Communications
Security
Establishment
Commissioner

ANNUAL REPORT 2016–2017

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

© Her Majesty the Queen in Right of Canada as represented by the
Office of the Communications Security Establishment Commissioner, 2017

Catalogue No. D95
ISSN 1206-7490

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 2017

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, 2016, to March 31, 2017, for your submission to Parliament.

Jean-Pierre Plouffe

P.O. Box/C.P. 1474, Station "B"/Succursale « B »
Ottawa ON Canada K1P 5P6

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

I was honoured to be re-appointed last October for two more years as Commissioner. My re-appointment came in the midst of government initiatives for exploring options to strengthen the accountability of federal government agencies and departments that carry out national security activities.

These government efforts aim to reassure Canadians that the activities of these organizations to protect against terrorism and cyber attacks – including any additional powers they may be granted – do not unreasonably infringe on the privacy of Canadians. At the core of this debate is my mandate, as well as the mandates of my review colleagues at the Security Intelligence Review Committee and the Civilian Review and Complaints Commission for the RCMP. It is the role of existing review bodies both to encourage transparency and, where information must be kept secret, to ensure that effective, comprehensive review is conducted to bridge the information gap in public debate. We are instruments of accountability for our respective national security organizations and instrumental in helping to build public trust. To this end, I continue to disclose statistics, and encourage the Communications Security Establishment (CSE) to do so, to better inform public discussion and enhance public trust.

While my role as an external, independent reviewer focuses on CSE, a bill before Parliament proposes a committee of parliamentarians on national security and intelligence that would view security activities through a wide-angle lens. I welcome the greater involvement of parliamentarians, who would be cleared to receive secret information, in the overall accountability framework for national security activities. In my presentation to the House of Commons committee examining this bill, I outlined my concerns about avoiding duplication by defining roles clearly, and noted that review bodies should be mandated in the law to conduct reviews jointly where there is overlap, for example, when CSE works with the Canadian Security Intelligence Service. I look forward to working with the committee of parliamentarians when it becomes a reality.

The government also held nation-wide public consultations on national security. This allowed me to offer my perspective on topics that I have raised before, including the proposed committee of parliamentarians, the importance of collaboration among review bodies, and how they would work with the committee of parliamentarians. I have also commented on ministerial authorizations for

CSE, and disagree with calls for CSE to be subject to judicial warrants where the unintentional or incidental interception of private communications is concerned. Drawing on my decades of experience as a judge, that has now been informed by more than three years of review of CSE's activities, I reiterated a proposal to re-inforce the Minister's accountability for CSE. Enhanced privacy protection could be accomplished for ministerial authorizations if the CSE Commissioner assessed whether the authorizations meet the conditions set out in the *National Defence Act* before the Minister signs them, instead of after. In this way, "judicial eyes" would carry out independent, impartial and advance assessment of CSE's request for an authorization through scrutiny by the CSE Commissioner who must be a supernumerary or retired judge of a superior court and be knowledgeable about the issues pertaining to ministerial authorizations and privacy protections.

During my appearance before the House of Commons Standing Committee on National Defence in March, I highlighted four key issues that have my attention, two of which I have already referred to above. A third issue is the long overdue amendments to Part V.1 of the *National Defence Act*. We are at a juncture where clarity of the legislation that mandates CSE and sets out what it can and cannot do is critical because it implicates the privacy of Canadians. It is also critical to allowing parliamentarians and the public to know exactly what authorities and limitations CSE is operating under and to be reassured that mechanisms are in place to ensure powers are not abused, and if they are, that they will be brought to light and dealt with. The fourth strategic issue is the need to re-examine what information is able to be disclosed to the public in an effort to promote transparency. Transparency has been a cornerstone of my approach as Commissioner. There have been significant strides in this regard in the United Kingdom and in the United States. It is time to do likewise in Canada.

Progress on these broader issues will strengthen the capacity to carry out my primary mandate of reviewing CSE activities and will also help create a more comprehensive and effective framework for accountability, by holding to account those agencies and departments carrying out national security activities that are not yet subject to review.

As I move through my fourth year reviewing CSE, I am mindful more than ever of the importance of remaining abreast of operational and technological developments at CSE and of external developments affecting CSE, where the threat environment and technology are constantly evolving, as is the legal landscape. My review program in this next year will continue to focus on the adequacy of CSE measures to protect privacy, the role of metadata, and the sharing of information between CSE and its partners, both domestically and internationally. In the coming year as well, I look forward to meeting with my counterparts from the United States, the United Kingdom, Australia and New Zealand for discussions about what we might learn from each other's experiences in review and oversight, and how we might address accountability for intelligence

sharing among the agencies of our respective countries, in order to enhance public trust.

At the formal event last September marking the office's 20th anniversary year, the Minister of National Defence, who is responsible to Parliament for CSE, expressed appreciation for the independent reviews and recommendations he receives from the CSE Commissioner and the importance of this work in supporting his accountability for CSE. I look forward to continuing to serve in this critical role of reviewing the activities of CSE, to determine whether they comply with the law, ensuring there are robust safeguards to protect the privacy of Canadians, and contributing to the overall accountability of national security activities.

COMMISSIONER'S MANDATE AND REVIEW WORK

The Office of the Communications Security Establishment (CSE) Commissioner is an independent review body.

MANDATE

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

1. to review activities of CSE – which includes foreign signals intelligence and information technology (IT) security activities to support the Government of Canada – 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 *National Defence Act* requires that the CSE Commissioner be a supernumerary or retired judge of a superior court. The *National Defence Act* 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.

CONSIDERATIONS IN A REVIEW

The Commissioner's approach to reviews is both purposive – based on his mandate – and preventive. CSE activities include collecting foreign signals 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 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.

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 under various lawful authorities. 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.

In this challenging environment, reviewers need specialized knowledge and expertise to understand the many technical, legal and privacy aspects of CSE activities. 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.

After an activity is selected for review, the activity is assessed 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 *National Defence Act*, 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

Classified report on each review to the Minister: 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 findings and conclusions are free of any interference by CSE or any Minister.

Public reports annually to Parliament: 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 – 106 to date – on its website.

