Communications Security Establishment Commissioner

ANNUAL REPORT
2015 – 2016

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: http://www.ocsec-bccst.gc.ca

Catalogue No. D95E
ISSN 1700-0874

Communications Security
Establishment Commissioner

The Honourable Jean-Pierre Plouffe, CD

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, CD

June 2016

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, 2015, to March 31, 2016, 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
Tel.: 613-992-3044 Fax: 613-992-4096

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

In the past year, legislation to deal with terrorism by granting new powers to security and intelligence agencies has raised questions about whether adequate oversight is in place. Stirring the debate have been the outrages of the terrorist group calling itself the Islamic State and the violent attacks of its followers, who include extremists in Canada and Canadian foreign fighters. As a backdrop, in exercising my duty as Commissioner, I informed the Minister of National Defence and the Attorney General of Canada of a Communications Security Establishment (CSE) metadata activity that I believed was not in compliance with the law. Such a finding was a first in the office's history. This finding was announced when my previous annual report was tabled in Parliament — six months later than usual because of the federal election call. I was nonetheless encouraged by the subsequent increased transparency of CSE activities.

The Office of the CSE Commissioner has been helping to ensure CSE complies with the law, including protecting the privacy of Canadians, for two decades and will have celebrated its 20th anniversary on June 19, 2016. As I reflect on my experience during my term as Commissioner, which is set to end in October 2016, this annual report offers an opportunity to recognize significant developments and some of the office's key accomplishments over the past 20 years. The office should be proud of the impact that it has had on the protection of the privacy of Canadians, on supporting the Minister in his accountability for and control of CSE, and on instilling public confidence that CSE is rigorously reviewed to determine whether its activities comply with the law and that it takes adequate measures to protect the privacy of Canadians. Indeed, as the Honourable Justice Dennis O'Connor wrote in his 2006 report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, the office "functions very well and I see no reason to interfere with that operation."

While the office can boast some major achievements over its 20 years, important work lays ahead. The new government made commitments to increase transparency, to strengthen accountability of security and intelligence agencies, and to ensure a better balance of collective security with rights and freedoms, which most assuredly includes satisfactory measures to protect the privacy of Canadians. To this end, I sent a letter to Mr. David McGuinty, M.P. — to whom the Prime Minister assigned a leadership role in a proposed national security committee of parliamentarians — and copied the letter to the ministers of National Defence and Public Safety, and to the Government House Leader, to provide observations and comments based on my experience as CSE Commissioner.

Canada's model of expert review of security and intelligence agencies is effective. It involves an independent review body specific to the agency under review at arm's length from government. These review bodies have powers that guarantee full access to the agencies they review, including to all personnel. Dedicated employees with many years of experience have resulted in an accumulated, in-depth knowledge of the operationally sensitive, and often technically and legally complex, nature of the agencies' activities. I know that my office has developed rigorous methodologies to enable comprehensive, robust review. Review bodies are also seasoned in the delicate task of informing the public about their work to the extent possible, while protecting sensitive information.

Much as I appreciate the model of review we have developed in Canada, change is necessary as the context evolves along with technology and security threats. Clarifying the *National Defence Act*, as recommended by Commissioners for more than 10 years, would support the government's commitments to strengthen CSE's accountability and transparency. Amendments to the Act could also provide the Commissioner, who is a retired judge of a superior court, with new functions to support the Minister in his accountability for, and control of, CSE; for example, the Commissioner could provide the Minister an independent expert assessment of proposed ministerial authorizations, whether the conditions of authorization set out in the Act are met, and concomitant privacy protections. This approach would be consistent with international models, such as reforms proceeding in the United Kingdom.

The legal and privacy concerns of cooperation and intelligence sharing among security and intelligence agencies present another issue, specifically the question of cooperation among review bodies. To a certain extent, Canadian review bodies can work collaboratively under existing law. However, as I have stated previously, legislation should be amended to explicitly authorize review bodies to exchange information, conduct joint investigations and prepare coordinated reports, and to require security and intelligence agencies to cooperate with the review bodies.

I welcome the government's commitment to establish a security-cleared committee of parliamentarians focused on national security. Together with expert review bodies, such a committee would provide a comprehensive framework for accountability of security and intelligence activities, and could contribute to enhancing public trust. The respective roles, however, must be clearly defined to avoid confusion, duplication of effort and wasting of resources. My office may require additional resources to work with the new parliamentary committee and to support the conduct of joint reviews.

Finally, a word about transparency — a cornerstone of my approach as Commissioner. Transparency is essential to demystify the work of CSE, to contribute to a better-informed public discussion, to enhance accountablility, and to the office's ultimate objective of maintaining public confidence in the important work CSE performs. As such, I have continued to challenge CSE to make public as much information as possible, within the restrictions of the *Security of Information Act*, and to carefully consider whether certain information needs to remain classified.

In the past year, I welcomed the opportunity to appear twice before the Senate Standing Committee on National Security and Defence to explain my office's activities and my findings. As the government pursues its overall security agenda, I hope to further contribute to the development of proposals that will strengthen both the accountability for CSE and public confidence.

COMMISSIONER'S MANDATE AND REVIEW WORK

Mandate

The Communications Security Establishment (CSE) Commissioner's mandate is set out under Part V.1 of the *National Defence Act* (NDA):

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

2. to undertake any investigation the Commissioner considers necessary in response to a written complaint; 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 activity that the Commissioner believes may not be in compliance with the law.

Under section 15 of the *Security of Information Act*, the Commissioner also has 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.

The NDA requires that the CSE Commissioner be a supernumerary or retired judge of a superior court. The NDA provides the Commissioner with full independence, as well as full access to all CSE facilities and systems, and full access to CSE personnel, including the power of subpoena to compel individuals to answer questions. The Commissioner has a separate budget granted by Parliament.

The review process

The review process is the Commissioner's approach to examining CSE activities. CSE activities include collecting foreign intelligence on foreign targets located outside Canada, that is, information about the capabilities, intentions or activities of foreign targets relating to international affairs, defence or security. CSE is also Canada's lead technical agency for cyber defence and for the cryptography and other information technology security technologies needed to protect government computer systems and networks containing sensitive national and personal information. CSE also has a mandate to use its unique capabilities to

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

The purpose of the Commissioner's review mandate is:

- to determine whether CSE complies with the law and, if the Commissioner believes 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 NDA are met;

- to verify that CSE does not direct its foreign signals intelligence and cyber defence activities at Canadians or any person in Canada; and

- to promote the development and effective application of satisfactory measures to protect the privacy of Canadians in all the operational activities CSE undertakes.

CSE's activities are distinct from security and criminal intelligence that is collected by other agencies, which is information on activities that could threaten the security of Canada or public safety and is usually acquired from targeting Canadians. CSE activities are specifically prohibited from being directed at Canadians or persons in Canada. Restricting intelligence gathering to foreign targets outside Canada is complicated by the interconnected and ever-evolving global information infrastructure, as well as by the foreign targets, who are themselves technologically savvy. CSE requires sophisticated technical capabilities to acquire and analyze information and to detect and mitigate malicious cyber activity. CSE's methods are effective only if they remain secret.

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

The office is 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.

Each review assesses CSE activities against the following standard set of criteria:

- **Legal requirements:** the Commissioner expects CSE to conduct its activities in accordance with the *Canadian Charter of Rights and Freedoms*, the NDA, the *Privacy Act,* the *Criminal Code*, and any other relevant legislation.
- **Ministerial requirements:** the Commissioner expects 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:** the Commissioner expects 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. He expects CSE employees to be knowledgeable about and comply with policies and procedures. He also expects 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.

Reporting on findings

The results of individual reviews are produced as classified reports to the Minister that document CSE activities, contain findings relating to the standard criteria, and disclose the nature and significance of any deviations from the criteria. If necessary, the Commissioner makes recommendations to the Minister aimed at improving privacy protections or correcting problems with CSE operational activities raised during the course of review. Following the standard audit practice of disclosure, CSE is provided with draft versions of reports to confirm factual accuracy.

