporting year, I submitted nine classified reports to the Minister of National Defence on my review of CSE activities. Three reports — one on foreign signals intelligence ministerial authorizations and two spot checks of intercepted, used and retained private communications under those authorizations — are combined into one since the private communications reviewed in the spot checks are those intercepted under the ministerial authorizations.

The reviews last year were conducted under my mandate:

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

The first review examined metadata activities related to CSE's foreign signals intelligence activities. This review was the first in an ongoing comprehensive review of CSE's metadata activities.

One review examined CSE assistance to the Canadian Security Intelligence Service (CSIS) related to section 16 of the *CSIS Act*. Two other reviews looked at specific activities: CSE's IT security activities to protect Government of Canada computer systems and networks; and CSE's relationship with the Canadian Forces Information Operations Group Cyber Support Detachments.

As in previous years, my office conducted its annual review of ministerial authorizations for foreign signals intelligence. However, because the ministerial authorizations gave CSE the authority to unintentionally intercept a foreign communication with a Canadian end, making it a "private communication" as defined in the *Criminal Code*,

this is an activity that needs continual scrutiny to ensure lawfulness and protection of privacy. Therefore, as a follow-up, to ensure that recommendations made last year were being implemented, my office also conducted spot checks this year on the private communications intercepted, used, retained, and destroyed, by CSE.

The remaining two reviews are also ones that I conduct every year because they concern areas that pose high risks to privacy: CSE disclosures of Canadian identity information and CSE incidents and procedural errors related to privacy.

The results

Each year, I provide an overall statement on my findings about the lawfulness of CSE activities. With the exception of one review related to metadata for which I am still examining the legal implications, all of the activities of CSE reviewed this past year complied with the law.

As well, this year, I made eight recommendations to promote compliance with the law and strengthen privacy protection, as well as to clarify the *National Defence Act*. The recommendations relate to reinforcing ministerial and policy guidance, as well as clarifying CSE's relationships with other organizations, including Second Party partners.

Five recommendations related to processes. The first recommendation stated that CSE use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization of metadata. Two recommendations related to updating governing documentation for processes related to section 16 of the *CSIS Act*. One recommendation was to update or create memoranda of understanding between CSIS and CSE, related to CSE's assistance to CSIS under part (c) of its mandate. The fifth process-related recommendation was for the attachment of caveats to certain material shared with CSE partners to ensure the material would not be used without the express authorization of CSE.

Two recommendations involved updating and clarifying certain

instruments. The first recommendation was to update the ministerial directive for metadata activities, last revised in 2011, to address the evolution of practices in this field as well as to clarify terminology that has changed over time. The second recommendation calls for an amendment of the *National Defence Act* to remove an ambiguity regarding CSE information technology (IT) security activities carried out under ministerial authorization.

The final recommendation relates to reporting to the Minister on private communications unintentionally intercepted by CSE in conducting its cyber defence activities. Such reporting should highlight important differences between private communications intercepted under the IT security ministerial authorization versus those intercepted under foreign signals intelligence ministerial authorizations. Under the IT security ministerial authorization, CSE intercepts many one-end-in-Canada e-mails containing malicious code, which have a lower expectation of privacy attached to them.

HIGHLIGHTS OF REVIEWS AND REPORTS SUBMITTED TO THE MINISTER IN 2014–2015

1. Review of CSE foreign signals intelligence metadata activities

Background

The collection and use of metadata has, over the past two years, been the focal point for public discussion about CSE, its activities and my review of those activities.

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

Planning for this comprehensive review of metadata was under way prior to the unauthorized disclosures by Edward Snowden in June 2013. Those disclosures heightened public interest in metadata-related issues, further confirming the value of our decision to undertake a broad review of CSE's collection, use and sharing of metadata, particularly in a foreign signals intelligence context. This review provided an opportunity to examine CSE's metadata activities on a broad scale, to assess changes to the activities, and to determine whether they comply with the law and whether, in conducting them, CSE protects the privacy of Canadians.

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.

Paragraphs 273.64(1)(*a*) and (*b*) of the *National Defence Act* authorize CSE to collect, use, share and retain metadata. CSE is allowed to use metadata only to understand the global information infrastructure, to provide intelligence on foreign entities located outside Canada, or to protect computer networks and systems of importance to the Government of Canada. A ministerial directive provides additional guidance and places limits on CSE metadata activities.

As with any of its activities, CSE is prohibited from directing its metadata activities at a Canadian or at any person in Canada. However, some metadata collected by CSE contains information about Canadians and CSE must take measures to protect privacy in the use of that metadata. The Minister of National Defence has provided direction to the Chief of CSE on metadata activities, including on the protection of the privacy of Canadians, through the 2011 ministerial directive entitled *Communications Security Establishment Collection and Use of Metadata*.

The ministerial directive defines metadata, describes the metadata activities that CSE can undertake under paragraph 273.64(1)(*a*) of the *National Defence Act*, and establishes privacy protections that CSE must apply when undertaking metadata activities. The directive serves to constrain CSE's activities, and does not provide authority for activities that CSE is unable to undertake under the *National Defence Act*. Through various internal policies, the Chief of CSE has further elaborated and provided guidance to CSE employees regarding the procedures and practices that must be followed for activities that use metadata.

This first report from my comprehensive metadata review, which I provided to the Minister of National Defence, focused on CSE's use of metadata in a foreign signals intelligence context. A second report will examine issues identified in *A Review of the activities of the CSEC Office of Counter Terrorism* from the 2013–2014 reporting year, and will also examine certain activities that involve metadata analysis, and certain other activities that involve information about Canadians. A third report, expected in the coming year, will focus on CSE's use of metadata in an information technology (IT) security context.

Findings and recommendations

During this review, CSE was forthcoming with information and assistance, both proactively and in response to specific requests by my office. The high profile of metadata activities by intelligence agencies in the wake of the unauthorized Snowden disclosures placed unique demands on both CSE and on my office throughout this review. CSE recognized the importance of responding to requests from my office in a timely manner. In addition, CSE proactively informed my office of incidents that it discovered during the review, which led to further in-depth investigation, and are described below.

I found that metadata collection and analysis have evolved considerably since the last in-depth review of metadata activities, and that metadata remains critical to all aspects of CSE's foreign signals intelligence mission. CSE 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 the collection and analysis of metadata by CSE continue to evolve, it will be important for my office to ensure it understands changes to CSE's processes and their potential corresponding impact on the privacy of Canadians and compliance with the law.

The Canadian legal landscape has also changed since my office last conducted an in-depth review of CSE's collection and use of metadata. Two recent decisions of the Supreme Court of Canada are particularly notable in this regard: decisions in *Wakeling* and *Spencer*. In *Wakeling* v. *United States of America*, 2014 SCC 72, the main issue raised was whether federal legislation authorizing the sharing of lawfully obtained wiretap information between Canadian and foreign law enforcement agencies is constitutional. The Court concluded that a disclosure will be reasonable under section 8 of the *Canadian Charter of Rights and Freedoms* if it passes a three-part test: that the disclosure is authorized by law, that the law authorizing the disclosure is reasonable, and that the disclosure is carried out in a reasonable manner. In *R.* v. *Spencer*, 2014 SCC 43, the Supreme Court

ruled on a person's reasonable expectation of privacy within the context of the use of the Internet. The Court found that, depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against section 8 of the *Charter*.

My office will continue to monitor how CSE responds to technological developments and their privacy implications, as well as developments in the legal landscape that could impact its collection, use and disclosure of metadata.