OFFICE RESOURCES

In 2016–2017, the Commissioner was supported by 11 employees, together with a number of subject matter experts, as required. The office's expenditures were $2,004,378, which is within the overall funding approved by Parliament. The office provides more detail on its expenditures on its website.

UPDATE ON CSE EFFORTS TO ADDRESS RECOMMENDATIONS

CSE has accepted and implemented, or is working to address, 95 percent (157) of the 166 recommendations made since 1997, including the five 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 16 active recommendations that CSE is working to address – 11 outstanding recommendations from previous years and five from this year.

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

Last year, in the office's review of CSE's assistance to the Canadian Security Intelligence Service (CSIS) under part (c) of CSE's mandate regarding a certain type of reporting involving Canadians (summarized in the 2015–2016 annual report), the Commissioner recommended that CSE keep the Minister informed, on an annual basis, of its activities under part (c) of its mandate to transmit reporting involving Canadians from Five Eyes partners to CSIS. CSE addressed this recommendation by providing to the Minister a summary of these activities.

CSE also addressed a recommendation from the office's review of CSE's foreign signals intelligence metadata activities (summarized in the 2014–2015 annual report). That review revealed that CSE's system for minimizing certain types of metadata was decentralized and lacked appropriate control and prioritization. CSE also lacked a proper record-keeping process. Therefore, the Commissioner recommended that CSE use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization of metadata involving Canadian identity information. CSE has advised that it has updated its information management processes for those areas responsible for collection systems with the objective of improving the record-keeping of decisions made and actions taken, particularly in regard to minimization. CSE will continue to examine these processes and improve as necessary through additional policy and business process changes. The Commissioner will also monitor these efforts.

The Commissioner reminded the Minister of 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 Canadians when a private communication or Canadian identity information is shared. The Minister has acknowledged that CSE is committed to addressing this as a priority.

The Minister has also acknowledged the Commissioner's encouragement for the government to hasten action on his 2015 recommendation to amend the *National Defence Act* and the Ministerial directive on metadata to provide explicit authority and more comprehensive direction for CSE's collection, use and disclosure of metadata.

OVERVIEW OF 2016–2017 FINDINGS AND RECOMMENDATIONS

During the 2016–2017 reporting year, the Commissioner submitted nine classified reports to the Minister on his reviews of CSE activities.

The reviews, and one study, 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 *National Defence Act*.

The first review examined the sharing of CSE's information with foreign entities other than the Five Eyes, in particular, the risk assessments conducted for deciding whether or not to send information to, or solicit information from, a foreign entity when doing so could substantially risk the mistreatment of an individual.

One review looked at CSE's collection activities in exceptional circumstances, such as, when CSE is obliged to acquire and report information involving Five Eyes nationals to support intelligence requirements that may not be satisfied otherwise.

Another review examined CSE's cyber defence metadata activities. This was the third and final part of a comprehensive review of CSE's metadata activities.

The Commissioner's office also completed a study of cyber threat information-sharing and -accessing activities between CSE's Foreign Signals Intelligence and Information Technology Security branches in order to acquire detailed knowledge of these activities as well as to identify any issues that may require follow-up review.

As in previous years, the Commissioner conducted annual reviews of ministerial authorizations for foreign signals intelligence and cyber defence, including spot check examinations of one-end Canadian communications (including private communications) acquired, used, retained and destroyed by CSE, and of CSE incidents and procedural errors related to privacy. The annual review of CSE disclosures of Canadian identity information will carry over into 2017–2018.

THE RESULTS

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

1. memoranda of understanding with foreign entities clearly specify CSE legal authorities and restrictions, including that CSE cannot receive, under its foreign signals intelligence mandate, information from the foreign entities acquired through activities that may have been directed at a Canadian or any person in Canada;
2. CSE issue overarching policy guidance to establish baseline measures for information exchanges with foreign entities;
3. CSE apply caveats consistently to all exchanges with foreign entities and that CSE use appropriate systems to record all information released;
4. because of the technical characteristics of certain communications technology, CSE reporting to the Minister on private communications contain additional information to better describe the private communications and explain the extent of privacy invasion – the current manner in which CSE counts the private communications provides a distorted view of the number of Canadians or persons in Canada that are involved in (i.e., are the other end of) CSE interceptions to obtain foreign intelligence under ministerial authorizations; and
5. because of the quasi-constitutional nature of solicitor-client privileged communications, CSE always seek and obtain written legal advice from Justice Canada concerning the retention or use of an intercepted solicitor-client privileged communication.

HIGHLIGHTS OF REPORTS SUBMITTED TO THE MINISTER IN 2016–2017

1. Review of CSE Information Sharing with Foreign Entities

BACKGROUND

CSE's ability to fulfil its foreign signals intelligence (SIGINT) collection and information technology (IT) security mandate rests, in large part, on building and maintaining productive relationships with its foreign counterparts. In addition to long-standing alliances with its Five Eyes partners, CSE information is also shared with other foreign entities.

The *National Defence Act* (NDA) does not contain explicit authority or any specific limitations respecting information sharing with foreign entities; such activities are implicitly authorized by the *National Defence Act*.

Sharing information with foreign entities is an integral part of the mandates of Canadian law enforcement and intelligence agencies, including CSE. To hold departments and agencies accountable for information shared outside of Canada, the Government of Canada enacted a *Framework for Addressing Risks in Sharing Information with Foreign Entities* that established a consistent approach across the government to conduct risk assessments for deciding whether or not to send information to, or solicit information from, a foreign entity when doing so could substantially risk the mistreatment of an individual. Under a corresponding directive from the Minister of National Defence, CSE is required to manage information sharing with foreign entities, assisted by policies that guide information-sharing practices, to ensure that sharing information does not give rise to a substantial risk of mistreatment.

This was the office's first focused review of the sharing of CSE's information with foreign entities other than the Five Eyes partners. For the period of February 1, 2010, to March 31, 2015, the office examined:

- the process for sharing foreign signals intelligence with foreign entities;
- the legislative and policy framework relating to sharing information with foreign entities;

- whether CSE acquired from foreign entities and/or disclosed to foreign entities private communications or information about Canadians;
- a sample of exchanges of information, including 161 mistreatment risk assessments that were conducted for information sharing; and
- existing formal agreements with foreign entities.