The Commissioner's annual report is a public document provided to the Minister, who by law must table it in Parliament. The Commissioner's office publishes the titles of all review reports submitted to the Minister — 97 to date — on its website.

In 2015–2016, the Commissioner was supported by 11 employees, together with a number of subject matter experts, as required. The office's expenditures were $2,034,877, which is within the overall funding approved by Parliament. To learn more about the Commissioner's office and its expenditures, please visit the website at: www.ocsec-bccst.gc.ca.

How the office's work has changed over 20 years

The quantity and depth of reviews being performed has expanded considerably over the years, increasing the amount of information available to support ministerial accountability and for informed parliamentary debate and public scrutiny. Over the last five years, Commissioners submitted 36 comprehensive review reports to the Minister (seven in 2011–2012, six in 2012–2013, seven in 2013–2014, nine in 2014–2015 and seven this year).

Reviews carried out over the last 20 years have produced 161 recommendations intended to promote compliance. CSE has demonstrated its commitment to implementing recommendations relating to privacy protection; since 1996, CSE has accepted and implemented 100% of the recommendations relating to privacy. This means that measures to protect the privacy of Canadians are continually being refined to adapt to the ever-changing technological and operational environment in which CSE must work.

Commissioners have had a significant positive impact on accountability, transparency and compliance of CSE activities. The office's work has led to CSE strengthening a number of fundamental policies and practices relating to privacy protection.

Commissioners instituted annual reviews of disclosures of Canadian identity information and privacy incidents to assess their inherent risk to privacy. Because ministerial authorizations permit the unintentional interception of a private communication – another risk to privacy – the authorizations and private communications are also reviewed each year.

Recommendations from Commissioners' reviews have also encouraged CSE to make significant revisions to practices and guidelines with respect to information sharing with second party partners. This includes clarifying language in information exchanges, clearly setting out privacy protection expectations for Canadian information shared with partners, and disseminating guidance to formalize and strengthen practices for addressing potential privacy concerns.

UPDATE ON CSE EFFORTS TO ADDRESS RECOMMENDATIONS

CSE has accepted and implemented, or is working to address, 94 percent (152) of the 161 recommendations made since 1997, including the four recommendations in reports this year. Commissioners track how CSE addresses recommendations and responds to negative findings as well as areas for follow-up identified in reviews. The Commissioner's office is monitoring 14 active recommendations that CSE is working to address — 10 outstanding recommendations from previous years and four from this year.

This past year, CSE advised the office that work had been completed in response to six past recommendations.

In its 2014–2015 ministerial authorizations year-end report, CSE implemented two recommendations to provide more precise information to the Minister:

- the fluctuation in the number of collected communications and unintentionally intercepted private communications that CSE acquires and retains is reported throughout the period that a ministerial authorization remains in effect, and not just at the end of the period (from the review of foreign signals intelligence ministerial authorizations summarized in the 2013–2014 annual report); and

- the difference is highlighted between private communications unintentionally intercepted under cyber defence activities — which often involve malicious code and a lowered or no expectation of privacy — and under foreign signals intelligence collection activities (from the review of information technology security activities conducted under ministerial authorization summarized in the 2014–2015 annual report).

CSE implemented two other recommendations by issuing policy guidance to:

- specify the circumstances and treatment of a particular type of one-end Canadian communication (also from the review of foreign signals intelligence ministerial authorizations summarized in the 2013–2014 annual report); and

- formalize and strengthen existing practices for addressing potential privacy concerns with second party partners (from the review of the activities of the CSE Office of Counter Terrorism summarized in the 2013–2014 annual report).

CSE addressed a recommendation from the review of its assistance to the Canadian Security Intelligence Service (CSIS) under section 16 of the *Canadian Security Intelligence Service Act* (summarized in the 2014–2015 annual report) by developing a caveat to attach to specific operational material that may be shared with second party partners to make clear that the material should not be used without the express authorization of CSE.

Finally, CSE has already adjusted the format of its Privacy Incidents File to address the Commissioner's recommendation in this year's report to make certain that future records contain adequate information to describe and document each incident in a thorough manner in order to demonstrate compliance and that appropriate actions have been taken to correct or mitigate any consequences of an incident. The Commissioner's office will assess the new record format as part of next year's annual review of privacy incidents.

The Commissioner has encouraged the Chief of CSE to hasten work on one important outstanding recommendation summarized in the 2013–2014 annual report: that the Minister issue a new general directive to CSE that sets out expectations for the protection of the privacy of Canadians when CSE shares foreign intelligence. While information sharing with second party partners is an essential component of CSE foreign signals intelligence and other activities, it has the potential to directly affect the privacy and security of a Canadian when a private communication or Canadian identity information is shared.

OVERVIEW OF 2015–2016 FINDINGS AND RECOMMENDATIONS

During the 2015–2016 reporting year, the Commissioner submitted seven classified reports to the Minister on his reviews of CSE activities.

The reviews last year were conducted under the Commissioner's authority:

- to ensure CSE activities are in compliance with the law — as set out in paragraph 273.63(2)(*a*) of the *National Defence Act* (NDA); and

- to ensure CSE activities carried out under a ministerial authorization are authorized — as set out in subsection 273.65(8) of the NDA.

The first review examined CSE support to the Canadian Security Intelligence Service (CSIS) under part (c) of CSE's mandate regarding a certain type of reporting involving Canadians, in particular, the risk such reporting presents to the privacy of Canadians.

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

Another review looked at a specific method used by CSE to collect foreign signals intelligence that regularly results in the highest number of private communications unintentionally intercepted.

As in previous years, the Commissioner conducted annual reviews of ministerial authorizations for foreign signals intelligence and cyber defence, including spot check examinations of private communications intercepted, used, retained and destroyed by CSE; of CSE disclosures of Canadian identity information; and of CSE incidents and procedural errors related to privacy.

The results

Each year, the Commissioner provides an overall statement on findings about the lawfulness of CSE activities. *This past year, all of the CSE activities reviewed complied with the law.*

As well, this year, the Commissioner made five recommendations to promote compliance with the law and strengthen privacy protection, including that:

- CSE keep the Minister informed of its activities to transmit to CSIS a certain type of reporting involving Canadians;
- CSE reconcile the discrepancies between its practices and the administrative requirements in the ministerial directive for a specific method of foreign signals intelligence collection;
- CSE issue guidance on marking and counting cyber defence private communications to ensure accuracy and consistency in reporting to the Minister;
- CSE make certain that future records in the Privacy Incidents File contain adequate information to describe and document each incident in a thorough manner; and
- the NDA be amended in order to clarify CSE's authority to collect, use, retain, share and disclose metadata.

20 years of effecting change through review

The Commissioner's reviews are an important factor in promoting a culture of compliance within CSE. The following are but a few examples of how the Commissioners' reviews have shaped CSE practices and strengthened the protection of the privacy of Canadians.

- Request memoranda for ministerial authorizations now contain enhanced explanations and rationales, so that the Minister can better understand what CSE is proposing that he authorize.
- CSE suspended certain metadata activities, that the Commissioner questioned, to re-examine how they are conducted.
- CSE implemented systems to better document and track requests from and disclosures to clients and partners of Canadian identity information.

- CSE enhanced its information management procedures, including centralizing its records management system and bolstering its rules for record retention and disposal, so that CSE can better document, track and provide evidence of its activities and compliance.

- CSE clarified authorities and revised procedures for the provision of operational assistance to Canadian law enforcement and security agencies.

- CSE sought input from the Commissioner's office when it made significant changes to the accountability framework and policies and procedures for cyber defence activities conducted under ministerial authorizations.

- CSE reports to the Minister relating to privacy are now more comprehensive, for example, relating to one-end Canadian communications and to information shared with and received from second party partners.

- CSE strengthened its policy for the active monitoring by CSE managers of the activities of employees relating to compliance and privacy protection, and ensuring employees are adequately trained on compliance and privacy requirements.