I found that the metadata ministerial directive lacks clarity regarding the sharing of certain types of metadata with Five Eyes partners, as well as other aspects of CSE's metadata activities. The 2011 directive updates the original directive of the same name, which was issued in 2005. While it includes several linguistic changes that improve on the 2005 document, the 2011 directive nevertheless lacks clarity regarding key aspects of CSE's collection, use and disclosure of metadata in a foreign signals intelligence context. For example, it does not define certain key terms, and fails to differentiate between other terms that, while similar in definition, are implicitly distinct concepts.

The ministerial directive lacks specificity regarding the application of privacy provisions to certain processes. Furthermore, the directive does not provide clear guidance regarding a specific metadata activity that is routinely undertaken by CSE in the context of its foreign signals intelligence mission. It is also unclear whether certain language in the directive is still applicable to CSE's use of metadata in a foreign signals intelligence context. For these reasons, **I recommended** that CSE seek an updated ministerial directive that provides clear guidance related to the collection, use and disclosure of metadata in a foreign signals intelligence context.

In January 2014, while in the early stages of this review, the Canadian Broadcasting Corporation (CBC) ran a news story relating to a classified CSE slide presentation to Five Eyes partners entitled

IP Profiling Analytics and Mission Impacts. The presentation, one of several unauthorized disclosures emanating from material taken from the National Security Agency systems by Edward Snowden, was originally created in May 2012. I released a public statement indicating that I was aware of the activities referred to in the story (it was also discussed in last year's public annual report).

Since the news story discussed an activity undertaken by CSE that involved Canadian metadata, I decided to investigate this matter in greater depth as part of the ongoing review of CSE's use of metadata in a foreign signals intelligence context. At my request, CSE briefed my office on the specific presentation referred to in the CBC story. My office then held several follow-up meetings with CSE officials, including the analyst who created the presentation and developed the tradecraft discussed within it. Over the course of these meetings and demonstrations, CSE explained the activity and its objectives in great detail, showed results of the activity described in the presentation and responded to numerous specific questions asked by my office. I found that these activities were authorized under paragraph 273.64(1)(*a*) of the *National Defence Act*. Based on our investigation, I concluded that CSE took measures to protect the privacy of Canadians in this activity.

In addition, while I was conducting this current comprehensive review, CSE discovered on its own that certain metadata was not being minimized properly. Minimization is the process by which Canadian identity information contained in metadata is rendered unidentifiable prior to being shared. The metadata ministerial directive provides guidance to CSE concerning the privacy protection measures that the Minister expects CSE to implement for the handling of this information. Minimization of certain types of metadata is one of these privacy protection measures. Therefore, the fact that CSE did not properly minimize Canadian identity information contained in certain metadata prior to being shared was contrary to the ministerial directive, and to CSE's operational policy.

Canadian identity information

Canadian identity information refers to information that may be used to identify a Canadian person, organization, or corporation, in the context of personal or business information. This may include any number, symbol or other data uniquely assigned to an individual.

I found that CSE took corrective actions and proactively suspended the sharing of certain types of metadata in order to protect the privacy of Canadians while developing a solution to the problems it encountered in this area. CSE informed me, as well as the Minister of National Defence, about these matters.

This review revealed that CSE's system for minimizing certain types of metadata was decentralized and lacked appropriate control and prioritization. CSE also lacked a proper record-keeping process.

As a result of this finding, **I recommended** that CSE use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization of metadata involving Canadian identity information.

In summary, based on my review, although I do not believe these actions were conducted intentionally, they do raise legal questions that I continue to examine and assess.

Finally, CSE's Five Eyes partners recognize each other's sovereignty and respect each other's laws by pledging not to target one another's communications. CSE trusts that its Five Eyes partners will follow the general statements in the agreements signed among partners, and not direct activities at Canadians or persons in Canada. Last year, I reported that I had obtained, through the cooperation of the Chief of CSE, detailed

documentation of CSE's international partners regarding each of their policies and procedures on the treatment of information about Canadians.

Also last year, I stated that I would explore options to cooperate with review bodies of Five Eyes countries to examine information sharing activities among respective intelligence agencies and to verify the application of respective policies. This year, in January 2015, I travelled to Washington, D.C., to meet with the Inspector General of the United States National Security Agency to personally seek assurances beyond those CSE provided to me. I was satisfied with the assurances I obtained.

Conclusion

In this first report of my current comprehensive review of CSE's metadata activities, I examined specific activities in a foreign signals intelligence context. CSE was forthcoming with documentation, interviews, written responses to questions and the provision of general support to my office throughout the review, and particularly in response to the incidents that arose during the course of this review. I do not believe that there was any intention on the part of CSE personnel to act in a way that did not conform to ministerial direction or operational policy. Nevertheless, I will carefully weigh the legal implications of the incidents referred to in this report.

Over the next fiscal year, my office will also continue work on two other reports that deal with CSE's use of metadata: the first report will examine issues identified in a 2014 report, entitled *A Review of the activities of the CSEC Office of Counter Terrorism*, and will also examine other metadata activities. A second report, expected in the coming year, will focus on CSE's use of metadata in an IT security context.

2. Review of CSE information technology security activities conducted under ministerial authorization

Background

The *National Defence Act* mandates CSE to conduct information technology (IT) security activities, specifically, to offer advice, guidance and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada. These activities, referred to as part (b) of CSE's mandate, shall not be directed at Canadians anywhere or at any person in Canada, and shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information (paragraphs 273.64(2)(*a*) and (*b*) of the *National Defence Act*).

An authorization issued by the Minister under the authority of subsection 273.65(3) of the *National Defence Act* authorizes CSE, while conducting IT security activities in the circumstances specified in paragraph 184(2)(*c*) of the *Criminal Code*, to intercept private communications. A ministerial authorization is valid for one year.

The primary objective of this review was to assess whether CSE's IT security activities complied with the law, and the extent to which CSE protected the privacy of Canadians in carrying out these activities. Particular attention was paid to CSE's interception and use of private communications as well as to information about Canadians.

This is the second review since CSE restructured its IT security activities and made changes to certain practices, policies and procedures, which were reported in my predecessor's annual report of 2010–2011. The review examined two types of IT security activities conducted by CSE under ministerial authorizations in 2009–2010, 2010–2011 and 2011–2012.

The first type of IT security activity involved CSE analyzing the computer system of a Government of Canada institution (i.e., CSE's client) under controlled circumstances, and on the request of the client, to assess vulnerabilities and to test the reaction of the client environment to cyber threats. A ministerial authorization was required for this activity because the activities may have resulted in the unintentional interception of private communications. CSE indicated it ceased offering these services in November 2012 because the activity was limited in scale and was no longer required due to technological advancements.

The second type of IT security activity my office reviewed was cyber defence operations conducted under the authority of a ministerial authorization, as they risk the unintentional interception of private communications. These activities detect and mitigate malicious activity directed toward Government of Canada computer systems and networks. Like the first type of IT security activity, cyber defence operations are conducted with the full consent of the client.

Cyber incident

A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of electronic devices and communications networks of importance to the Government of Canada.

CSE's cyber defence operations involve developing and using network defence tools; detecting, analyzing and reporting on malicious network traffic; and providing advice to Government of Canada clients on reducing the risk or extent of harm. Cyber defence tools trigger alerts when malicious activity is detected. These alerts are then forwarded for further analysis to identify and confirm threats to the network.