FINDINGS

The office concluded that CSE information sharing with foreign entities conducted during the review period complied with the law, the *Framework for Addressing Risks in Sharing Information with Foreign Entities* and ministerial direction.

CSE assesses and mitigates the risk of mistreatment whenever its information is being considered for sharing with foreign entities. The office examined 161 mistreatment risk assessments conducted by CSE, where CSE demonstrated that it had appropriately assessed and mitigated the risk of sharing the information, and applied the necessary approval and decision-making criteria. This included 35 cases where CSE shared information involving a substantial risk of mistreatment; CSE applied reasonable measures to mitigate the risk, including ensuring compliance with caveats and assurances from the foreign entities, or, in instances where risk could not be mitigated, appropriately weighed the risk of mistreatment against the risk of withholding the information, including, for example, information in relation to a threat to Canada's national security.

In the cases where CSE did not conduct a mistreatment risk assessment prior to sharing information, the office found no indications that an assessment should have been performed.

Information sharing with foreign entities assists CSE in fulfilling its mandate, particularly in support of counter terrorism, support to military operations, computer network defence and detecting threats against Canadian interests generally.

CSE disclosure of Canadian identity information to foreign entities is rare. Of the 161 mistreatment risk assessments examined, only five involved the disclosure of Canadian identity information to a foreign entity. In those few instances, CSE conducted the necessary risk assessment as well as assessed the privacy impact prior to approving the disclosure.

As CSE deals in information derived from signals intelligence, it is unlikely that CSE would receive information derived from mistreatment. Nevertheless, the office was satisfied that CSE took reasonable measures to determine that information it received from foreign entities was not the result of mistreatment.

However, the office found differences in how the risk assessment process was implemented by the responsible sections within CSE. CSE information sharing

procedures are managed by two different sections. While one section followed consistent protocols, the other maintained inadequate records for some cases and applied caveats to information exchanges inconsistently. By the end of the review period, however, that section had made substantial improvements in conducting risk assessments. CSE has since advised the Commissioner's office that it has revised and standardized the caveats to be used with all disclosures. The Commissioner will verify this in a future review.

During the review period, the office noted an absence of general policy guidance on information sharing with foreign entities. The office also noted an absence of specific policy guidance on conducting mistreatment risk assessments for sharing information with foreign entities. CSE issued a new policy on such risk assessments after the review period. Nonetheless, during the review period, CSE did have broader, established risk assessment policy and procedures to rely on, and did conduct regular assessments of its information-sharing arrangements to ensure that the behaviour of the partner remained consistent with Canada's foreign, defence or security interests.

While conducting the review, the office raised concerns that the formal agreements currently existing with certain foreign entities refer only in broad terms to measures to protect the privacy of Canadians. The office expected that CSE agreements would explicitly enumerate CSE legal authorities and restrictions, including that under its foreign signals intelligence mandate CSE cannot receive any private communications and other information derived from directing activities against a Canadian. CSE subsequently provided letters to these foreign entities describing its legal authorities and restrictions as an interim measure pending changes to the agreements. The Commissioner was satisfied with this approach; however, he emphasized the need to quickly conclude and/or amend all agreements with foreign entities at the first opportunity.

CONCLUSION AND RECOMMENDATIONS

In addition to **recommending** that formal agreements with foreign entities specify CSE legal authorities and restrictions, the Commissioner also **recommended** that caveats be applied consistently to all exchanges and that CSE use appropriate systems to keep a record of all information released. The Commissioner further **recommended** that CSE issue overarching policy guidance for information exchanges with foreign entities. The office will monitor CSE efforts to address the Commissioner's recommendations and will continue to regularly review CSE interactions with foreign entities, including information sharing and the conduct of mistreatment risk assessments.

As a result of this review, the office is conducting a separate review of CSE authorities for participation in a multilateral operational initiative currently focused on the terrorist threat to Western interests.

2. Review of CSE Collection Activities in Exceptional Circumstances

BACKGROUND

Last year, the office explained exceptional circumstances where cooperative agreements may not be respected by CSE's Five Eyes partners when the partners acquire and report information about Canadians located outside of Canada, for example, because they are known to be engaging in or supporting terrorist activities. This review examined the exceptional circumstances where CSE acquired information and reported on similar activities involving Five Eyes nationals.

CSE'S FIVE EYES PARTNERS

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

Paragraph 273.64(1)(*a*) of the *National Defence Act* (NDA) (part (a) of CSE's mandate) authorizes CSE to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities. Activities conducted under part (a) of CSE's mandate shall be:

- consistent with Government of Canada intelligence priorities;
- not directed at Canadians or any person in Canada; and
- subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

To fulfil its foreign signals intelligence (SIGINT) collection mandate, CSE also depends on productive relations with its foreign counterparts.

The cooperative agreements and resolutions that exist among the Five Eyes include a commitment by the partners to respect each other's laws by pledging to respect the privacy of each other's nationals. Consequently, CSE policies and procedures state that collection activities are not to be directed at Five Eyes nationals located anywhere, or against anyone located in Five Eyes territory.

Nevertheless, it is recognized that each of the Five Eyes partners is an agency of a sovereign nation that may deviate from these agreements if it is deemed necessary for their respective national interests. Accordingly, in such exceptional circumstances it may become necessary for CSE to acquire information involving Five Eyes nationals or a foreigner on Five Eyes territory.

CSE's longstanding relationships with its Five Eyes partners are particularly important because they enable the alliance to collaborate in pursuit of common priorities, such as identifying extremist travellers headed to, or who have arrived in, conflict zones to join terrorist groups or other organizations such as Daesh, and whose possible return to their home countries may pose a threat.

EXTREMIST TRAVELLERS

An extremist traveller (also known as "foreign fighter") can be defined as an individual who is suspected of travelling abroad to engage in terrorism-related activity, for example, women and men who have left Canada to join the terrorist group calling itself the Islamic State.

This is the first time these types of activities have been reviewed by the Commissioner's office. Therefore, this review was an opportunity to acquire detailed knowledge of these activities and the circumstances in which they would occur. The objectives of the review remained familiar: to determine whether these activities complied with the law and ministerial direction related to intelligence priorities, as well as to ensure adequate measures are being taken to protect the privacy of Canadians as these activities are carried out.