- Another success story demonstrates the importance of entrenching review body collaboration and cooperation in legislation, since security and intelligence agencies already work together. In a review of CSE operational assistance to the Canadian Security Intelligence Service (CSIS) under certain Federal Court warrants authorizing collection of intelligence on Canadians outside of Canada, the Commissioner recommended that CSE advise CSIS to further inform the Court of the nature of the assistance CSE was providing with the involvement of its second party partners. With the tabling of the Commissioner's public annual report, the Court became aware of the matter and found that it had no jurisdiction to approve the assistance, and that the failure to disclose certain information to the Court was the result of a deliberate decision to keep it in the dark. At the time, CSIS suspended its requests to CSE for assistance involving the second party partners.

HIGHLIGHTS OF REPORTS SUBMITTED TO THE MINISTER IN 2015–2016

1. Review of CSE support to the Canadian Security Intelligence Service under part (c) of CSE's mandate regarding a certain type of reporting involving Canadians

Background

The cooperative agreements that exist between the five eyes partners include a commitment to respect the privacy of each nation's citizens and to act in a manner consistent with each nation's policies relating to privacy. Nevertheless, it is recognized that each of the partners is an agency of a sovereign nation that may, in exceptional circumstances, derogate from the agreements if it is judged necessary for their respective national interests. In such exceptional circumstances, one of CSE's partners may acquire and report on information about a Canadian or a person in Canada. A partner may report on Canadians located outside of Canada who are known to be engaging in or supporting terrorist activities, for example, a report about a known Canadian "foreign fighter" that may be planning to return to Canada or to attack Canadians. When a partner does undertake an activity relating to a Canadian, the partner may acquire information that, in addition to meeting its own national security requirements, relates to the security of Canada and, as such, may be provided to the Canadian Security Intelligence Service (CSIS) in support of its mandate to investigate and advise government on threats to the security of Canada.

Foreign fighter

A foreign fighter can be defined as an individual who leaves her or his country of origin to join an insurgency abroad and whose primary motivation is ideological or religious, for example, women and men who have left Canada to join the terrorist group calling itself the Islamic State.

Prohibition on CSE targeting of Canadians

Under its *foreign signals intelligence mandate*, CSE is prohibited from directing its foreign signals intelligence collection activities at Canadians – wherever they might be in the world – or at any person in Canada. CSE cannot request any person to undertake activities on its behalf that CSE itself is prohibited from conducting. For example, it would be unlawful for CSE to ask a partner to target a Canadian, and CSE should not knowingly receive a report derived from an activity directed at a Canadian. However, this prohibition does not apply to CSE activities conducted under its *mandate to assist federal law enforcement and security agencies*. When acting under this mandate, CSE is instead subject to any limitations imposed by law on the requesting agency. CSE may, for example, support CSIS in its mandate to investigate threats to the security of Canada. In such cases, if the *Canadian Security Intelligence Service Act* allows CSIS to receive information about a Canadian, it would be lawful for CSE to assist CSIS in receiving it.

Prior to February 2015, the process to provide this kind of reporting to CSIS was manual and did not involve CSE. To help address the evolving terrorist threat and the increase in the number of foreign fighters, CSIS required a more timely mechanism to securely exchange information. To this end, CSIS requested CSE assistance under part (c) of CSE's mandate (paragraph 273.64(1)(*c*) of the *National Defence Act* (NDA)), to establish a mechanism for CSIS to receive and handle these reports via CSE's established channels.

The objectives of this review were: to acquire detailed knowledge of and to document CSE assistance to CSIS with respect to these reporting activities; to assess whether the activities complied with the law and ministerial direction; and to assess the extent to which CSE protected the privacy of Canadians in carrying out the activities.

The Commissioner conducted a review of all such reporting that CSE transmitted to CSIS from February 5, 2015, to May 15, 2015.

Findings

When undertaking activities under part (c) of its mandate, CSE is subject to any limitations imposed by law on the requesting agency (subsection 273.64(3) of the NDA). For the activities reviewed, CSE assistance to CSIS was, therefore, subject to the legal limitations enshrined in the *Canadian Security Intelligence Services Act* (CSIS Act). Section 12 of the Act sets out CSIS's mandate to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada."

In addition, as a government institution, all CSE activities are subject to the *Canadian Charter of Rights and Freedoms*, which protects a person's reasonable expectation of privacy, and ministerial direction requires CSE — when providing assistance — to manage information in a manner consistent with the *Privacy Act*.

The Commissioner found that CSE's activities to transmit these reports to CSIS were conducted in accordance with the law and with ministerial direction relating to the protection of the privacy of Canadians.

Specifically, the Commissioner was satisfied that:

- the activities consisted of technical and operational assistance that is permitted under part (c) of CSE's mandate;

- it was lawful for CSE to approve CSIS's request for assistance in the development of a mechanism to transmit these reports because it is within CSIS's mandate to receive reports that pertain to threats to the security of Canada as defined in section 2 of the CSIS Act; and

- all reports transmitted to CSIS during the period under review contained information that pertained to a threat to the security of Canada; CSIS had both the authority and the operational justification for obtaining the information relating to a Canadian.

CSE has procedures in place that provide sufficient direction to its employees respecting the protection of the privacy of Canadians for the activities. An operational plan contains clearly delineated roles and responsibilities, and restricts access to the reports to a very limited number of employees. CSE managers routinely and closely monitored the conduct of the activities to make certain the transmission of this reporting complied with relevant authorities. The office verified the monthly logs kept by CSE management to record which employees had viewed these reports and was satisfied with the written rationale given for their access.

The Commissioner noted that the CSIS request encompassed threats to the security of Canada defined in section 2 of the CSIS Act. In addition, although CSE — as an agent of CSIS — provided guidance to partners, the determination of what constitutes information pertaining to a threat to the security of Canada was left to those partners.

Conclusion and recommendation

Because the reporting transmitted to CSIS during the period under review contained information relating to Canadians, there is a risk to the privacy of Canadians associated with these activities. Therefore, **the Commissioner recommended** that CSE keep the Minister informed, on an annual basis, of its activities under part (c) of its mandate to transmit this kind of reporting to CSIS.

The Commissioner's office will continue to examine this assistance to CSIS to verify that CSE complies with the law, namely that the information relating to Canadians that CSE obtains and transmits to CSIS is consistent with CSIS's authority and operational justification, and that CSE takes sufficient measures to protect the privacy of Canadians in the conduct of the activities.

Subsequent to the completion of the review, officials from the office met with officials from the Security Intelligence Review Committee (SIRC) — which was commencing a review of CSIS activities relating to this subject — to describe the review methodology employed, to provide a summary of findings, and to outline areas of inquiry relating to CSIS that were outside of the Commissioner's mandate, but that SIRC could follow up on as it deems appropriate.

2. Review of CSE foreign signals intelligence metadata activities (Part 2)

Background

The Commissioner's office has been reviewing CSE metadata activities for quite some time. In fact, almost every review addresses metadata, which is fundamental to both CSE's foreign signals intelligence and cyber defence activities. Metadata helps CSE understand the global information infrastructure. It is also used by CSE to direct its activities at foreign entities located outside of Canada, and to mitigate the risk of intercepting the private communications of Canadians. An initial review focused on metadata was completed in 2006, and planning for a broad review of metadata started in 2012. The first part of this review, summarized in last year's annual report, included detailed information on CSE foreign signals intelligence metadata authorities and on certain activities relating to the use and disclosure of metadata. This second part of the review addressed specific foreign signals intelligence metadata activities that were set aside during the first part of the review in order to fully investigate incidents relating to CSE's failure to minimize Canadian identity information in certain metadata it shared with its second party partners. Minimization is the process by which Canadian identity information contained in metadata is rendered unidentifiable before it is shared.

Metadata

Paragraph 273.64(1)(*a*) of the NDA authorizes CSE to acquire and use information from the global information infrastructure for foreign intelligence purposes, including metadata. A 2011 ministerial directive provides additional guidance and places limits on CSE metadata activities. CSE describes metadata as the context, but not the content, of a communication. 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 Internet Protocol address, and network and location information.

The objectives of this review were: to examine specific CSE signals intelligence metadata activities to assess whether the activities complied with the law, ministerial direction, and CSE operational policies and procedures; to assess the extent to which CSE protected the privacy of

Canadians in carrying out the activities; to follow up on past findings of Commissioners; and to identify any areas for future in-depth review.