CSE policy describes necessary privacy measures and CSE systems can automate a large portion of these legal and policy requirements. For example, a system may prompt an analyst to determine the number of

private communications within the data the analyst intends to use and retain. The analyst then makes this determination. Other systems may calculate the number of private communications; in such cases, it is the analyst's responsibility to make certain the private communication count is correct.

My office examined applicable written and electronic records, files, correspondence and other documentation relevant to CSE's IT security activities, including policies, procedures and legal advice. Interviews were conducted with managers and other personnel involved in the activities.

CSE demonstrated its IT security activities, as well as delivered detailed briefings on related tools and databases. My office tested the contents of these systems, with CSE officials acting under our direction, to ensure conformity with legal and ministerial requirements, and associated policies and procedures.

Findings

Based on the information reviewed and the interviews conducted, CSE's IT security activities were appropriately authorized and conducted in accordance with the law as interpreted by Justice Canada and in accordance with ministerial authorizations and ministerial direction.

At my office's request, the list of cyber defence operations incidents CSE initially provided contained only incidents that CSE had identified as containing private communications. My office uncovered several private communications that had not been included in the counts. Furthermore, our questioning uncovered incidents that were incorrectly identified, either indicating a private communication when such was not the case or vice versa. As a result, my office decided to examine all incidents in 2011–2012, regardless whether or not they were identified as private communications.

These human errors were coupled with system errors that CSE had to pinpoint, delaying the review. In response to the errors my office uncovered, IT Security immediately developed two main system improvements. It is positive that CSE acted quickly to make system improvements intended to promote and demonstrate compliance. I will examine these improvements in a future review to verify that these systems are working well.

CSE has sufficient policies and processes to satisfy the legal requirements (1) not to direct its IT security interception activities at a Canadian or any person in Canada, and (2) to protect the privacy of Canadians in the use and retention of private communications and intercepted information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. Interviews with and observations of IT security managers and other employees demonstrated that they are knowledgeable about policies and procedures aimed at compliance with the law and the protection of the privacy of Canadians. CSE managers routinely monitored IT security activities for compliance and protection of the privacy of Canadians.

However, policies and procedures relating to the retention of private communications were not followed in some instances. CSE could improve some policies and procedures regarding private communications retention and minimum record-keeping requirements and practices.

Legal issues and recommendations

In the course of this review, two legal issues arose that were discussed between my office and CSE, and are the subject of my recommendations.

The first issue related to ambiguities arising from the wording of subsection 273.65(3) of the *National Defence Act*. The *National Defence Act* was modified by the *Anti-Terrorism Act* in 2001 to, among other things, legislate CSE as well as its activities. Regarding IT security

ministerial authorizations, it was established that the Minister of National Defence could authorize CSE to intercept private communications for the sole purpose of protecting Government of Canada computer systems or networks from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(*c*) of the *Criminal Code*.

Subsection 184(1) of the *Code* establishes the offence of intercepting a private communication and subsection 184(2) sets out circumstances where the interception is not an offence. Paragraph 184(2)(*c*) applies to persons engaged in providing a telephone, telegraph or other communication service to the public who intercept private communications while providing the service.

Since CSE rarely acts in the circumstances set out in paragraph 184(2)(*c*) of the *Criminal Code*, it can be argued that an IT security ministerial authorization issued under subsection 273.65(3) of the *National Defence Act* would not include CSE's primary cyber defence activities. Therefore, if a private communication were intercepted while CSE undertook an activity that was not included "in the circumstances specified in paragraph 184(2)(*c*) of the *Criminal Code*," CSE would not be shielded from the application of Part VI of the *Criminal Code*.

Consequently, I believe subsection 273.65(3) of the *National Defence Act* does not accurately reflect CSE's activities because CSE undertakes activities beyond those considered in "the circumstances specified in paragraph 184(2)(*c*) of the *Criminal Code*." **I therefore recommended** that subsection 273.65(3) of the *National Defence Act* be amended as soon as practicable to remove any ambiguities respecting CSE's authority to conduct IT security activities that risk the interception of private communications.

The second legal issue related to CSE's practice, while conducting cyber defence operations under ministerial authorization, of treating all unintentionally intercepted one-end-in-Canada e-mails as private communications as defined in the *Criminal Code*.

This issue was previously raised by former Commissioner Gonthier in the context of the 2009 *Study of CSE IT Security Activities*. He concluded that "the protection of a malicious code as a private communication may unnecessarily limit CSE's ability to fulfill part (b) of its mandate." While this is not an issue of compliance with the law *per se*, it does raise the question of whether this practice accurately reflects the privacy risk and how that risk is portrayed to the Minister.

The majority of private communications my office examined and that CSE intercepted consisted of unsolicited e-mails sent from a cyber threat actor to a Government of Canada employee and contained nothing more than malicious code and/or an element of social engineering. That is to say, there was no exchange of any personal or other consequential information between the cyber threat actor and the Government of Canada employee.

Social engineering

Social engineering can generally be defined as a deceptive process in which cyber threat actors "engineer" or design a social situation to trick others into allowing them access to an otherwise closed network, for example, by making it appear as if an e-mail has come from a trusted source.

Based on the legal opinions I have received, and with which I agree, a communication containing nothing more than malicious code and/or an element of social engineering sent to a Government of Canada computer system or network in order to compromise it is not a private communication as defined by the *Criminal Code*. Accordingly, CSE may not need a ministerial authorization to intercept such communications during the course of performing part (b) of its mandate. Therefore, CSE may not need to report to the Minister the interception of such communications.

Those e-mails used or retained by CSE are included in the number of private communications that, in accordance with the ministerial authorization, are reported to the Minister for accountability purposes. This results in a large number of communications that CSE treats as private communications, thus distorting the privacy risk implications of CSE's cyber defence activities.

I therefore recommended that CSE reporting to the Minister on private communications unintentionally intercepted under ministerial authorizations should highlight the important differences between one-end-in-Canada e-mails intercepted under cyber defence operations and private communications intercepted under foreign signals intelligence activities, including the lower expectation of privacy attached to the private communications intercepted under cyber defence operations.

Conclusion

One of the recommendations that arose from this review reflects an ongoing concern that my predecessors and I have voiced about ambiguous wording in the *National Defence Act* in relation to CSE's mandate. Reviewing and amending the *National Defence Act* would enhance the measures to protect the privacy of Canadians in the course of CSE's effort to protect Government of Canada computer systems and networks.

In future reviews, I intend to follow up on system improvements related to private communications unintentionally intercepted by CSE during its IT security activities. I will also follow up on CSE's policies and procedures for record-keeping of private communications.

3. Review of the Canadian Armed Forces Cyber Support Detachments

Background

The Canadian Armed Forces Information Operations Group (CFIOG) — a component of the Canadian Armed Forces (CAF) — may, in accordance with CSE's foreign signals intelligence mandate and on behalf of CSE, respond to the military-related requests to CSE from the CAF on foreign signals intelligence. The CFIOG Cyber Support Detachments act as the go-between to provide CSE reports on foreign signals intelligence to clients within the CAF.

The CFIOG Cyber Support Detachments provide foreign signals intelligence support to select CAF commanders for a spectrum of activities, ranging from planning to direct support to combat operations. The Detachments are not involved in either the collection of foreign signals intelligence or the production of related reports; they primarily provide situational awareness to their respective intelligence and operational staff. To fulfill those duties, the Detachments may access CSE's foreign signals intelligence systems holding data acquired under the authority of Part V.1 of the *National Defence Act*. CSE takes measures to ensure that access to these systems and the use of data acquired from these systems comply with legislation, ministerial direction, and CSE policies and procedures.