For the period of January 2015 through August 2016, the office examined:

- all CSE-initiated activities involving Five Eyes nationals or a foreigner on Five Eyes territory;
- related CSE authorities and policies, databases and systems;
- operational justifications; and
- any associated reporting.

FINDINGS

In all 11 cases where CSE's activities involved Five Eyes nationals located anywhere or anyone located in Five Eyes territory during the period under review, the office found that the activities complied with the law, were not directed at Canadians or any person in Canada, and were consistent with Government of Canada intelligence priorities. Further, these types of activities are rare and present a low risk to the privacy of Canadians.

This review also confirmed that the criteria set out in CSE policy were met – in addition to meeting the requirements under part (a) of CSE's mandate, these particular collection activities occurred under only very limited and specific circumstances, such as meeting a Government of Canada intelligence priority that is otherwise unable to be met.

In 2015, CSE updated its policy to more effectively respond to operational requirements and emergencies, and formalized certain existing practices. Upon examination, the office suggested the policy needed further clarification. The review also found that CSE analysts applied the policy inconsistently, for example, in the way that the required request forms were filled out or how much detail was provided. CSE indicated it is working to address these findings to clarify the policy as well as ensure its proper application.

CONCLUSION

Given the limited number of these types of activities and the low risk to the privacy of Canadians, the office will not review them regularly, but will monitor the extent and nature of these activities.

While not directly related to this review, the Commissioner again encouraged the Minister to address an outstanding July 2013 recommendation to issue a new ministerial directive to provide general direction to CSE on its foreign signals intelligence information-sharing activities with its Five Eyes partners. That review raised the broader issue of the relationships and agreements among partners. The office was informed that a new ministerial directive is being developed that will explicitly acknowledge the risks associated with this type of sharing, given that CSE cannot, for reasons of sovereignty, demand that its Five Eyes partners account for any use of such information. The Commissioner will continue to monitor developments.

3. Review of CSE Cyber Defence Metadata Activities

BACKGROUND

This is the third and last part in a series of recent reviews focused on metadata; the first two parts – reported in the Commissioner's last two annual reports – addressed foreign signals intelligence (SIGINT) metadata activities. This review focused on CSE's use of metadata in cyber defence activities. The objectives of the review were to determine whether CSE's metadata activities complied with the law and were not directed at Canadians or any person in Canada, as well as to determine whether CSE effectively applied satisfactory measures to protect Canadians' privacy. The office examined CSE operational policy and procedures, received technical briefings and demonstrations, and interviewed CSE technical and operational staff.

CSE conducts cyber defence metadata activities under the authority of paragraph 273.64(1)(*b*) of the *National Defence Act* and cyber defence ministerial authorizations. The 2011 ministerial directive on metadata defines metadata as "information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content." CSE may acquire cyber defence metadata from its own sources, from domestic and international partners, and from owners of computer systems of importance to the Government of Canada, which includes critical infrastructure. CSE uses metadata under this part of its mandate to identify and mitigate sophisticated foreign malicious cyber threats and to help protect computer systems of importance to the Government of Canada.

CYBER DEFENCE

CSE conducts cyber defence activities. Cyber defence helps protect Government of Canada systems from foreign states, hackers and criminals. CSE tracks threats from around the world, monitors government networks to detect cyber threats, and works with government departments to defend and strengthen systems that have been compromised. CSE helps protect information of value to the government, including personal information, from theft.

FINDINGS

The office confirmed that its past reviews have revealed what there is to know about CSE cyber defence metadata activities. No new activities or specific risks of non-compliance or to privacy were identified. Metadata remains essential to CSE's cyber defence mandate.

CSE cyber threat detection capabilities copy and store a subset of Government of Canada client network data – including metadata – to identify and permit ongoing analysis of anomalous and sophisticated foreign malicious cyber events. Similarly, CSE acquires only a small proportion of the data passing through its cyber defence sensors. It then extracts metadata from the data acquired and uses it, for example, to contextualize the threat and any malware, and to develop mitigation advice for the client and other Government of Canada institutions.

Cyber defence activities acquire data from Government of Canada networks relating to cyber events. It is to be expected that CSE cyber defence activities may involve metadata relating to Canadians because the activities involve data from Canadian networks located in Canada – acquired either by CSE under a ministerial authorization, or by system owners and Government of Canada institutions under *Criminal Code* and *Financial Administration Act* authorities and subsequently disclosed to CSE.

However, previous reviews have demonstrated that the cyber defence data used and retained by CSE generally involves no exchange of any personal or other consequential information between the foreign cyber threat actor and a Government of Canada employee or other Canadian. CSE cyber defence activities generally acquire communications containing nothing more than malicious code or an element of "social engineering" sent to a computer system in order to deceive the recipient and compromise the system.

SOCIAL ENGINEERING

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

Even so, the privacy protection measures CSE applies to a private communication are also applied to cyber defence metadata that could identify a communicant or the communication in Canada – for example, the "from" and "to" fields of an e-mail, or an Internet protocol address linked to the communication. The office verified that cyber defence metadata relating to a Canadian is used or retained by CSE only if it is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks, for example, when it is necessary to the understanding of foreign malicious cyber activity, capabilities or intentions, and for the purpose of mitigating the threat.

Based on the information reviewed, the technical briefings and demonstrations received, and the interviews conducted, the Commissioner found no evidence of non-compliance with the law. CSE did not direct its cyber defence metadata activities at Canadians or any person in Canada.

CSE's cyber defence metadata activities are consistent with the requirements and limitations set out in the ministerial directives concerning accountability and the privacy of Canadians.

The Commissioner was satisfied that a comprehensive series of CSE operational policies and procedures relating to the conduct of cyber defence activities provide sufficient guidance related to cyber defence metadata activities. This includes policies and procedures on: using system owner data; accessing, handling and sharing data; and the writing and managing of cyber defence reports. Interviews and observations of information technology security managers and employees demonstrated that they are knowledgeable about the policies and procedures. CSE's cyber defence activities are also subject to internal audit and continuous compliance monitoring.