Findings

Three distinct metadata activities were examined.

First, certain metadata analysis activities undertaken for foreign intelligence purposes were examined. While it is a positive development that CSE updated its relevant operational policy, the Commissioner found that guidance on a specific metadata activity that involves Canadian identity information remains vague and should be clarified. The Commissioner's office will continue to examine the conduct of these activities as part of future activity-based reviews.

For these activities, we examined in depth a sample involving Canadian identity information conducted over a one-year period. While a small number of the activities raised questions about CSE authorities and the Commissioner noted inconsistencies in CSE documentation and record-keeping practices, he found that the activities were authorized and generally conducted in a manner consistent with ministerial direction and policy. While not fully satisfied with CSE's approach, the Commissioner did not make any recommendations to address the identified issues and irregularities because, subsequent to the period under review, CSE suspended indefinitely these particular metadata analysis activities in response to case law developments (*Canadian Security Intelligence Service Act (Re)*, 2012 FC 1437, relating to the application of "directed at"). It is positive to observe that CSE followed and modified its practices to address related jurisprudence.

Prior to its decision to suspend these activities, CSE did not meet its commitment to address a recommendation the Commissioner made in a February 2014 review of the activities of the Office of Counter Terrorism (OCT) to amend relevant policy to reflect current practices and to enhance record keeping. However, this can be explained by the short period of time between the OCT review and the suspension of the activities. As long as the suspension remains in effect, the Commissioner does not expect CSE to implement the recommendation.

Second, the Commissioner followed up on another recommendation he had made in the OCT review that CSE issue written guidance to formalize and strengthen existing practices for addressing potential privacy concerns with second party partners. The Commissioner accepts

CSE's responses to the issues identified in the OCT review and CSE issued guidance to operational employees to address cases where the privacy of Canadians may be at risk.

Third, the office examined certain network analysis activities involving metadata that help CSE, for example, to identify foreign threat actors, such as terrorist groups and cyber actors. The Commissioner had no questions about the authorities or policies for the activities and found that this analysis remains critical to the execution of CSE's foreign signals intelligence mandate.

Conclusion

The broad review of CSE use of metadata in a foreign signals intelligence context is now complete. In this part of the review, the Commissioner found no evidence of non-compliance, nor did he make any recommendations. The Commissioner's office will continue to review CSE use and disclosure of metadata, which is fundamental to all of its foreign signals intelligence activities. A third report, which will be completed in the coming year, is focused on CSE use of metadata in a cyber defence context.

Update on CSE failure to minimize certain Canadian identity information prior to it being shared with its second party partners

In January 2016, the Commissioner described the investigation of CSE metadata minimization deficiencies that led him, for the first time in the history of the office, to write to the Minister and to the Attorney General of Canada to inform them that he had found CSE to be non-compliant with the law, in particular, with sections 273.64 and 273.66 of the NDA, and, as a result, section 8 of the *Privacy Act*. He stated that while he believed the actions of CSE were not intentional, the agency did not act with due diligence when it failed to ensure that Canadian identity information was properly minimized prior to being shared with its second party partners. Subsequently, the Minister and the Attorney General accepted the Commissioner's recommendations relating to metadata, including that the NDA be amended to provide an explicit authority and a clear framework for CSE metadata activities.

The Commissioner discussed his findings with the Privacy Commissioner of Canada, Daniel Therrien, who has responsibility for oversight of the *Privacy Act*. Officials from the office were present when CSE explained the activities to Mr. Therrien's representatives, and were able to respond to questions from the Privacy Commissioner and his office. As issues of common interest arise, such collaboration with the Office of the Privacy Commissioner is expected to continue.

As it had done during the investigation, CSE continued to act in a forthcoming and transparent manner. Not only did it proactively suspend sharing of metadata with its second party partners after the deficiencies were discovered, but for the first time in its 69-year history, CSE provided a detailed technical briefing to the media, and put information on its website about its metadata activities.

At the time of writing, CSE had not yet resumed sharing this kind of metadata with its second party partners. The Minister and the Chief of CSE have provided assurances that CSE will continue to withhold this metadata from its second party partners until systems are in place to effectively protect the privacy of Canadians. The Commissioner expects to be informed by CSE before it resumes these activities, and the office will conduct a follow-up review to determine whether CSE complies with the law and effectively applies satisfactory privacy protections.

The office will also monitor CSE efforts to implement the two recommendations from the first report on metadata relating to: an updated ministerial directive that provides clear guidance related to the collection, use and disclosure of metadata in a foreign signals intelligence context; and CSE's use of its existing centralized records system to record decisions and actions taken regarding new and updated collections systems, as well as decisions and actions taken regarding minimization of metadata.

3. Review of a specific CSE foreign signals intelligence method of collection conducted under ministerial authorization

Background

This year the office completed an ongoing review of CSE foreign signals intelligence activities relating to a specific method of collection under ministerial authorization. This method of collection provides information about: foreign targets relating to international affairs, defence and security; metadata in support of target discovery and network analysis; and information about cyber threats. A 2004 ministerial directive set out specific requirements — including an approval framework and expectations relating to security and the management of the risk of operational activities — applicable to the sample that was selected for review. Subsequent to the period under review, the Minister issued an updated directive on these activities.

The objectives of the review were to assess whether the activities complied with the law, ministerial direction, and CSE operational policies and procedures, and to assess the extent to which CSE protected the privacy of Canadians in carrying out the activities.

Compared with other foreign signals intelligence methods of collection, these activities result in the highest number of unintentionally intercepted private communications recognized by CSE. One particular aim of the review was to better understand any potential impact of these activities on the privacy of Canadians.

In 2008, Commissioner Gonthier completed a comprehensive review of the activities. One finding of consequence was that CSE had not acted in accordance with all of the administrative requirements of the ministerial directive relating to security and risk management. As a result, he recommended that CSE reconcile the discrepancies between its practices and the directive's requirements. Commissioner Gonthier also identified deficiencies relating to insufficient and incomplete records. This review followed up on CSE actions to address the past recommendations and negative findings.

Findings and recommendation

For a number of reasons — including limited resources of the office and of CSE, employee turnover, and an unanticipated incident of high priority — this review, which had been ongoing for some time, could not be completed until now. In addition, CSE answers to the office's questions relating to this particular review were often delayed, incomplete or inconsistent, requiring officials to regularly follow up. However, in this context, based on the information reviewed and the interviews conducted, the Commissioner found no evidence of non-compliance with the law.

CSE has made improvements since the 2008 review. A number of issues remain outstanding, however, and the Commissioner made negative findings that are similar to those of his predecessor. CSE did not, for example, maintain an up-to-date plan to prevent and mitigate the potential negative impact of an unauthorized disclosure, as prescribed by the ministerial directive. Other documents have been in draft form for years, and contain insufficient information. The Commissioner is concerned that certain important documents relating to security and risk management remain incomplete. Therefore, like his predecessor, **the Commissioner recommended** that CSE reconcile the discrepancies between its practices and the administrative requirements in the ministerial directive.

The Commissioner found more than one instance where, because of a lack of clarity and explanation of key terms found in the approval framework of the ministerial directive, it could be argued that CSE should have sought specific approval prior to conducting an activity. The updated ministerial directive does, however, contain a new approval framework and additional guidance that the Commissioner's office will assess as part of a planned follow-up review.

In addition, the office sought statistics for the number of communications intercepted by CSE on behalf of, and sent to, its second party partners using this specific method of collection. Although CSE provided some information, its existing systems did not automatically track and record such information, and it was difficult and time-consuming for CSE to provide it. In a 2013 review of foreign signals intelligence ministerial authorizations, CSE indicated that it was working on a technical solution to more easily track the number of communications intercepted by CSE and sent to its second party partners. In a subsequent review, the Commissioner's office will follow up on CSE efforts to implement the

solution. Recording and regularly reporting to the Minister a wider range of statistical information relating to information shared with the Second Parties would support the Minister in his accountability for CSE.