An evaluation report by CSE's Directorate of Audit, Evaluation and Ethics concerning the foreign signals intelligence support elements (as the Cyber Support Detachments were formerly called) made assertions that raised questions regarding the ability of the Detachments to demonstrate to CSE, and ultimately to my office, that their foreign signals intelligence activities complied with the law, ministerial direction, and CSE policy and procedures. CSE was to take action to address these questions, as well as the 15 recommendations in the report.

When my office became aware of this evaluation report, it informed CSE that it would wait for the implementation of corrective actions before deciding whether a review of the CFIOG Cyber Support Detachments was warranted. A decision was subsequently taken to review changes made by CFIOG and CSE to address the recommendations made in the evaluation report, and to examine a sample of foreign signals intelligence activities carried out by the Detachments during the period of March 2013 to March 2014.

At the outset, my authority under the *National Defence Act* to review the CFIOG-controlled Cyber Support Detachments was questioned. After a six-month delay and many discussions between my office, CSE and the CAF, I exercised my authority and was provided direct access to Detachment staff and premises to ensure that their foreign signals intelligence activities conducted under Part V.1 of the National Defence Act complied with the law, ministerial direction, and CSE policy and procedures. The CAF fully cooperated with my office.

A total of three site visits were conducted during the course of this review. One of these marked the first time that my office visited a CAF establishment located outside the National Capital Region that conducts certain foreign signals intelligence activities. The sites were chosen based on their level of command, the diversity of the work being performed and the length of time the site had been in operation.

The objectives of this review were:

- to acquire detailed knowledge of, and to document, the foreign signals intelligence activities of the Cyber Support Detachments;
- to determine whether CSE ensured that the foreign signals intelligence activities of the Cyber Support Detachments complied with the law; and
- to assess the extent to which CSE ensured the protection of privacy of Canadians in activities conducted by the Cyber Support Detachments.

Findings

During the course of this review, it became apparent that considerable care was taken within the CFIOG organizational chain of command to ensure the Cyber Support Detachments complied with the law and policy. While the individual detachments are guided by the local military chain of command on a day-to-day basis, a CFIOG Oversight and Compliance Section monitors activity at all detachment locations, including yearly inspections, and is the main source of policy advice on foreign signals intelligence for both the Detachments and the wider CFIOG establishment.

Unlike CSE, the Cyber Support Detachments do not collect raw data, intercept private communications, nor produce original reports, and therefore do not deal with Canadian identity information from their own activities. Foreign signals intelligence reporting is received from CSE by the Detachments for dissemination within the CAF; such reports may contain Canadian identity information that has been suppressed, that is, replaced by a generic reference such as "a named Canadian." In the event that there would be a request for the disclosure of suppressed information, the Detachments would follow an established process and pass the request to CSE for action. To date, however, there has never been a request for the disclosure of suppressed Canadian identity information.

Furthermore, CSE routinely scrutinizes monthly compliance reports generated by the individual Cyber Support Detachments that, in turn, are incorporated into compliance reports prepared by the CSE Signals Intelligence Programs Oversight and Compliance section. In this way, CSE actively ensures that the foreign signals intelligence activities of the Detachments comply with the law. My staff examined a sample of monthly compliance reports from all the Detachments and found them satisfactory.

Appropriate policies and procedures are in place to guide the activities of the Detachment staff. Each of the various Cyber Support Detachments were set up at different times and the documentation establishing them was not consistent. However, this does not appear to impede the operation, oversight or compliance of the individual Cyber Support Detachments.

Cyber Support Detachment employees interviewed and observed were aware of relevant policies and procedures, including those relating to the protection of the privacy of Canadians, and their application to routine Detachment activities. The CAF employs a comprehensive training system for all of its individual military occupations that involve handling foreign signals intelligence material. All personnel granted access to foreign signals intelligence systems participate in a program to confirm their understanding of specific CSE policies.

Furthermore, no one is granted a foreign signals intelligence qualification without passing an annual CSE test on how to protect privacy and ensure legal compliance in the conduct of CSE activities. This is the same standard required of CSE employees.

Finally, I examined the activities of the CFIOG Cyber Support Detachments as a result of CSE's Directorate of Audit, Evaluation and Ethics evaluation report. I was satisfied that the report's questions regarding compliance were answered. Of the 15 recommendations in that report, I was satisfied that either CFIOG or CSE acted on the four recommendations relevant to this review.

Conclusion

Based on the information received, the documents examined, the activities observed and the interviews conducted, I concluded that the Cyber Support Detachment activities conducted under the authority of Part V.1 of the National Defence Act were in compliance with the law, ministerial direction, and CSE policies and procedures. In addition, the activities, as they are currently carried out by the Cyber Support Detachments, do not affect the privacy of Canadians.

4. CSE assistance to the Canadian Security Intelligence Service under part (c) of CSE's mandate and section 16 of the *Canadian Security Intelligence Service Act*

Background

CSE may provide the Canadian Security Intelligence Service (CSIS) with technical and operational assistance under part (c) of its mandate and section 16 of the *CSIS Act*. Section 16 empowers CSIS to assist the ministers of Foreign Affairs and of National Defence in foreign intelligence collection activities, within Canada, in support of the international affairs and defence interests of the Government of Canada. Section 16 activities require a personal request for assistance from one of the above-noted ministers, more commonly the Minister of Foreign Affairs.

Certain section 16 activities, for example interception of communications, require a warrant from a Federal Court judge in accordance with section 21 of the *CSIS Act*. In these instances, CSIS must obtain a warrant from the Court authorizing the use of specific powers of collection to be directed against specific targets. The Minister of Public Safety must grant personal written consent prior to CSIS submitting a warrant application to the Court.

In 2007 and early 2008, interdepartmental discussions were held that related to changes in how the section 16 process worked within the security and intelligence community. One of the changes made was the elimination of the *1987 Tri-Ministerial Memorandum of Understanding* between the Minister of Foreign Affairs, the Minister of National Defence and the Solicitor General (now Minister of Public Safety). Although discussions culminated in a new process, it did not outline the roles and responsibilities of the parties involved.

CSE may provide CSIS with technical and operational assistance for section 16 activities under part (c) of CSE's mandate (paragraph 273.64(1)(*c*) of the *National Defence Act*). In such cases, CSE acts as an agent of CSIS in the interception, processing and analysis of information collected pursuant to a warrant. When carrying out activities under part (c) of its mandate for section 16 warrants, CSE must abide by the legal limitations imposed on CSIS, as stated in subsection 273.64(3) of the *National Defence Act*. These limitations include those found in the *CSIS Act* and the section 16 warrants. Not all section 16 activities may involve warrants or assistance from CSE.

Within the new process, CSE is also guided by the terms and conditions of not only the new section 16 process signed off by the ministers of Foreign Affairs, National Defence and Public Safety, but also several CSE-CSIS memoranda of understanding that cover operational cooperation in general, as well as for section 16 activities specifically.

Although the approval process changed, CSE still acts as an agent of CSIS in processing intercepted communications obtained under the authority of the warrants granted by the Federal Court. CSE also acts as an agent of the requesting minister in the dissemination of foreign intelligence reports obtained as a result of authorities exercised under warrant.

