Office of the
Communications Security
Establishment Commissioner

CANADA

Bureau du
Commissaire du Centre de la
sécurité des télécommunications

December 16, 2013

BY COURIER

The Honourable Daniel Lang
Chair
Senate Standing Committee
on National Security and Defence
The Senate of Canada
Ottawa, Ontario
K1A 0A4

Dear Senator Lang,

I appreciated the opportunity to appear before the Senate Standing Committee on National Security and Defence this past Monday.

By way of this letter, I would like to provide you and members of your committee with additional information about areas of interest to the Committee, as reflected in the questions posed to me and my Executive Director during our appearance on December 9th.

Establishing Intelligence Priorities

Questions were asked about how intelligence priorities are established. When CSEC operates under part a) of its mandate (273.64 (1)(a) of the *National Defence Act* attached), it is required to collect foreign intelligence "in accordance with Government of Canada priorities". In this regard, there is a very brief description in a document on the PCO website, entitled "The Canadian Security and Intelligence Community", produced in 2001. I have enclosed the relevant pages, as well as the web link: http://www.pcobcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=aarchives/csis-scrs/table-eng.htm .

Metadata

Appended to this letter is information from previous Commissioners' public reports that dealt with metadata. The previous reports, however, could not at that time explicitly refer to the term itself because it was classified information. After the first U.S. classified documents were revealed by Edward Snowden in June, my predecessor pushed CSEC to disclose more information to help clarify the public discussion. There was agreement on the part of the Government to allow the Commissioner to use the term publicly, which he did in his Statement dated June 13, 2013. Now that the term is de-classified, I hope this additional information will

P.O. Box/C.P. 1984, Station "B"/ Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax (613) 992-4096
info@ocsec-bccst.gc.ca

be helpful to a better understanding by the Senate Committee of how metadata may be used by CSEC, how long the Commissioner's office has been reviewing it, and the significant results of some of those reviews. However, questions about the extent and details of CSEC activities that may use metadata should be directed to CSEC.

Capacity of Commissioner's Office to Review CSEC

With respect to the relative size of my office and the question whether I can adequately review such a large organization as CSEC, I would make the following points, having had the opportunity over my first two months to read material from my office and CSEC, to discuss the situation with my staff and to examine the range of reviews currently nearing completion and underway. I have also had an opportunity to discuss with my predecessor his opinions on this issue. Obviously, a Commissioner could do more review with more resources, but resources have increased over these past years.

My assessment at this time is that my office can, with my and CSEC's mandates as they are currently legislated, adequately review the activities of CSEC for compliance with the law and the protection of the privacy of Canadians, for the following reasons:

- The Commissioner's office has grown from eight full-time staff five years ago to eleven presently – a one-third increase. In addition, I have two subject matter experts conducting reviews, one of whom was engaged within the past two years;
- A process of risk analysis determines review priorities;
- The focus of CSEC's intelligence collection activities is foreign, whereas the number of private communications unintentionally intercepted, used and retained by CSEC under Ministerial Authorizations is small; we can review all of them and are doing so;
- Not all of the over 2100 employees of CSEC are operational. Those who are operational are split between SIGINT collection and IT security, the latter involving advice, guidance and services to help protect government information (which includes information of Canadians who have submitted it to various government departments and programmes) and information systems;
- The CSEC's processes are increasingly automated, with privacy protections being built into them, which diminishes the possibilities of human error. My office also verifies CSEC's use of technology;
- The size of my office relative to CSEC is similar to other review bodies, e.g. the Security Intelligence Review Committee that reviews CSIS. There are many models to examine in many countries. For example, the Inspector General of Intelligence and Security in Australia has a staff size the same as my office but is responsible for reviewing six intelligence agencies, including the Australian Signals Directorate, the CSEC equivalent in Australia.

Parliamentary Oversight

I would welcome appearing more frequently before Parliamentary committees dealing with national security and intelligence review. If committee members had security clearances to enable them to hear classified information, that would certainly help fill in some of the information gaps. My view at this time is that a Parliamentary committee with access to classified information could usefully examine resources allocated to security and intelligence organisations (including agencies and review bodies), budgets, whether it agrees with intelligence priorities set by the government, and could call the heads of the review bodies, as well as the agencies, to appear before it to discuss their respective priorities and activities. It would be important, however, to avoid duplication of effort.

A number of questions posed by Committee members seemed to lead to areas that are not dealt with by my office, for example, whether the intelligence priorities are appropriate, and internal security controls of government. It is part of my mandate to examine whether CSEC is collecting foreign signals intelligence "in accordance with Government of Canada intelligence priorities", but not to determine whether those priorities are appropriate.

If I can provide you with any additional information that is of interest to the Committee, please let me know and I will comply to the extent possible.