Conclusion

Given the scope and nature of this method of foreign signals intelligence collection, the newer ministerial directive, the ongoing negative findings and the time that has elapsed since this review was started, at the time of writing, the Commissioner has already commenced another review of these activities, with a particular focus on CSE targeting activities, that is, the process and practices by which CSE determines that entities of foreign intelligence interest are foreign entities located outside of Canada. The Commissioner will monitor the timeliness of the responses from CSE.

4. Annual combined review of CSE foreign signals intelligence ministerial authorizations and private communications

Background

This is the sixth consecutive annual combined review of foreign signals intelligence ministerial authorizations. It is one way Commissioners fulfill the obligation under the NDA to review activities carried out under ministerial authorization to ensure they are authorized and to report annually to the Minister on the review.

The review encompassed three foreign signals intelligence ministerial authorizations in effect from December 1, 2014, to June 30, 2015, relating to three distinct methods of collection. This involved examining the authorization documents themselves and the activities described in the authorizations compared with previous years, to identify any significant changes to each method of collection and to the foreign signals intelligence collection program as a whole. It was an objective of the review to assess the impact of any changes on the risks to compliance and privacy, and, as a result, identify any subjects requiring follow-up review.

According to CSE policy, if an analyst whose functions are directly related to the production of foreign intelligence reports recognizes that an intercepted communication is a private communication, a communication of a Canadian located outside Canada, or contains Canadian identity information, and that the communication is not essential to international affairs, defence or security, then the analyst must, on recognition of these characteristics, process this communication for deletion. A communication deemed essential to international affairs, defence or security can be used in a CSE report or retained.

Ministerial authorizations

Ministerial authorizations shield CSE from the prohibition respecting the interception of private communications found in Part VI of the *Criminal Code*. It is a written document by which the Minister of National Defence authorizes CSE to engage in an activity or class of activities that risks the unintentional interception of private communications. Authorizations cannot be in effect for a period of more than one year. To learn more about the authorities for and limitations on CSE activities, please visit the office's website at: www.ocsec-bccst.gc.ca.

To verify compliance with the law and to assess the extent to which CSE protected the privacy of Canadians, the Commissioner examined the status of the 13 recognized foreign signals intelligence private communications that CSE had used or retained at the end of the 2013–2014 ministerial authorization period and of the 342 private communications that CSE had used or retained at the end of the 2014–2015 ministerial authorization period. The review included two spot check reviews of the 262 private communications used or retained by CSE during the periods of March 1, 2015, to April 30, 2015, and September 1, 2015, to October 31, 2015. CSE had no prior warning that the office was about to conduct the spot checks.

Findings

The Commissioner found that the 2014–2015 foreign signals intelligence ministerial authorizations met the conditions for authorization set out in the NDA, namely that:

- the interception will be directed at foreign entities located outside Canada;
- the 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.

There were no significant changes to the 2014–2015 ministerial authorizations and associated request memoranda to the Minister.

Accountability was enhanced respecting solicitor-client communications by incorporating measures to inform the Minister of cases when unintentionally intercepted solicitor-client communications containing foreign intelligence are retained, used or disclosed. CSE operational policy is not, however, fully consistent with the new process, and it should be revised. During the period under review, there were no solicitor-client communications used or retained by CSE; in fact, CSE has not used or retained a solicitor-client communication in the past five years. The office will continue to monitor and examine CSE retention or use of private communications, including any solicitor-client communications.

It is also positive that details were added to the ministerial authorizations and memoranda about what is an "essential" private communication, and to clarify the circumstances under which CSE may unintentionally intercept a private communication.

CSE implemented a recommendation of the Commissioner from 2013–2014 by modifying operational policy to specify who is responsible to approve specific foreign signals intelligence collection activities. CSE is also working on an updated policy for certain other activities, which the office will examine when it is issued.

CSE made changes to technology used for some of its foreign signals intelligence collection activities that continue to be challenged by unauthorized disclosures made by Edward Snowden in 2013. The disclosures resulted in the increased use of encryption and other countermeasures by foreign intelligence targets who hope to evade CSE and second party collection efforts.

Protection of Canadians' privacy

CSE is prohibited from directing its foreign signals intelligence and cyber defence activities at Canadians anywhere in the world or at any person in Canada. The foreign focus of CSE's work means that, unlike Canada's other security and intelligence agencies, CSE has limited interaction with Canadians. When CSE does incidentally acquire information relating to a Canadian, it is required by law to take measures to protect the privacy of the Canadian. The Commissioner's review of CSE activities includes verifying that CSE does not target Canadians and that CSE effectively applies satisfactory measures to protect the privacy of Canadians in all the operational activities CSE undertakes.

Respecting private communications, based on the information reviewed and the interviews conducted, the Commissioner was satisfied that:

- all private communications that were recognized by CSE were intercepted unintentionally and treated in accordance with CSE policies and procedures — nothing suggested that any of the private communications that were recognized by CSE during this period were intercepted intentionally, which would have been unlawful;

- all private communications used and retained by CSE were essential to international affairs, defence or security, as required by the NDA; and

- private communications that were non-essential were deleted. CSE did not retain private communications beyond the retention and disposition periods prescribed by its policy.

The Commissioner observed that, during the review period, the number of private communications recognized by CSE increased in comparison to previous ministerial authorization periods. This was a consequence of the technical characteristics of a particular communications technology and of the manner in which private communications are counted.

It is positive that the Chief's ministerial authorization year-end report to the Minister for 2014–2015 contained more comprehensive information respecting the number of private communications retained throughout the reporting period as the Commissioner had recommended, including an explanation of the reason for the increase during the period of March to April 2015.

Conclusion

CSE is taking action to implement recommendations from previous reviews relating to ministerial authorizations and private communications. This current review did not result in any recommendations. The Commissioner's office will continue to conduct annual reviews to verify that ministerial authorizations are authorized, and to conduct spot check reviews of one-end Canadian communications acquired and recognized by CSE to verify that CSE does not target Canadians and protects Canadians' privacy. Next year, to provide additional assurance, spot check reviews will be expanded to encompass a sample of other one-end Canadian communications acquired by CSE, including from second party partners.

One–end Canadian communication

Canadian means a Canadian citizen, a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act* or a body corporate incorporated and continued under the laws of Canada or a province.

One-end Canadian communication means a communication where one of the communicants is physically located in Canada (i.e., a private communication) or if one communicant is a Canadian physically located outside Canada.

5. Annual review of CSE cyber defence activities conducted under ministerial authorization

Background

To detect and protect against sophisticated cyber threats — including foreign state, criminal and terrorist threat actors — CSE may, on receiving a written request from a Government of Canada institution to conduct cyber defence activities, deploy measures to collect and analyze data from that client's computer systems or networks. Because these CSE cyber defence activities risk the interception of private communications, CSE must conduct these activities under the authority of a ministerial authorization.

Protection of Canadians' privacy

In cyber defence activities, data intercepted by CSE, including any private communications, may be used or retained only if it is relevant and essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

This annual review encompassed two cyber defence ministerial authorizations in effect from December 1, 2013, to November 30, 2014, and from December 1, 2014, to June 30, 2015.

The review included examining the cyber defence ministerial authorization documents and the activities they described to ensure the conditions for authorization set out in the NDA were met. The authorizations and activities were compared with previous years to identify any significant changes. An objective of the review was to assess the impact of any changes on the risks to compliance and privacy, and, as a result, identify any issues requiring follow-up review.

To verify compliance with the law and to assess the extent to which CSE protected the privacy of Canadians, the office examined a sample of intercepted data and recognized private communications intercepted pursuant to the ministerial authorizations that were used or retained on the basis that they were essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

The office selected and examined a sample of intercepted data relating to approximately 20 percent of the total number of cyber incidents identified in the 2013–2014 and 2014–2015 ministerial authorization periods. A cyber incident may involve one or more cyber events, and one or more private communications. Approximately 70 percent of the sample contained one or more recognized private communications. It is not possible to reveal the number of private communications used and retained by CSE relating to cyber defence activities because it would allow adversaries to assess CSE's capabilities. The office examined:

- the cyber events that made up the incidents;
- the malware, which is the software used by the threat actors, for example, to attempt to steal information from a computer system or to disrupt a network;
- CSE internal and external reports relating to the cyber threats;
- e-mails;
- analyst notes; and
- details contained in associated tools and databases, such as the rationale for the retention of a particular private communication, and information about the threat actor.