CONCLUSION

The Commissioner made no recommendations as a result of this review; however, he encouraged the Government of Canada to hasten work in response to recommendations he made in 2015 – supported by the Privacy Commissioner of Canada – to amend the *National Defence Act* and the ministerial directive on metadata to provide explicit authority and more comprehensive direction for the collection, use and disclosure of metadata in a foreign signals intelligence context. These amendments should include explicit authority and privacy protections for all CSE metadata activities, including cyber defence activities under part (b) of CSE's mandate.

The Commissioner's office will continue to examine CSE metadata activities in an information technology security context as part of regular reviews of cyber defence ministerial authorizations, private communications used and retained by CSE, and CSE disclosures of Canadian identity information to Government of Canada and international partners.

4. Study of Sharing and Accessing of Cyber Threat Information Between CSE's SIGINT and IT Security Branches

BACKGROUND

The complexity of the global information infrastructure is increasing exponentially as more people, information and infrastructure become connected to it. While expansion offers many benefits, information technology (IT) systems are also vulnerable for many reasons: they are generally not designed with security in mind, they are interconnected, they are used to store large amounts of easily copied and valuable information, and security often depends on user authentication that can be easily compromised (e.g., a single password). The division between information and the underlying technology used to process the information is blurring; an attack on one is often inseparable from an attack on the other.

Cyber threats are characterized by rapidly increasing complexity, speed, scale, intensity and portability. Wireless and anonymous connectivity to the global network is becoming the default. Not only can cyber threats affect electronic information and information infrastructures of importance to the Government of Canada, but they can also be used by sophisticated government-sponsored actors that pose a threat to national security.

Deliberate threats include: unauthorized access or disclosure, malware, denial of service attacks, hijacking of computers, spoofing, phishing, tampering and threats from insiders. Accidental threats and natural hazards also exist.

In this dynamic environment, the Foreign Signals Intelligence (SIGINT) and IT Security branches of CSE have worked increasingly closely to exchange data and analysis on cyber threats to and compromises of electronic information and information infrastructures of importance to the Government of Canada. In 2009, CSE created the Cyber Threat Evaluation Centre (CTEC) to ensure greater coordination and synchronization between the IT Security branch and the SIGINT branch. CTEC also acts as the Government of Canada entry point into CSE for all matters related to cyber defence.

In October 2010, Canada's Cyber Security Strategy was released and CSE received funding that was put toward enhancing information-sharing capabilities between the SIGINT and IT Security branches on cyber threat information.

The SIGINT and IT Security branches operate under their respective parts of CSE's legislated mandate. The activities of CSE's SIGINT branch are undertaken pursuant to paragraph 273.64(1)(*a*) of the *National Defence Act* (part (a) of CSE's mandate):

to acquire and use information from the global information infrastructure for foreign intelligence purposes. The activities of CSE's IT Security branch are undertaken pursuant to paragraph 273.64(1)(*b*) of the *National Defence Act* (part (b) of CSE's mandate): to provide advice, guidance and services to help protect electronic information and information infrastructures of importance to the Government of Canada. One of IT Security's primary functions is to place sensors on Government of Canada network gateways for detecting cyber threats. Data related to those threats can then be passed to SIGINT to be used for lead purposes in gathering foreign intelligence on hostile actors.

Under the *National Defence Act*, the IT Security and SIGINT branches are prohibited from directing their activities at Canadians or any person in Canada, and they must take measures to protect the privacy of Canadians. However, exchanging and accessing information related to cyber threats may include private communications and Canadian identity information, which is one of the reasons the Commissioner's office undertook this study. It was undertaken under the Commissioner's authority as set out in paragraph 273.63(2)(*a*) of the *National Defence Act*.

The objectives of the study were: to acquire detailed knowledge of and to document the sharing and accessing of information related to cyber threat activities between CSE's SIGINT and IT Security branches; to observe how well CSE employees know the relevant authorities; to determine what activities, if any, may raise issues about risk to compliance with the law or the protection of the privacy of Canadians; and, as appropriate, to identify any issues that may require follow-up review.

OBSERVATIONS

When analyzing cyber threat activities, the SIGINT and IT Security branches share tools and workspaces; therefore, both cyber teams are given access to data acquired under parts (a) and (b) of CSE's mandate. This is on purpose: it ensures that both areas are able to conduct comprehensive analyses of cyber threats. Restrictions on access to both part (a) and part (b) data are implemented by the parameters detailed in both SIGINT and IT Security policies and procedures. Analysts from both areas must follow all related policies and procedures when handling each other's data. Analysts within SIGINT who are assisting IT Security with cyber threats are given approval and authorization to conduct cyber defence activities under part (b) of CSE's mandate.

Each of these CSE employees is trained and must pass the policy tests applicable to their mandate responsibilities and the mandate responsibilities of their peers. Due to the complexities of policies and procedures, designated individuals supervise and direct the implementation of these guidelines in an operational environment.

Although each employee is trained to perform work assigned under either part (a) or (b) of CSE's mandate, it is the application of the policies, the separation of IT Security and SIGINT data, and the use of distinct analytic tools that are the focus for the supervisors. By assigning tasks under only part (a) of CSE's mandate or part (b), the supervisor is able to monitor compliance.

According to CSE, data that IT Security shares with SIGINT may be used only for the purpose for which it was collected, that is, cyber defence. CSE SIGINT and IT Security analysts generally work independently because legal and policy requirements on the use, retention and disclosure of information differ, depending on the applicable mandate. As such, the disclosure of personal information between SIGINT and IT Security can be achieved only after specific legal requirements are met.

CSE's two operational branches can share personal information under paragraphs 8(2)(*a*) and (*b*) of the *Privacy Act*. The disclosure of personal information under paragraph 8(2)(*a*) is permitted because it is undertaken for a purpose that is the same as, or consistent with, the purpose for which the information was originally obtained (identifying foreign cyber threat activities, be it for foreign intelligence purposes or cyber defence purposes). The disclosure is also permitted pursuant to paragraph 8(2)(*b*) in that the information is disclosed for a purpose in accordance with an Act of Parliament (paragraph 273.64(1)(*a*) or (*b*) of the *National Defence Act*).

The Commissioner is of the view that the cyber threat information-sharing and -accessing activities between SIGINT and IT Security are consistent with *National Defence Act* and *Privacy Act* authorities, and that the information currently shared between the branches poses a minimal risk to the privacy of Canadians.