The objectives of my review were:

- to acquire detailed knowledge of and to document CSE's assistance to CSIS under section 16 of the *CSIS Act* and any changes since my office's last in-depth review; and
- to assess whether CSE activities complied with the law, including with the terms of the warrants issued to CSIS by the Federal Court.

Findings and recommendations

All section 16 warrants issued to CSIS by the Federal Court, for which CSE support was sought, were examined. From those, a number were examined in depth. For each warrant selected for this review, I was able to verify that:

- CSE had a copy of the warrant and had clear and sufficient information about the assistance sought by CSIS;
- the communications acquired by CSE for CSIS were only those communications referred to in the warrants;
- the communications were not acquired before the warrants came into force and were no longer acquired once the warrants expired;
- CSE acquired only the types of communications and information that were authorized in the warrants to be intercepted or obtained; and
- CSE complied with the limitations imposed by law on CSIS, for example, the conditions in the warrants.

CSE received copies of the warrants from CSIS when they were issued by the Federal Court.

In conducting this review, I examined: the associated technology, databases and systems used by CSE in the section 16 activities; the resulting foreign intelligence reporting; the extent to which technology was used and other efforts were applied to protect the privacy of Canadians; and CSE activities in response to previous associated findings and recommendations made by past Commissioners.

I found that, during the period under review, CSE had in place operational policies and procedures of general application to CSE's assistance in support of these warrants and related activities. Those policies and procedures provided direction to CSE employees respecting

compliance with the law and the protection of the privacy of Canadians in regards to CSE's assistance to CSIS. CSE indicated that its internal processes, including its support to CSIS's warrant renewal process, had not changed substantively despite the change in the interdepartmental process. I also found that CSE respected the condition contained in section 16 warrants to protect the privacy of Canadians when using intrusive measures, by following CSE policy to destroy all information about Canadians unless the information:

- relates to activities that would constitute a threat to the security of Canada as defined in the *CSIS Act*;
- could be used in the prevention, investigation or prosecution of an alleged indictable offence; or
- relates to those foreign states, persons or corporations for which the requesting minister has requested assistance, in writing, pursuant to section 16 of the *CSIS Act*.

I found that CSE employees who were interviewed were well aware of the policies and procedures, and demonstrated knowledge of their respective responsibilities. Interviews with CSE managers, team leaders and employees showed that managers routinely monitored CSE's assistance to CSIS for compliance with governing authorities.

I found that CSE's assistance to CSIS and all related activities was consistent with the requirements in the *Accountability Framework* and *Privacy of Canadians* ministerial directives to CSE. I also found that CSE complied with the law and took measures to protect the privacy of Canadians.

I made four recommendations: two related to the updating or creation of governing process documentation; one on the updating or creation of interdepartmental memoranda of understanding between CSIS and CSE, where applicable; and one that CSE should develop caveats to attach to

specific operational material that may be shared with Second Party partners to ensure that the material would not be used without the express authorization of CSE.

Conclusion

I concluded that CSE conducted its activities in accordance with the law and ministerial direction, and included measures to protect the privacy of Canadians. Nonetheless, I recommended that interdepartmental agreements and internal CSE policies be updated in a timely manner to reflect current procedures and practices. Given that CSIS is implicated in the updates of certain memoranda of understanding, I informed the Interim Chair of the Security Intelligence Review Committee of my recommendations.

5. Annual combined review of foreign signals intelligence ministerial authorizations and private communications, 2013–2014

Background

The *National Defence Act* prohibits CSE from directing its activities at Canadians. The Minister of National Defence may, under the Act, for the purpose of obtaining foreign signals intelligence, authorize CSE in writing to intercept private communications, i.e., communications that risk originating from or being received in Canada. The law specifies the conditions under which a ministerial authorization can be issued (see box on page 42). Ministerial authorizations relate to an "activity or class of activities" related to acquiring foreign signals intelligence — the how. The authorizations do not relate to a specific individual or subject — the who or the what. (More information on ministerial authorizations, as well as on the authorities for and limitations on CSE activities, is available on the office's website and on the CSE website.)

Conditions for foreign signals intelligence ministerial authorizations

The four conditions for a ministerial authorization under the *National Defence Act* are:

- interception must be directed at foreign entities located outside Canada;
- information could not be reasonably obtained by other means;
- the expected value of the interception would justify it; and
- satisfactory measures are in place to protect the privacy of Canadians.

The law also directs the CSE Commissioner to review activities carried out under a ministerial authorization to ensure they are authorized 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 I fulfill this part of my mandate. This year, I examined the three foreign signals intelligence ministerial authorizations in effect from December 1, 2013, to November 30, 2014, relating to three activities or classes of activities. I also conducted spot checks of private communications used and retained.

The purpose of the combined ministerial authorization review was to:

- verify that 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 CSE activities or class of activities described in the authorizations; and
- assess the impact of any changes on the risks to compliance and privacy, and, as a result, identify any subjects requiring follow-up review.

In past years, as part of the combined annual review of foreign signals intelligence ministerial authorizations, Commissioners examined samples of unintentionally intercepted private communications used and retained by CSE during the period of the ministerial authorization. Last year, my office reviewed all 66 private communications used in reports or retained at the end of the ministerial authorization period. My report on the same subject last year included four recommendations related to privacy:

- that CSE 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;
- that CSE 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;
- that CSE 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; and
- that CSE promulgate policy on the specific circumstances and handling of a particular type of communication.

To verify that the recommendations have been implemented, I decided to conduct spot checks of private communications intercepted, used and retained during certain periods through the year, as determined by my office. CSE did not have knowledge of either when these spot checks would be conducted or the period of time that would be examined.

There were 16 private communications used in reports or retained at the end of the ministerial authorization period, that is, as of November 30, 2014. CSE continues to use the same method as in previous years to count and report recognized private communications. My employees test the contents of CSE systems and databases, listen to the intercepted voice recordings, read the written contents or examine the associated transcripts of the communications, and interview CSE employees.

I examined those private communications intercepted, used and retained during the periods of April 1, 2014, to June 20, 2014, and September 1, 2014, to October 15, 2014. During these spot checks, I wanted my staff to obtain a more accurate picture of the number of foreign signals intelligence private communications intercepted throughout the year by:

- verifying whether CSE analysts immediately identified recognized private communications for essentiality — as noted in one of my recommendations last year;
- assessing whether the essentiality test was met — an ongoing aspect of reviews of intercepted private communications; and
- verifying whether the analysts regularly assessed if the ongoing retention of a recognized private communication was strictly necessary — also noted in one of my recommendations last year.

Findings

I found that the activities conducted under the 2013–2014 foreign signals intelligence ministerial authorizations were authorized, as required by the *National Defence Act*.

I examined key information relating to interception and to the privacy of Canadians for each of the three activities or class of activities, to permit comparisons. I found the 2013–2014 foreign signals intelligence ministerial authorizations did not contain any significant changes from the previous year and CSE did not make any significant changes to the technologies used for these activities.

For the spot checks, my office asked CSE to provide a list of all foreign signals intelligence private communications intercepted and recognized during the periods from April 1, 2014, to June 20, 2014, and from September 1, 2014, to October 15, 2014. My office verified this list by examining the database and confirming the number of private communications intercepted and recognized.