Another objective was to follow up on past findings and recommendations of Commissioners, including those in last year's in-depth review of cyber defence activities conducted during the 2009–2010 to 2011–2012 ministerial authorization periods.

Findings and recommendation

The Commissioner found that the 2013–2014 and 2014–2015 cyber defence ministerial authorizations met the conditions for authorization set out in the NDA, namely that:

- the interception was necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks;
- the information could not be reasonably obtained by other means;

- the consent of persons whose private communications may be intercepted could not reasonably be obtained;

- satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks was used or retained; and

- satisfactory measures were in place to protect the privacy of Canadians in the use or retention of that information.

Based on the information reviewed and the interviews conducted, the Commissioner found no evidence of non-compliance with the law as interpreted by the Department of Justice Canada. CSE's compliance validation framework for cyber defence activities — which includes extensive audit logging and monitoring of compliance with operational policies and procedures — provides evidence that CSE complied with legal requirements.

There were no significant changes to the ministerial authorizations and associated request memoranda to the Minister or to the conduct of the cyber defence activities that affected the risks to compliance or privacy.

The cyber defence ministerial authorizations contained changes similar to those made to the foreign signals intelligence authorizations to enhance accountability respecting solicitor-client communications. Cyber defence operational policy should also be amended to address the new requirements.

The Commissioner recognized the benefit of another change made in 2014–2015, which is to notify the Minister *when* CSE accepts a request from a Government of Canada institution to conduct cyber defence activities under the authority of a ministerial authorization. This will streamline CSE assistance to clients and support a timely response to cyber incidents (the 2013–2014 and previous authorizations required CSE to inform the Minister *before* it could accept such activities).

Recently, CSE started using a new specialized defensive technology to detect and mitigate malicious or abnormal cyber activity on Government of Canada client systems and networks. The technology appears to be generally consistent with existing CSE cyber defence activities, and CSE is applying the existing operational policies and procedures, compliance validation framework, and privacy protections

to the new activities. However, as a newly deployed technology, the new activities merit in-depth examination in a future comprehensive review.

Respecting private communications, based on the information reviewed and the interviews conducted, the Commissioner was satisfied that:

- all private communications that were recognized by CSE were intercepted unintentionally and treated in accordance with CSE policies and procedures — nothing suggested that CSE directed any of its cyber defence activities at Canadians or at any person in Canada;

- all private communications used and retained by CSE were essential to identify, isolate or prevent harm to Government of Canada computer systems or networks, as required by the NDA; and

- private communications that were non-essential were deleted; CSE did not retain private communications beyond the retention and disposition periods prescribed by its policy.

However, analysts were observed using two different methods for marking and counting cyber defence private communications. For accuracy and consistency in reporting to the Minister, **the Commissioner recommended** that CSE issue guidance on this subject.

All of the cyber defence private communications used or retained by CSE that were examined this year contained nothing more than malware or anomalous system and network activity.

As has generally been the case in the past, the private communications examined involved no exchange of any personal or other consequential information between the cyber threat actor and a Government of Canada employee or other Canadian. The Commissioner continues to question CSE's practice of treating all unintentionally intercepted one-end-in-Canada e-mails related to cyber defence activities as private communications and whether this accurately reflects the privacy risk and how that risk is portrayed to the Minister. The Commissioner noted the progress made in that CSE reporting to the Minister on private communications now highlights the important differences — including in the expectation of privacy — between private communications intercepted under foreign signals intelligence activities and under cyber

defence activities. However, the Commissioner remains of the view that a communication containing nothing more than malicious code or an element of social engineering sent to a computer system in order to compromise it *is not* a private communication as defined by the *Criminal Code*.

The Commissioner observed an increase in the proportion of incidents that did not contain a private communication. CSE explained that this resulted from increased use of certain techniques designed to reduce the risk of unintentionally intercepting private communications.

It is positive that the Chief's ministerial authorization year-end report to the Minister for 2014–2015 contained more comprehensive information respecting the number of recognized private communications acquired by CSE using particular cyber defence activities.

In last year's report, the Commissioner noted that CSE could improve some policies and procedures relating to the retention of certain private communications. However, in view of explanations provided in the context of this review, this suggestion was withdrawn; the Commissioner has no expectation that CSE should take any action on this subject.

CSE is taking action to address negative findings and to implement past recommendations, including:

- new guidance and regular communications to operational management and employees on changes to policy;
- a new mandatory policy course to enhance analyst understanding of policy requirements;
- enhanced record keeping through the planned deployment of a new cyber defence data repository; and
- more detailed and accurate marking and recording of private communications — including more comprehensive information about the justification for the retention of a private communication — which provided enhanced evidence of compliance and facilitated the conduct of the review.

Conclusion

The Commissioner made one recommendation to enhance policy relating to consistency in the marking and counting of private communications. The office will continue to conduct annual reviews of cyber defence ministerial authorizations and private communications to verify that the activities are authorized and that CSE does not target Canadians and protects Canadians' privacy. The office will monitor CSE actions to address issues identified in this review. This year, the Commissioner will complete a study of cooperation and information sharing between CSE's IT Security employees and its foreign signals intelligence employees to defend against cyber threats, which will be summarized in the 2016–2017 annual report.

6. Annual review of CSE disclosures of Canadian identity information, 2014–2015

Background

This is the seventh consecutive annual review of a sample of CSE disclosures of Canadian identity information — which includes any information uniquely relating to and that may identify a Canadian. The objective of the review was to verify that CSE, in its disclosures of Canadian identity information, complied with the law, ministerial direction and its policies and procedures, including assessing the extent to which it protected the privacy of Canadians.

For this year's review, the Commissioner's office selected and examined a sample of approximately 20 percent (225 requests) of the 1,126 requests from CSE's Government of Canada clients for disclosure of Canadian identity information contained in CSE reports. The requests were received during the period of July 1, 2014, to June 30, 2015. The sample included all government institutions that made a request during that period. The office also examined all 111 requests from second party partners and the six requests for disclosure to non-five eyes entities; one Government of Canada client made five requests and a second party made one request — which was denied — to share specified Canadian identity information with non-five eyes entities. It is important to note that the number of requests represent the number of instances that institutions or partners submitted separate requests for disclosure of identity information suppressed in reports, providing a unique operational justification in each case. One request may involve multiple Canadian identities, and one Canadian identity may be disclosed multiple times to different institutions or partners. Different types of Canadian identity information may have different levels of privacy interest.

Canadian identity information

Information that may identify a Canadian is generally suppressed – that is, replaced by a generic term, such as "named Canadian," as a measure to protect that Canadian's identity. CSE's Government of Canada clients and second party partners may request and receive this information if they have both the authority and operational justification to do so. The disclosure of Canadian identity information must be done in compliance with the *Privacy Act* and CSE's operational policy framework. To learn more about the authorities for and limitations on CSE activities, please visit the office's website at: www.ocsec-bccst.gc.ca.

Findings

The Commissioner was satisfied that:

- CSE disclosures of Canadian identity information complied with the law;
- the requesting Government of Canada client or second party partner had both the authority and operational justification for obtaining the information;
- CSE effectively applied the privacy protections contained in ministerial direction and in its operational policies and procedures;
- CSE acted in accordance with the Cabinet framework for addressing risks in sharing information with foreign entities that could result in the mistreatment of an individual; and
- no privacy incidents were identified that had not already been found and recorded by CSE in its Privacy Incidents File.

CSE is responsible for conducting a mistreatment risk assessment when it is the approval authority for the release of the information; however, other Government of Canada institutions continue to be responsible when the information is being released via their own channels. It is a positive development that in disclosures involving non-five eyes recipients CSE included a specific caveat to remind the requesting government client of its responsibility to conduct an assessment of the risks in sharing information with a foreign entity that could result in the mistreatment of an individual.