Sincerely,

Hon. Jean-Pierre Plouffe
Commissioner

CSE Commissioners'review of metadata

Commissioner Décary's June 13, 2013 statement described Commissioners' reviews of CSEC activities that may use metadata:

In the case of metadata, I verify that it is collected and used by CSEC only for purposes of providing intelligence on foreign entities located outside Canada and to protect information infrastructures of importance to the government. I have reviewed CSEC metadata activities and have found them to be in compliance with the law and to be subject to comprehensive and satisfactory measures to protect the privacy of Canadians.

Commissioner Décary noted that given that these activities may impact the privacy of Canadians, he had already approved, prior to the leaks by Mr. Snowden, a follow-up review relating to these activities. This work is ongoing. However, review of CSEC activities involving metadata has been conducted since 2006, and metadata has been the focus of a particular in-depth review.

Commissioner Décary's 2010–2011 public annual report explained certain CSEC activities that may use metadata (at a time when the term itself was classified):

> CSEC conducts a number of activities for the purposes of locating new sources of foreign intelligence. When other means have been exhausted, CSEC may use information about Canadians when it has reasonable grounds to believe that using this information may assist in identifying and obtaining foreign intelligence. CSEC conducts these activities infrequently, but they can be a valuable tool in meeting Government of Canada intelligence priorities. CSEC does not require a ministerial authorization to conduct these activities because they do not involve interception of private communications [i.e. metadata does not reveal the content of a communication and therefore is not considered to be a private communication]. However, a ministerial directive provides guidance on the conduct of these activities.

Commissioner Décary also noted "some Commissioners' recommendations have resulted in CSEC suspending certain activities to re-examine how the activities are conducted." Subsequent to questions raised by Commissioner Gonthier in reviews in 2006–2008 about the proper authority for conducting the activities, CSEC took the significant step of stopping certain metadata activities. Commissioner Décary's 2010–2011 public annual report explains: "Subsequent to these reviews and statements in the annual reports, the Chief of CSEC suspended these activities. CSEC then made significant changes to related policies, procedures and practices."

It has been the opinion of Commissioners, as voiced in public annual reports and statements, that CSEC could speak more openly about its work without undermining national security, intelligence activities or foreign affairs. To this end, Commissioners have

recommended to CSEC that it make publicly available additional information on its activities, including those activities that may use metadata.

In addition, CSEC is consulting the Commissioner's office on a number of requests under the *Access to Information Act* for copies of the Commissioners' classified reports to the Minister, including on CSEC activities that may use metadata. These requests represent another opportunity to provide Canadians with additional factual information about CSEC's activities and how the Commissioner's office goes about its work. We anticipate that the reports will be released by CSEC in the coming weeks.

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.

Fonctions du commissaire

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

Transitional

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

2001, c. 41, s. 102.

Disposition transitoire

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

2001, ch. 41, art. 102.

Mandate

273.64 (1) The mandate of the Communications Security Establishment is

(*a*) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

(*b*) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

(*c*) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Mandat

273.64 (1) Le mandat du Centre de la sécurité des télécommunications est le suivant:

a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;

b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;

c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.

Protection of Canadians

(2) Activities carried out under paragraphs (1)(*a*) and (*b*)

(*a*) shall not be directed at Canadians or any person in Canada; and

(*b*) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

Protection des Canadiens

(2) Les activités mentionnées aux alinéas (1)*a*) ou *b*):

a) ne peuvent viser des Canadiens ou toute personne au Canada;

b) doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés.

Limitations imposed by law

(3) Activities carried out under paragraph (1)(*c*) are subject to any limitations imposed by law on federal law enforcement and security agencies in the performance of their duties.

2001, c. 41, s. 102.

Limites

(3) Les activités mentionnées à l'alinéa (1)*c*) sont assujetties aux limites que la loi impose à l'exercice des fonctions des organismes fédéraux en question.