For the above-noted periods, CSE retained only two private communications, both of which were used in a single report. All other recognized private communications incidentally intercepted by CSE were destroyed. I am satisfied that the two private communications used were essential to international affairs, defence or security, as required by law, and that the related report contained foreign intelligence. I found nothing to suggest that any of the private communications that were recognized by CSE, either retained or deleted, were intercepted intentionally, which would be unlawful.

My office also interviewed foreign signals intelligence personnel who had knowledge of the private communications and CSE systems and databases. I found no cases of an analyst retaining a private communication longer than strictly necessary, that is, no longer than necessary to determine if it was essential to international affairs, defence or security, which was an issue in my previous review of foreign signals intelligence ministerial authorizations and private communications.

Conclusion

I concluded that the metrics and results of my reviews of the foreign signals intelligence authorizations and the spot checks of private communications indicate that CSE has taken action to quickly implement the recommendations in my previous review. I made no recommendations and will continue to conduct spot checks of private communications intercepted under foreign signals intelligence ministerial authorizations.

6. Annual review of disclosures of Canadian identity information, 2013–2014

Background

This annual review of disclosures by CSE of Canadian identity information from reports includes disclosures to Government of Canada clients and to CSE's Second Party partners. It also included disclosures to non-Five Eyes recipients through a Government of Canada client or Second Party partner. The review period covered July 1, 2013, to June 30, 2014.

The *National Defence Act* and the *Privacy Act* require CSE to take measures to protect the privacy of Canadians, including their personal information. Canadian identity information may be included in CSE foreign signals intelligence reports if the information is essential to understanding the intelligence. However, with some limited exceptions that are stated in CSE 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, CSE 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 CSE provide that information. A request for release of Canadian identity information from a CSE report may involve the release of more than one identity.

Findings

My office has conducted regular annual reviews of CSE's disclosure of Canadian identity information to Government of Canada clients and found CSE to be rigorous and thorough in its handling of such requests. Therefore, my office examined only a six-month period of such disclosures to Government of Canada clients. We continued for this review, however, to examine all of the disclosure requests received over

a period of one year from Second Party partners, as well as all requests by Government of Canada agencies or Second Party partners for disclosure of Canadian identity information to non-Five Eyes recipients.

I found that CSE's disclosure of Canadian identity information from reports to Government of Canada clients and Second Party partners complied with the law and ministerial direction and that CSE took appropriate measures to protect the privacy of Canadians.

During the six-month period, CSE received 710 requests from Government of Canada clients for Canadian identity information supressed in foreign intelligence and IT security reporting. The number does not represent the quantity of identity information disclosed, but rather the number of instances that Government of Canada clients have submitted separate requests for identity information suppressed in reports to be disclosed, providing a unique operational justification in each case. Of these 710 requests, my office examined a sample of over 20 percent, along with all reports that contained the suppressed identity information that was the subject of the request. CSE ensured that all requesting agencies or departments had the necessary authority and the operational justification prior to the information being released. Requests not supported by adequate authority or operational justifications were denied.

CSE also received requests for the disclosure of Canadian identity information from Second Party partners. My office examined all the requests and related reports. The requests resulted in roughly an equal number of denials and disclosures of Canadian identity information.

Six requests were made for disclosure of Canadian identity information to non-Five Eyes recipients. Five of these requests were made by a Government of Canada client and one was made by a Second Party partner. None were denied.

In February 2011, Cabinet approved a framework for addressing risks in sharing information with foreign entities that could result in the mistreatment of an individual. This was to be accomplished through ministerial direction to Government of Canada departments and agencies. As a result, the Minister of National Defence issued a directive to CSE in 2011 that required CSE to develop policies to guide information sharing with non-Five Eyes entities, including approval authorities that are commensurate with the risks of mistreatment. CSE complied with this requirement.

A mistreatment risk assessment must be conducted before CSE can disclose Canadian identity information to non-Five Eyes recipients through Second Party partners or Government of Canada clients. My office reviewed all six requests as well as some of the corresponding mistreatment risk assessments.

The only privacy incidents that my office found when examining all requests for disclosure had been identified by CSE; these incidents had already been added to CSE's Privacy Incident File, which my office reviews separately (see review number 7).

CSE has comprehensive policies and procedures that guide its disclosure of Canadian identity information from reports to Government of Canada clients. It is a positive development that CSE has updated its policies to encompass disclosures to Second Party partners and to non-Five Eyes recipients through Government of Canada clients and Second Party partners.

My office examined all request forms, reports, internal documentation and approvals, and made inquiries of CSE staff as appropriate. The examination of these documents found that CSE employees conducting activities related to disclosures of Canadian identity information complied with policies and procedures. In addition, for the requests

reviewed, we found that CSE employees and managers responsible for the disclosure of Canadian identity information were consistent and rigorous in applying all relevant ministerial direction, policies, procedures and standards related to disclosure of Canadian identity information, including privacy protections.

CSE has now completed the full automation of its information and records management processes for the disclosure of Canadian identity information to Government of Canada clients. This system appears to be working well. CSE has indicated that it is now undertaking the automation of a similar system to handle the process for all Second Party partner requests. I will monitor its development in future annual reviews.

Conclusion

My review did not result in any recommendations. CSE conducted its activities in a thorough manner and complied with the law, ministerial direction and internal CSE policies and procedures. During the course of this review, I became aware of information involving the Canadian Security Intelligence Service and referred the matter to the interim Chair of the Security Intelligence Review Committee for any follow-up she deems appropriate. I intend to continue to conduct an annual review of disclosures. I will also monitor the progress and impact of automating the process for handling Second Party requests for disclosure of Canadian identity information.

7. Review of CSE's Privacy Incidents File and Minor Procedural Errors Record, 2014

Background

CSE requires its employees who conduct foreign signals intelligence and information technology security activities to report and document privacy incidents. The objectives are to prevent further incidents and to strengthen compliance with legal and ministerial requirements and with CSE policies. A privacy incident occurs when the privacy of a Canadian is put at risk in a manner that runs counter to or is not provided for in CSE's policies, which are based on CSE's legislative requirements not to direct activities at Canadians and to have measures to protect the privacy of Canadians.

Incidents are documented in one of two files, depending on the extent of risk. The Privacy Incidents File is a record of incidents where privacy was breached. The Minor Procedural Errors Report contains operational errors that occurred in connection with information relating to Canadians but did not result in that information leaving control of CSE or in that information being exposed to external recipients who ought not to have received it. CSE began the Privacy Incidents File and Minor Procedural Errors Report in 2007 and notified the Commissioner's office of these tools.

During the year, each review I undertake of CSE activities generally includes an examination of any privacy incident relating to the subject of the review. Individual reviews, however, may not capture all incidents. Even incidents that are captured during a review may not allow for examination of CSE's response, which might be pending at the time of the issuance of the report. The annual review of the Privacy Incidents File focuses on privacy breaches not examined in detail in the course of my other reviews, to ensure that CSE took appropriate corrective actions for all breaches identified.

My review consisted of an examination of the Privacy Incidents File and Minor Procedural Errors Report records, as well as CSE's answers to my questions. My office also made an independent verification of a sample of reports from the Privacy Incidents File by searching one of CSE's databases.

The objectives of this review were to:

- examine the incidents, procedural errors and subsequent actions by CSE to correct the incidents or mitigate the consequences;
- follow up on specific incidents identified in past reviews and the associated corrective actions taken by CSE;
- determine what incidents may raise issues about compliance with the law or the protection of the privacy of Canadians;
- identify any systemic issues that suggest the need for broader corrective actions on the part of CSE; and
- contribute to the evaluation of CSE's policy compliance validation framework and monitoring activities.