During the course of the review, the Commissioner informed the Chair of SIRC of information involving CSIS for any follow-up that SIRC may deem appropriate.

The automated information and records management system for requests from government clients continues to be effective. For a number of valid reasons, work on a similar system for processing second party partner requests has been delayed. The office will monitor changes to systems and processes for the disclosure of Canadian identity information.

Conclusion

The review did not result in any recommendations. The office will continue to conduct annual reviews of CSE disclosures of Canadian identity information to clients and partners to verify that CSE complies with the law and protects Canadians' privacy.

7. Annual Review of CSE's Privacy Incidents File and Minor Procedural Errors Record, 2015

Background

Since 2011, Commissioners have conducted an annual review of all incidents recorded by CSE that put the privacy of a Canadian at risk in a manner that runs counter to, or is not provided for, in its operational policies. CSE records in its Privacy Incidents File those incidents where privacy was breached. CSE uses the File to monitor and address incidents involving a privacy interest and to enhance processes and policies where required. The Minor Procedural Errors Record contains operational errors that occurred in connection with privacy-related information, but did not result in the information leaving the control of CSE or being exposed to external recipients who ought not to have received that information.

The Commissioner may investigate a material privacy breach, which according to government-wide policy is defined as a breach that involves sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals. The Commissioner also investigates privacy incidents in detail in the course of reviews of particular activities.

The objectives of this review were:

- to acquire knowledge of the privacy incidents, procedural errors and consequent actions taken by CSE to correct the incidents or mitigate the consequences;

- to acquire knowledge of any CSE operational material privacy breaches and associated corrective actions;

- to determine what incidents, if any, may raise questions about compliance with the law or the protection of the privacy of Canadians;

- to identify any trends or systemic weaknesses that might suggest a need for additional corrective action by CSE, changes to CSE processes or policies, or in-depth review by the Commissioner of a specific incident or activity; and

- to help evaluate CSE's policy compliance validation framework and monitoring activities.

The Commissioner examined all of the privacy incidents and the subsequent actions taken by CSE to address them. The incidents involved, for example: the unintentional sharing or inclusion in a report to, or in an e-mail exchange with, clients of unminimized Canadian identity information; unknowingly targeting a Canadian or a person in Canada; and unknowingly querying information related to a Canadian or person in Canada. Some of the incidents will be examined next year because CSE was continuing to take action to address them at the time of review.

Certain other incidents that relate to the transmission to CSIS of information from CSE's partners will also be investigated next year as part of the planned follow-up review of CSE support to CSIS under part (c) of CSE's mandate regarding a certain type of reporting involving Canadians.

The Commissioner also examined all of the minor procedural errors recorded by CSE in 2015. The procedural errors included, for example: the retention of Canadian identity information longer than permitted by policy; the disclosure of information relating to a Canadian to the wrong recipients within CSE; and sending Canadian identity information to external recipients, although in this instance, the error was corrected before the recipients accessed the information.

Findings and recommendation

Based on review of the Privacy Incidents File and the Minor Procedural Errors Record, answers to questions, and verification of information contained in CSE databases, the Commissioner found that CSE took appropriate corrective actions in response to the privacy incidents and minor procedural errors it identified in 2015.

The Commissioner had no questions about CSE's assessment that the privacy incidents it identified in 2015 did not consist of material privacy breaches, and the Commissioner agreed with CSE's assessment that the procedural errors it recorded were minor and did not result in privacy incidents.

CSE added information to the Privacy Incidents File to indicate whether the incidents consisted of a material privacy breach and whether the incidents required consideration or action by management. However, overall, the file contained less detail than in previous years. While CSE answered the office's questions about the incidents, it is important to document in the File sufficient information to demonstrate

compliance and that appropriate actions have been taken to correct or mitigate any consequences of an incident. Therefore, **the Commissioner recommended** that CSE make certain that its Privacy Incidents File contains adequate information to describe and document each incident in a thorough manner.

While reviewing reports referred to in one privacy incident, it was discovered that a small number of reports had not been cancelled or reissued as recommended and documented by CSE. As a result, CSE corrected the problem, and the office verified that the reports were cancelled.

CSE implemented a recommendation contained in the 2013 review of privacy incidents by revising its operational policy to clarify issues related to naming conventions and the suppression of Canadian identity information in foreign signals intelligence reports. The office will review the application of the new policy in the conduct of future activity-based reviews.

Conclusion

The recording and reporting of privacy incidents continues to be one effective measure used by CSE to promote compliance with legal and ministerial requirements, operational policies and procedures, and to enhance the protection of the privacy of Canadians. The review did not reveal any material privacy breaches, systemic deficiencies or issues that required follow-up review. According to CSE, it did not become aware of any adverse impact on the Canadian subjects of the privacy incidents. Commissioners will continue to investigate CSE privacy incidents and procedural errors. The office will continue to monitor developments relating to the findings and recommendation made in this review. It will also collaborate with the Office of the Privacy Commissioner on material privacy breaches, as appropriate.

A recurring theme: Amendments to the *National Defence Act*

On December 24, 2001, Bill C-36, the *Anti-terrorism Act*, came into force. This omnibus bill – enacted quickly following the events of September 11 – contained numerous elements affecting many government institutions and activities. The addition of Part V.1 to the *National Defence Act* (NDA) and the amendments to the *Official Secrets Act* were welcome developments, providing a legislative basis for both the activities of CSE and of the CSE Commissioner, setting out respective mandates, powers and relationships with Parliament and the Minister of National Defence. Shortly after enactment, however, the Commissioner's predecessors started voicing concerns about the application and interpretation of the NDA. Over the years, Commissioners have recommended eliminating ambiguities in the legislation and strengthening the accountability of CSE. Over a decade has passed since Commissioners first called for amendments that have yet to be made.

- The terms "activities" and "activity or class of activities" are used in the legislation in different contexts – relating to both CSE and to the Commissioner – and it has been recommended they be defined. Notably, CSE foreign signals intelligence ministerial authorizations permit CSE to unintentionally intercept private communications in relation to an "activity or class of activity" specified in the authorizations as a method of acquiring the foreign intelligence – the how. However, the authorizations could be interpreted as relating to a specific individual or subject – the who, or the what.

- The threshold required to satisfy the Minister that the conditions to be met before he may issue an authorization is unclear. The NDA should be amended to clarify that the conditions for authorization are based either on reasonable belief or on reasonable suspicion.

- When undertaking its mandated activities to acquire information, CSE may unintentionally intercept a private communication – as defined in the *Criminal Code* – but requires a ministerial authorization to do so. The term "acquire" is not defined in the NDA. The terms "intercept" and "interception" are also not defined in the NDA, nor referenced back to the *Criminal Code*. As a result, the point at which CSE "acquires" or "intercepts" information through its foreign signals intelligence collection activities is ambiguous. These terms are of operational significance to CSE foreign signals intelligence and cyber defence activities and of significance to the Commissioner's mandate to determine whether CSE complies with the law.

- The authority for CSE cyber defence ministerial authorizations refers to circumstances in the *Criminal Code* that apply to persons engaged in providing a telephone, telegraph or other communication service to the public who may intercept private communications while providing the service. An amendment to the NDA to refer to a different part of the *Criminal Code* – enacted since part V.1 of the NDA came into force – would remove any ambiguities respecting CSE's authority to conduct cyber defence activities that risk the unintentional interception of private communications.

- The Commissioner recommended an amendment to the NDA to provide explicit authority for CSE to collect, use, retain and disclose metadata. Inserting specific privacy protections for CSE metadata activities in the NDA like those found in ministerial direction and policy would enhance accountability and transparency.

- Finally, the NDA could be amended to provide the Commissioner with new functions to support the Minister in his accountability and control of CSE. For example, the Commissioner could provide an independent expert assessment of proposed ministerial authorizations, whether the conditions of authorization set out in the Act are met, and concomitant privacy protections. The Commissioner is already doing this work; only the timing would change, so that the Commissioner can provide an assessment to the Minister before the authorizations are signed, enhancing accountability. Reforms in this direction are proceeding in the United Kingdom.