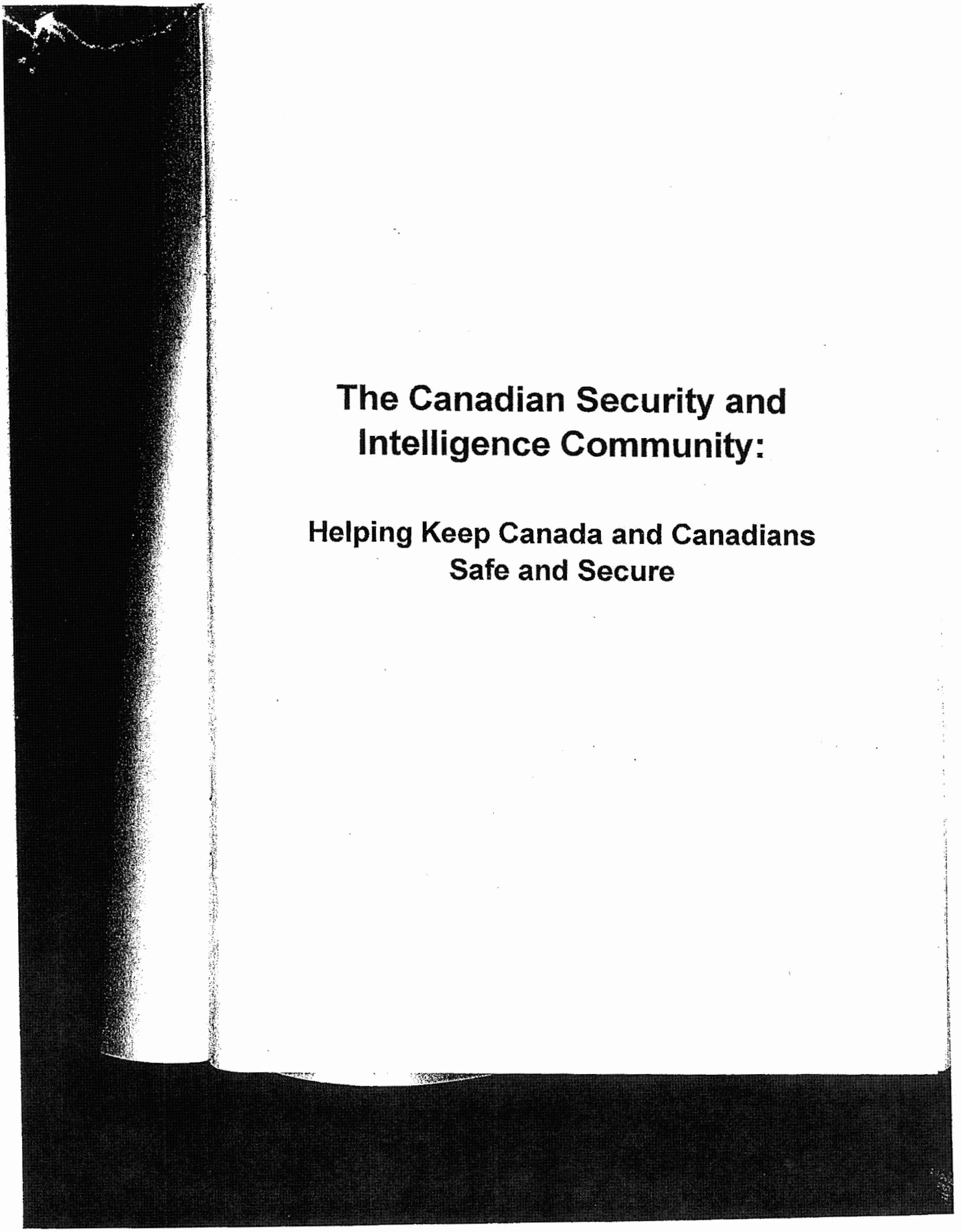
2001, ch. 41, art. 102.

Ministerial authorization

273.65 (1) The Minister may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communi-

Autorisation ministérielle

273.65 (1) Le ministre peut, dans le seul but d'obtenir des renseignements étrangers, autoriser par écrit le Centre de la sécurité des télécommunications à intercepter des communica-



The Canadian Security and Intelligence Community:

Helping Keep Canada and Canadians Safe and Secure

National Library of Canada cataloguing in publication data

The Canadian Security and Intelligence Community

Text in English and French on inverted pages.
Title on added t.p.: La collectivité canadienne de la sécurité et du renseignement.
Issued also on the Internet (www.pco-bcp.gc.ca)
ISBN 0-662-65480-3
Cat. No. CP32-74/2001

1. Intelligence service – Canada.
2. Internal security – Canada.
3. National security – Canada.
I. Canada. Privy Council Office.
II. Title: La collectivité canadienne de la sécurité et du renseignement.

JL86.I58C32 2001 352.3'79'0971 C2001-980037-1E

www.pco-bcp.gc.ca

Others are technical experts who keep the community technologically on par with such adversaries as organized criminals and international terrorists.

Together, they constitute a significant asset working together to advance Canada's national interests.

In doing their work, some components within the community possess a unique capability and authority to collect and assess information that is not available from conventional sources — in other words, secret information. In doing their work, security and intelligence community staff must blend this information with all other available information, including openly-available information from international broadcasts, newspapers, the Internet and academia, other parts of government, and intelligence generated by foreign countries.

III. The Role of Ministers

The Prime Minister of Canada is ultimately accountable to Parliament and to the people of Canada for the security and integrity of the nation. The Prime Minister therefore provides broad guidance to the security and intelligence community.

No single Cabinet minister is responsible for Canada's security and intelligence community. Instead, a number of ministers are accountable for the activities of the organizations that report to each of them.

Ministers collectively establish intelligence priorities for the security and intelligence community at the annual Meeting of Ministers on Security and Intelligence, usually chaired by the Prime Minister. Through discussions at Cabinet committee meetings, ministers also provide direction on major policy and resource issues related to security and intelligence, such as airport security upgrades, policy regarding the sale of Canadian encryption technology abroad, or funding for the community's action against organized crime.