Cyber threat information collected and disseminated within CSE poses less of a risk to privacy than other types of information collected under part (a) of CSE's mandate. The Commissioner's office has repeatedly questioned CSE's practice, while conducting cyber defence operations under ministerial authorization, of treating all unintentionally intercepted one-end-in-Canada e-mails as private communications as defined in the *Criminal Code*. As also noted in this year's IT security ministerial authorization review, the Commissioner believes that a communication that consists of nothing more than malware and/or an element of social engineering, sent by a cyber threat actor located outside Canada, where it is reasonable to expect that the purpose of the communication is to compromise Government of Canada computer systems or networks, is not a private communication within the meaning of the *Criminal Code*.

Furthermore, in cyber defence activities, the concern is not the content of the communication but rather information that helps in attributing cyber threat information to the perpetrator and threat vector. It is rare that the content of any one communication would provide information in determining the origin of a threat vector or the necessary mitigation measures to be applied. However, this cyber threat information may contain Canadian identity information that is necessary to CSE's cyber security mandate.

Whenever Canadian identity information may be acquired during these activities, CSE has measures in place to protect the privacy of Canadians – in policy and procedure, as well as being built into the technology. The study found that both SIGINT and IT Security have comprehensive policies and procedures in place relating to these activities and that compliance monitoring occurs.

While conducting this study, the office requested from CSE a relevant legal opinion. Contrary to longstanding practice, CSE did not provide the opinion, choosing instead to provide a summary. Historically, CSE has always provided the Commissioner's office with access to its legal opinions with the understanding that solicitor-client privilege is not waived. However, the Commissioner appreciates that CSE has, since then, provided the office with legal opinions relevant to other ongoing reviews. It is essential, in examining activities for compliance with the law, to know how the law is being interpreted, and whether and how it is being applied by the agency.

CONCLUSION

The study provided the Commissioner's office the opportunity to learn the intricacies of information exchanges between the SIGINT and IT Security branches, and to determine whether there are areas or activities that require follow-up review.

The Commissioner did not have any outstanding questions about compliance with the law or the protection of the privacy of Canadians. The study did not identify any new issues requiring a follow-up review. However, CSE use of a repository and tool for cyber threat detection is being examined in more detail in the context of an ongoing review.

The office will continue to examine cyber threat information-sharing and -accessing activities between the SIGINT and IT Security branches in reviews of SIGINT and cyber defence activities conducted under ministerial authorization and of disclosures of Canadian identity information.

5. Annual Review of Privacy Incidents and Procedural Errors Files

BACKGROUND

CSE reports and documents any incidents that are associated with its operational activities, or those of its Second Party partners, where the privacy of a Canadian may have been put at risk contrary to CSE operational policy or procedures on protecting the privacy of Canadians or any person in Canada.

Such incidents, along with corrective actions taken, are recorded in one of three files, depending on where the incident occurred and its potential to cause harm. These are CSE's Privacy Incidents File (PIF), the recently created Second Party Incidents File (SPIF) and the Minor Procedural Errors File (MPEF).

The PIF is a record of incidents attributable to CSE involving information about a Canadian or any person in Canada that was handled in a manner counter to CSE privacy policy and exposed to external parties who ought not to have received it. This type of mishandling is labelled a "privacy incident." The SPIF is a record of privacy incidents that are attributable to Second Party partners. These incidents may be identified by the partners themselves, or by CSE. The MPEF is a record of instances where CSE improperly handled information about a Canadian but the information was contained within CSE and was not exposed to external parties.

The office's annual review of the PIF, SPIF and MPEF focuses on incidents not examined in detail in the course of other reviews. The review is an opportunity to identify trends or systemic weaknesses that might suggest a need for corrective action, changes to CSE's procedures or policies, or an in-depth review of a specific incident or activity. For example, the office could challenge whether or not one of the incidents constituted an operational "material privacy breach," which government-wide policy defines 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.

Besides reviewing the procedural errors, incidents and subsequent actions taken by CSE to correct the incidents or mitigate the consequences, the objectives of the review were: to examine any CSE operational material privacy breaches and CSE's associated corrective actions; to determine if any incidents raise questions about compliance with the law or the protection of the privacy of Canadians; and to evaluate CSE's policy compliance validation framework and monitoring activities in this context.

While such reviews usually cover a full calendar year, this review covered six months: January 1, 2016, to June 30, 2016. Future reviews of these files will cover a 12-month period, but from July 1 to June 30, rather than the calendar year. The period was changed to alleviate the office's reporting workload at the end of the fiscal year.

The office examined all 55 privacy incidents in the PIF and SPIF and subsequent corrective actions taken by CSE to address them. The office also examined the six minor procedural errors documented by CSE during the review period.

FINDINGS

The privacy incidents included, for example, the inadvertent sharing or inclusion in a report of Canadian identity information without suppressing the information in accordance with CSE policy, as well as the unintentional targeting or database searches for information relating to individuals not previously known to be Canadian or persons in Canada. In all instances, the reports were cancelled or corrected with the identities properly suppressed, or CSE deleted any associated intercepted communications or reporting.

CANADIAN IDENTITY INFORMATION

Canadian identity information refers to information that may be used to identify a Canadian person, organization or corporation, in the context of personal or business information. Canadian identity information includes, but is not limited to, names, phone numbers, e-mail addresses, Internet protocol addresses and passport numbers. When CSE includes Canadian identity information in a report, this information must be suppressed and replaced with a generic term, such as "named Canadian," as a measure to protect that Canadian's identity.

The review found two instances where reports containing unsuppressed Canadian identity information had been cancelled but had not been deleted from CSE databases. CSE therefore manually purged these reports from the system. Two incidents involved the sharing within CSE of reporting on information about a Canadian or a person in Canada that a Five Eyes partner provided to the Canadian Security Intelligence Service via CSE and that should have had a limited internal distribution. (The office's review of CSE's assistance to the Canadian Security Intelligence Service regarding this type of reporting was highlighted in last year's annual report). CSE's response to these two incidents included providing remedial training to those involved, as well as those likely to encounter such reporting.