Findings

I found that CSE took appropriate corrective actions in response to the privacy incidents and minor procedural errors it identified and recorded during 2014. During the course of my review, none of these suggested any systemic deficiencies or issues that require follow-up review.

Last year, I had recommended that CSE request confirmation from Second Parties that they had addressed any privacy breaches relating to a Canadian. I recommended that CSE indicate in its file the response from Second Party partners. This year, I found CSE's response and follow-up activities on the issue to be satisfactory. A review of a sample of CSE's requests to Second Parties, as well as the review of the Privacy Incidents File, demonstrated that CSE is taking measures to implement my recommendation. I will continue to monitor this.

As well, CSE is in the process of revising policy to incorporate new guidance related to how CSE handles identity information in foreign signals intelligence reports — strengthening the protection of the privacy of Canadians. In future reviews, I will consider the impact of the changes to this policy.

This year, a technical deficiency in one CSE system — recorded as a separate privacy incident — affected the handling of other privacy incidents. In reviewing the documentation provided, I am satisfied that CSE acted in a timely manner and took appropriate measures to correct that situation.

As mentioned in last year's *Annual review of a sample of disclosures by CSEC of Canadian identity information to Government of Canada clients and second party clients*, my office identified two privacy incidents pertaining to two Canadians whose identities were not suppressed in intelligence reports, incidents that CSE subsequently recorded in the Privacy Incidents File. I reviewed the privacy breaches and the re-issued reports to ensure that the Canadian identity information was now suppressed and found that CSE took appropriate mitigation measures.

In May 2014, CSE informed me of a privacy incident involving an information flow between a Government of Canada client and CSE's Second Party partners that risked unauthorized disclosure of privacy-related information. At the time, my office reviewed a briefing note to CSE management on the issue and believed the actions and commitments taken by CSE for this practice to stop were appropriate and did not raise any pressing questions. While examining the Privacy Incidents File, I reviewed additional documents in relation to this incident. I can report that CSE took appropriate corrective actions in response to the privacy incident. CSE's proactive disclosure to my office of this incident demonstrated its commitment to transparency and to protecting privacy.

Conclusion

My review did not result in any recommendations nor did it reveal any systemic deficiencies. Future reviews will take into account the impact of the updated policy on how CSE handles identity information in foreign signals intelligence reports.

COMPLAINTS ABOUT CSE ACTIVITIES

In 2014–2015, my office was contacted by a number of individuals who were seeking information or expressing concern about CSE activities. However, the inquiries were assessed as outside of the Commissioner's mandate, not related to CSE's operational activities or without merit. There were no complaints about CSE activities that warranted my 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 CSE activities — on the grounds that it is in the public interest. No such matters were reported to me in 2014–2015. (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

As part of my goal to increase transparency, my officials and I make concerted efforts to broaden public awareness of the work of my office. This is accomplished in many ways, including making more information available through our website and my public annual report, speaking at and participating in conferences and seminars, responding to media inquiries, and participating in bilateral meetings with colleagues in the other Canadian review bodies and with review bodies of other countries.

When I indicated in last year's annual report that the office's website included new information, to clarify misconceptions and to address issues and criticisms raised about the role and work of the Commissioner, I promised to post more detail about how my office reviews the operational activities of CSE. This past year I added detailed information on reviews: about how I select activities for review, how I conduct reviews, the criteria on which reviews are structured, and how I report on the findings of my reviews. (More information regarding reviews is available on the office's website.)

My office also continued to deliver presentations about our work as part of the orientation of new CSE employees. These sessions ceased in the late spring when CSE began moving into its new building but are expected to start again later in 2015. As in the old CSE facilities, we will have dedicated, secure, separate office space in the new building, where we can conduct interviews and work on-site during our reviews.

The Executive Director attended the Privacy and Security Conference in Victoria B.C. in February. This leading conference explores topical and controversial issues related to information and communications technology, information security, the role of government and government agencies, and privacy.

Throughout the year, staff from my office also attended many other conferences dealing with international affairs, information technology security, national security and privacy, sponsored by many different organizations such as the Canadian Institute for the Administration of Justice, the Conference of Defence Associations Institute, and the Canadian Association for Security and Intelligence Studies.

My office also provided support to the Canadian Network for Research on Terrorism, Security and Society (TSAS), a network initiated by a number of university academics with the support of government departments and agencies. Our support was in-kind and will consist of my staff offering to read and comment on certain TSAS reports, to engage in discussions with researchers and to attend meetings or workshops of relevance.

Throughout the year, I met with a number of my review colleagues in Canada as well as internationally.

Consulting with review bodies in Canada

The Review Agencies Forum is a meeting of representatives of my office, the Security Intelligence Review Committee (SIRC), the Civilian Review and Complaints Commission for the RCMP (CRCC) and the Office of the Privacy Commissioner of Canada. This forum provides an opportunity to compare best practices in review methodologies and to discuss issues of mutual interest and concern, but excludes any exchange of operational details of reviews. The forum met in November and March.

I met with the interim Chair of SIRC for general discussions regarding cooperation between our organizations and our respective executive directors agreed to coordinate certain basic elements of two reviews of activities that involved both CSE and CSIS. As already noted in the review section, I referred two recommendations and another issue, all involving CSIS, to the interim Chair of SIRC for SIRC's information and any follow-up it deemed appropriate. The executive directors of my office, SIRC and CRCC also met to discuss further possibilities for cooperation and to exchange views on issues related to review of intelligence and security agencies.

In June 2014, the Executive Director of my office joined with his SIRC counterpart in a panel at the third annual Chief Information Security Officers Executive Summit in Vancouver. They described the roles of their respective organizations in contributing to the public accountability of the intelligence agencies they are responsible for reviewing. This specialized and informed group, with an interest in the threat environment and in the role of the intelligence agencies, discussed whether the current operating environment and the public interest are adequately reflected in existing legislation and frameworks.

I met with the new Privacy Commissioner of Canada, Daniel Therrien, a few months after his appointment. In October, I addressed the meeting of federal, provincial and territorial privacy and information commissioners in Ottawa. I explained my mandate, my role and the common interest we serve in ensuring the protection of the privacy of Canadians. These commissioners have a much broader area of responsibility, in terms of covering most of the departments and agencies within their respective jurisdictions, whereas my mandate concentrates exclusively on CSE. I found the discussion with the privacy and information commissioners to be productive and helpful in learning about their particular perspectives and concerns.

Consulting with review bodies of other countries

Last July, the Executive Director and the Director of Operations joined me in attending the ninth International Intelligence Review Agencies Conference in London, England. Representatives from 14 other countries attended. These biennial conferences are an opportunity for legislators and senior office holders working in the field of intelligence review and oversight to exchange views and experiences on topics of mutual concern. The conference also supports countries in the development of intelligence review and oversight mechanisms, drawing on the experience of countries with existing structures. Conference sessions were devoted to topics such as the future of intelligence oversight, public expectations of privacy and what is proportionate, and working toward greater transparency. Broadening the dialogue and expanding our expert networks through these conferences benefits our work in Canada. We have an opportunity to hear the experiences of, and to share best practices with, a wide variety of review and oversight bodies.

In December, some of my officials and I met with the U.K. Independent Reviewer of Terrorism Legislation, David Anderson, Q.C. Mr. Anderson was tasked by the British government to examine whether the United Kingdom needs new or amended legislation to address the interception powers of security and intelligence agencies. His focus includes communications data, which is the term used in the United Kingdom for

what we refer to as metadata. In this useful exchange we also learned more about his overall role as independent reviewer.