Proceeding to clarify the law would support the government's commitments to strengthen accountability and transparency of CSE's legislation and activities, and the Commissioner maintains that the amendments recommended are not controversial.

COMPLAINTS ABOUT CSE ACTIVITIES

In 2015–2016, the 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 operational activities or without merit. There were no complaints about CSE activities that warranted investigation.

DUTY UNDER THE *SECURITY OF INFORMATION ACT*

The Commissioner has a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information — such as certain information relating to CSE activities — on the grounds that it is in the public interest. No such matters were reported to the Commissioner in 2015–2016.

ACTIVITIES OF THE OFFICE

The office's work on reviews requires a strong foundation, not only in its legislative authority and the technical and broadly based knowledge and skills of reviewers, but also in the government's understanding of the office's role and the public's understanding of the office's findings. The office's outreach, networking and learning activities strengthen its ability to deliver on the Commissioner's mandate.

Senate Standing Committee on National Security and Defence

This year, the Commissioner appeared twice before the Senate Standing Committee on National Security and Defence. His first appearance, in April 2015, was in relation to hearings being held on the *Anti-terrorism Act 2015* (Bill C-51), which was passed into law by Parliament under the previous government on June 9, 2015. Part 1 of the Bill, the *Security of Canada Information Sharing Act*, allows the sharing of information with the 17 specified Government of Canada institutions. The Commissioner advised the Committee that he had written to the Chair of the House of Commons committee examining this Bill, questioning why the existing review bodies were not also given explicit authority to share information among themselves. In reiterating his position stated in the letter, the Commissioner emphasized the importance of pairing the expansion of authorities governing information sharing among law

enforcement, security and intelligence agencies with an expansion of the ability of the respective review bodies to share and cooperate. He advised the Committee that the law should explicitly authorize cooperation between the office, the Security Intelligence Review Committee (SIRC) and the Civilian Review and Complaints Commission for the RCMP (CRCC).

Part 4 of Bill C-51 added measures to reduce threats to the security of Canada that were proposed for the Canadian Security Intelligence Service (CSIS). These measures have a direct impact on SIRC, which will review CSIS's performance in that regard. The Commissioner advised the Committee that these measures may also affect the office: it is possible that CSIS might request assistance from CSE in taking measures to reduce threats to the security of Canada and that CSE could provide technical and operational assistance to CSIS. The impact on the office of the Part 4 measures is unknown. However, should CSIS and CSE cooperate under these provisions, the Commissioner will monitor whether the office's resources need to be increased as a result.

The Commissioner's second appearance before the Committee in February 2016 addressed questions the Committee had concerning the 2014–2015 public annual report. (Because of the federal election call last summer, the report was not tabled in Parliament until this past January.) The Commissioner's remarks to the Committee dealt with the important issues that arose in the reviews conducted during the 2014–2015 fiscal year. The unclassified summary of these reviews can be found in the 2014–2015 Annual Report on the office's website.

Outreach, learning and networking

In April 2015 and in March 2016, the Commissioner spoke to University of Ottawa law students on the office's mandate and role. Throughout the year, he also continued to meet with a number of review colleagues in Canada and other senior government officials.

Once again, the office delivered presentations about its work to new CSE employees as part of CSE's foundational learning curriculum. As well, several office employees attended courses at CSE, which provided them with the same fundamental information given to CSE employees.

The office in-house counsel spoke to graduate students of the University of Sherbrooke on the Commissioner's authorities and activities. The office in-house counsel and Executive Director attended privacy

and security conferences in Vancouver and Victoria, B.C., in November and February. Office staff also attended conferences throughout the year dealing with international affairs, information technology security, national security, privacy and cyber security. These conferences were held by such organizations as the Canadian Defence Industries Association, International Association of Privacy Professionals, Canadian Military Intelligence Association, and the Canadian Association for Security and Intelligence Studies. Such events help employees to keep abreast of issues related to security, intelligence and privacy.

The office continued to provide support to the Canadian Network for Research on Terrorism, Security and Society (TSAS), initiated by a number of university academics.

Consulting with Canadian review bodies

The Review Agencies Forum is a meeting of representatives of the office, SIRC, 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. The forum met in September and March. In March, the Forum extended an invitation to senior government officials from the Privy Council Office and the Department of Public Safety who discussed ideas and approaches to ensuring accountability and cooperation.

The Commissioner continued to meet with the Chair of SIRC for general discussions regarding cooperation between the two organizations and the respective executive directors regularly discuss the coordination of basic elements of reviews of mutual concern involving both CSE and CSIS. As noted in the review section, several matters involving CSIS that arose during the review of joint activities of CSE and CSIS were referred to SIRC for any follow-up it deemed appropriate. Senior officials of the 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.

The Commissioner met with the Privacy Commissioner of Canada, Daniel Therrien, several times during the past year. Mr. Therrien and his provincial counterparts have a much broader area of responsibility, in terms of covering all public as well as private sector institutions within their respective jurisdictions, whereas the CSE Commissioner's mandate deals exclusively with CSE compliance and privacy protection.

Consulting with review bodies of other countries

In November, the Executive Director met with the visiting Senior Advisor of the Norwegian Oversight Committee to discuss review in general, including scope and methodologies. The office also had contact and exchanges with a number of review bodies in other countries.

WORK PLAN – REVIEWS UNDER WAY AND PLANNED

The Commissioner uses a three-year work plan, which 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 from the Chief of CSE on priorities and legal, policy and management issues of significance. To learn more about the Commissioner's risk-based and preventive approach to reviews, please visit the office's website at: www.ocsec-bccst.gc.ca.

Three reviews and one study started in 2015–2016 will be completed in 2016–2017: a focused review of metadata activities by CSE's IT Security section; a review of a particular method of collecting foreign signals intelligence conducted under a ministerial authorization and a ministerial directive; a review of CSE sharing of foreign signals intelligence with non-five eyes recipients, including mistreatment risk assessments; and a study of cooperation and information sharing between CSE's IT Security employees and its foreign signals intelligence employees to defend against cyber threats.

Other reviews planned to commence in 2016–2017 are: a follow-up review of a specific CSE foreign signals intelligence method of collection conducted under ministerial authorization with a focus on CSE targeting activities; a review of other CSE targeting activities conducted under

exceptional circumstances; a follow-up review of a certain type of reporting involving Canadians; and a follow-up review of CSE assistance to the Canadian Security Intelligence Service (CSIS) under part (c) of CSE's mandate and sections 12 and 21 of the *Canadian Security Intelligence Service Act* relating to the interception of the telecommunications of specified Canadians located outside Canada (formerly called Domestic Intercept of Foreign Telecommunications and Search warrants).

In addition, the Commissioner will continue to conduct annual reviews of:

- foreign signals intelligence and cyber defence ministerial authorizations, including spot check reviews of one-end Canadian communications acquired and recognized by CSE;

- CSE disclosures of Canadian identity information; and

- privacy incidents and procedural errors identified by CSE and the measures subsequently taken by CSE to address them.

ANNEX A: BIOGRAPHY OF THE HONOURABLE JEAN-PIERRE PLOUFFE, CD

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 of the Canadian Armed Forces. He retired as a Lieutenant-Colonel in 1976. He then worked in private practice with the law firm of Séguin, Ouellette, Plouffe et associés, in Gatineau, Quebec, specializing in criminal law, as disciplinary court chairperson in federal penitentiaries and also as defending officer for courts martial. Thereafter, Mr. Plouffe worked for the Legal Aid Office as office director of the criminal law section.

Mr. Plouffe was appointed a reserve force military judge in 1980, and then as a judge of the Quebec Court in 1982. For several years, he was a lecturer in criminal procedure at the University of Ottawa Civil Law Section. 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.

During his career, Mr. Plouffe has been involved in both community and professional activities. He has received civilian and military awards.

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

National Defence Act – Part V.1

Appointment of Commissioner

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

Duties

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

Annual Report

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

Powers of Investigation

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

Employment of legal counsel, advisers, etc.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

Directions

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council. . . .

Review of authorizations

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

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 discussion 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.