In regard to the minor procedural errors, the Commissioner agreed with CSE that all of these were minor and did not constitute "privacy incidents." These procedural errors included, for example: a folder that contained unviewed data, and possibly private communications, that was retained beyond the applicable retention schedule; Canadian identity information being accidentally released to unintended recipients within CSE; and limited cyber defence data being briefly accessible to – but never seen by – certain non-Canadians. The privacy impact of such incidents is considered less severe since they were contained internally and addressed prior to the information being accessed by anyone outside CSE.

Based on a review of the three files, answers to questions posed to CSE, and examination of associated CSE records, the Commissioner found that in all instances, CSE took appropriate corrective action, including, where feasible, measures to preclude similar occurrences in the future.

According to government-wide policy, it is a department's or agency's responsibility to identify material privacy breaches. CSE did not identify any operational material privacy breaches as having occurred during the period under review. The Commissioner agreed that the incidents listed in the PIF/SPIF for this review period did not constitute material privacy breaches.

This review benefited from the additional information CSE included to thoroughly describe and document each incident, in response to the Commissioner's recommendation in last year's review of these files. The file entries were notably more comprehensive, with detailed descriptions and timelines of the incidents, the reasons that the incidents occurred, mitigative actions and any planned follow-up activities. The segregation of CSE incidents and Second Party incidents provided additional clarity. Another development further enhancing measures to protect the privacy of Canadians was CSE's new policy instrument setting out the procedures for CSE employees to follow in handling privacy incidents and procedural errors.

CONCLUSION

This review did not identify any material privacy breaches, systemic deficiencies or issues that require follow-up review that was not already planned. According to CSE, it did not become aware of any adverse impact on the Canadian subjects of any of the privacy incidents.

The Commissioner was satisfied that CSE responded appropriately to privacy incidents and minor procedural errors identified during the review period.

The recording and reporting of privacy incidents and minor procedural errors continues to be one effective means used by CSE to promote compliance with legal and ministerial requirements, and with operational policies and procedures, as well as to enhance the protection of the privacy of Canadians. The improvements made in relation to this reporting and to associated file structures should further strengthen privacy protections.

The Commissioner made no recommendations. However, he encouraged CSE to seek a practical means to ensure that cancelled reports containing Canadian identity information are promptly removed from CSE databases and that a confirmation of the cancellation occurs. Also, this is the second consecutive PIF review that found inappropriate distribution of Canadian identity information in relation to a Five Eyes partner report involving a Canadian or a person in Canada. The Commissioner committed to including these incidents in the upcoming follow-up 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.

6. Annual Review of CSE Cyber Defence Activities Conducted Under Ministerial Authorization

BACKGROUND

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

Subsection 273.65(3) of the *National Defence Act* permits the Minister to authorize CSE in writing – for the sole purpose of protecting the computer systems or networks of the Government of Canada from cyber threats – to intercept private communications in relation to an activity or class of activities specified in a ministerial authorization. To detect and protect against sophisticated cyber threats, CSE may, on receiving a written request from a Government of Canada institution to conduct information technology security activities, deploy measures to collect and analyze data from that client's system or network. These activities are commonly referred to as cyber defence activities. Because these activities risk the interception of private communications, CSE must conduct them under the authority of a ministerial authorization. A ministerial authorization is valid for one year.

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

The review covered the cyber defence ministerial authorization in effect from July 1, 2015, to June 30, 2016 and also followed up on findings and recommendations from last year's report.

FINDINGS

The Commissioner found that the 2015–2016 cyber defence ministerial authorization met the conditions for authorization set out in the *National Defence Act*.

The Commissioner found no evidence that CSE conducted any cyber defence ministerial authorization activities contrary to the law. Overall, CSE made no

significant changes to the conduct of cyber defence activities or changes that affected the risk of non-compliance with the law or to privacy.

Changes made to the 2015–2016 cyber defence ministerial authorization itself were not significant; however, they were positive. Also positive was the increased clarity brought about by the changes made to the associated request memoranda to the Minister.

Since last year's review, CSE made one substantial change to its cyber defence policy that expanded the situations in which certain Canadian identity information associated with compromised or targeted infrastructure may be disclosed, unsuppressed, to select Government of Canada institutions, private sector entities and Second Party partners when the information is necessary for analytic and mitigation purposes. The Commissioner accepted this change because of the lower expectation of privacy attached to this type of Canadian identity information. According to CSE, the change will help it meet its cyber mitigation role under Canada's Cyber Security Strategy, for example, by facilitating timely sharing of cyber threat information with data owners and partners. However, CSE should work with its Second Party partners to finalize an information-sharing agreement for cybersecurity, which was in draft form at the time the report was being prepared.

The Commissioner's office continues to follow CSE's implementation of a service introduced in 2014–2015 that is used to detect and mitigate malicious or abnormal cyber activity on electronic communications devices. The office will also monitor CSE use of a tool that was deployed as a pilot project during the period under review. These new services appear to be generally consistent with existing cyber defence activities, and CSE is applying the existing operational policies and procedures, compliance validation framework, and privacy protections to these new services.

During the period under review, CSE upgraded its repository for used and retained cyber defence data and the system for tracking records related to the private communications that CSE collects under its information technology security mandate. Data in the new repository is used, for the most part, for conducting cyber threat analysis and writing reports. It provides enhanced record-keeping capabilities, including requiring more detailed information about the justification for the retention of a private communication, which permits CSE to better demonstrate compliance. The repository also uses attributes of intercepted data to automate the identification of potential private communications. This is expected to reduce human error and standardize the counting of cyber defence private communications, and addresses a recommendation the Commissioner made last year to enhance the accuracy and consistency in reporting to the Minister. The Commissioner's office will continue to monitor CSE tracking and reporting of cyber defence private communications.

Intercepted data, including any private communications, may be retained or used by CSE only if it is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. A cyber incident may involve one or more cyber events and one or more private communications. The Commissioner's office selected and examined a sample of cyber defence data CSE intercepted in 2015–2016, including a majority (approximately 75 percent) of the cyber incidents that CSE identified as containing private communications. The office examined: internal and external reports; the cyber events that made up the incidents, including malware, e-mails, analyst notes; and details contained in tools and databases, such as private communication count, the rationale for retention of a private communication, and information about the threat actor and threat vector.

THREAT VECTOR

A threat vector is a path or a tool that a threat actor uses to attack a target. For example, a threat actor could use the following vectors to attack a target: a fake Internet site; links or attachments found in emails; or mobile devices.