In last year's annual report, I concluded my review of sharing of foreign signals intelligence with international partners with the statement that I was going to 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. While in London for the International Intelligence Review Agencies Conference, we met with the U.K. Interception of Communications Commissioner's Office to discuss and compare experiences in review methodologies, privacy issues and legal frameworks. In January, I travelled to Washington, D.C., accompanied by my Executive Director and acting Director of Operations, to meet with the Inspector General of the United States Intelligence Community and then with the Inspector General of the National Security Agency (NSA).

The Inspector General of the U.S. Intelligence Community is responsible for conducting audits, investigations, inspections and reviews of the entire U.S. intelligence community. Our meeting included inspectors general and representatives from a number of other agencies. Despite significant distinctions between my office and the inspectors general — a principal one being that the inspectors general have a much broader mandate whereas I have a mandate specific to compliance with the law — the main purpose of our meeting was to learn about the level of cooperation among the intelligence community inspectors general and how I might apply that to my efforts to encourage cooperation among Canadian review bodies. I was also interested to discuss the interactions between the inspectors general and other offices more recently established within the intelligence agencies, such as those that deal with civil liberties and privacy, and with whistleblower and source protection. I was struck by my hosts' candidness in discussing issues and sharing views. This highly worthwhile meeting will stimulate reflections on my own work.

Following the meeting with the Inspector General of the Intelligence Community and his colleagues, we met with the Inspector General of the NSA. These detailed discussions were specific to the review in my annual report last year regarding CSE foreign signals intelligence sharing with its international partners. As I state elsewhere in this report, I wished to hear — and received — personal assurances from the Inspector General as to NSA's policies and procedures on the treatment of information about Canadians.

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 CSE on new activities and changes to existing activities. Another is the classified annual report to the Minister of National Defence from the Chief of CSE on CSE's priorities and its legal, policy and management issues of significance.

With the exception of my review of CSE's foreign signals intelligence metadata activities (some aspects will continue in the coming year) and my review of particular foreign signals intelligence activities under ministerial authorizations, all of the reviews that were under way last year have been completed.

Reviews planned for 2014–2015 are: a focused review of CSE's information technology security (IT) metadata activities, a review of particular foreign signals intelligence activities conducted under ministerial authorization and ministerial directive; CSE's sharing of foreign signals intelligence with foreign entities; a review of a specific CSE activity in support to the Canadian Security Intelligence Service (CSIS) under part (c) of its mandate and section 12 of the *CSIS Act*; and

a study of the sharing of information between the foreign signals intelligence and IT security sections within CSE.

In addition, I will conduct annual reviews of: (1) foreign signals intelligence and IT security ministerial authorizations; (2) CSE disclosures of Canadian identity information; and (3) privacy incidents and procedural errors identified by CSE and the measures subsequently taken by CSE to address them. I also plan to continue to conduct spot checks of the private communications CSE has intercepted, used and retained.

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, advisors, 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.

[...]

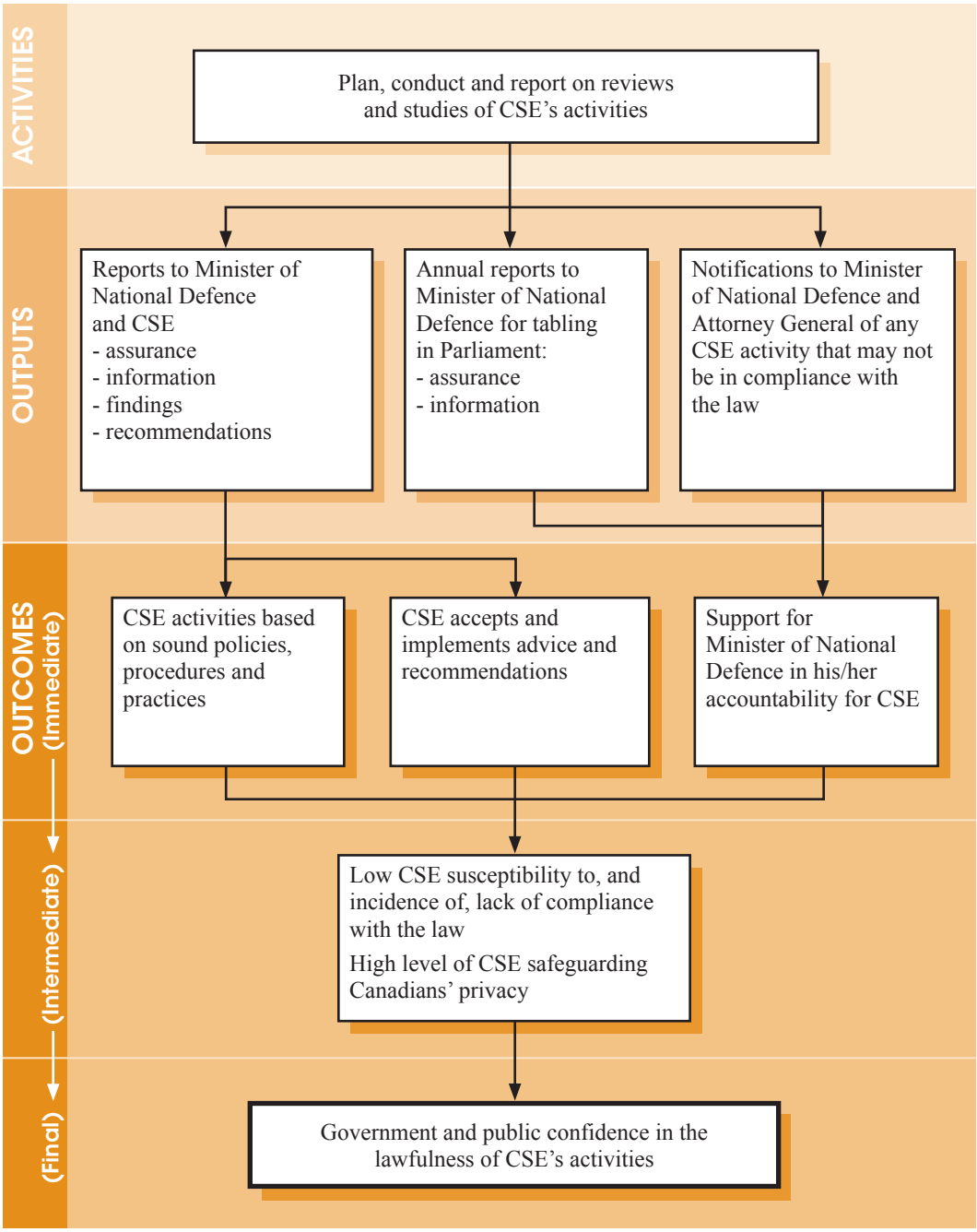
Prior disclosure to authorities necessary

(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: 2014–2015 STATEMENT OF EXPENDITURES

Standard Object Summary ($)

Salaries and Benefits	1,241,763
Transportation and Telecommunications	47,916
Information	12,931
Professional and Special Services	353,986
Rentals	325,649
Repairs and Maintenance	2,029
Material and Supplies	12,616
Machinery and Equipment	1,850
Capital Assets	8,700
Other Payments (one- time transition payment for salary payments in arrears)	36,120
Total	**2,043,560**