The Commissioner found that the private communications that were recognized by CSE during the period under review were intercepted unintentionally – CSE did not direct cyber defence activities at Canadians or any person in Canada. Intercepted private communications related solely to malware signature and anomalous system behaviour. Retained and used private communications examined were essential to part (b) of CSE's mandate, and the reports based on the private communications contained information essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. CSE treated intercepted private communications in accordance with its policies and procedures. The Commissioner did not identify any instances where CSE retained a private communication beyond the retention and disposition periods prescribed by its policies.

In 2015–2016, there was a substantial increase in the number of private communications intercepted. It is positive that, in its 2015–2016 ministerial authorization year-end report to the Minister, CSE continued to provide a breakdown of the number of private communications recognized during new cyber defence services carried out at a number of Government of Canada institutions. The reasons for the increase from the previous year include: expanded network coverage and access to more data; improved detection capabilities; and automation of analysis.

As in previous years, a majority of the private communications that CSE counted as retained or used in 2015–2016 consisted of unsolicited e-mails sent from a cyber threat actor to a Government of Canada employee and contained nothing more than malicious code and/or an element of social engineering – that is, there was no exchange of any personal or other consequential information between the cyber threat actor and the employee. CSE acts cautiously and counts all of these communications as private communications. As a result of CSE's counting method, it appears that cyber defence activities unintentionally intercept a significantly higher number of private communications than CSE's foreign signals intelligence collection activities. In 2015, the Commissioner recommended that CSE reporting to the Minister should highlight the important differences between one-end-in-Canada e-mails intercepted under cyber defence activities and private communications intercepted under foreign signals intelligence collection activities, including the lower expectation of privacy attached to the private communications intercepted under cyber defence activities. In the conduct of this review, CSE noted that it is considering the implications of the Commissioner's legal interpretation on cyber defence activities. 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*.

It is positive that CSE is also taking action to address other findings and implement past recommendations made in the last cyber defence review, including:

- new guidance and regular communications to operational management and employees on changes to policy;
- enhancing the accuracy and consistency in reporting to the Minister;
- 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 annotation of private communications – including more comprehensive information about the justification for the retention of private communications – which provided enhanced evidence of compliance and facilitated the conduct of the review.

CONCLUSION

CSE made no significant changes to the conduct of cyber defence activities or any changes that affected the risk of non-compliance with the law or to privacy. The Commissioner found that the private communications that were recognized by CSE during the period under review were intercepted unintentionally, that is, CSE did not direct cyber defence activities at Canadians or any person in Canada.

Retained and used private communications examined were essential to part (b) of CSE's mandate, and the reports based on the private communications contained information essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

The Commissioner's office will monitor CSE actions to address issues identified in this review, and will continue to conduct annual reviews of cyber defence ministerial authorization activities.

7. Annual Combined Review of CSE Foreign Signals Intelligence Ministerial Authorizations and One-end Canadian Communications Spot Checks (2015–2016 and 2016–2017)

BACKGROUND

This summary combines the findings of the annual foreign signals intelligence (SIGINT) ministerial authorizations review and two spot check reviews of one-end Canadian communications. The review of foreign signals intelligence ministerial authorizations was executed under the *National Defence Act* (NDA), which requires the Commissioner to review CSE activities under the ministerial authorizations to ensure they are authorized, and to report annually to the Minister on the review. The office also reviewed the status, at the end of the ministerial authorization period, of private communications retained or used by CSE that were intercepted under these ministerial authorizations. The spot check reviews examined one-end Canadian communications retained, used or deleted by CSE during specified periods of time.

PRIVATE COMMUNICATION VERSUS 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.

Private communication is defined in section 183 of the *Criminal Code* as "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it."

One-end Canadian communication means a communication where one of the communicants is physically located in Canada (i.e., a private communication) or one communicant is a Canadian physically located outside Canada. Such a communication may be acquired either by CSE or by Five Eyes partners and transmitted to CSE.

CSE conducts foreign signals intelligence collection activities under the authority of paragraph 273.64(1)(*a*) of the *National Defence Act* – part (a) of CSE's mandate – to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities. These activities must not be directed at Canadians anywhere or at any person in Canada, and must include measures to protect the privacy of Canadians in the use and retention of intercepted information (paragraphs 273.64(2)(*a*) and (*b*) of the *National Defence Act*).

Subsection 273.65(1) of the *National Defence Act* permits the Minister to authorize CSE in writing, for the sole purpose of obtaining foreign intelligence, to intercept private communications in relation to an activity or class of activities specified in the ministerial authorization. Because foreign signals intelligence activities risk the unintentional interception of private communications, CSE must conduct these activities under the authority of a ministerial authorization. An intercepted private communication may be retained or used by CSE only if it is deemed essential to international affairs, defence or security. All collected information used in a foreign intelligence report is retained indefinitely by CSE.

MINISTERIAL AUTHORIZATIONS

Ministerial authorizations shield CSE from the prohibition respecting the interception of private communications found in Part VI of the *Criminal Code*. A ministerial authorization 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 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.

INCIDENTAL AND UNINTENTIONAL

In describing the interception of a private communication under a ministerial authorization, CSE qualifies the interception using the term "incidental," whereas the Commissioner's office uses the term "unintentional." Why and what is the difference?

The "incidental" interception of a private communication occurs when CSE intercepts communications between a foreign entity located outside Canada and a person in Canada.

"Unintentional" is a legal description of the "incidental" interception of a private communication made by CSE in a technical or operational context. It is "unintentional" in a legal perspective because the interception was not done with the aim of targeting a Canadian or a person in Canada, but rather as a by-product or a subordinate part of the targeting of a foreign entity located outside of Canada.

During fiscal year 2016–2017, CSE conducted foreign signals intelligence collection activities under ministerial authorizations – three of which were in effect July 1, 2015, to June 30, 2016, and three that came into effect on July 1, 2016, and expire on June 30, 2017. The office reviewed these ministerial authorizations.

The objectives of the review were: to ensure the ministerial authorizations were authorized, that is, that the conditions for authorization set out in subsection 273.65(2) of the *National Defence Act* were satisfied; to identify any significant changes – for the year(s) under review, compared with previous years – to the ministerial authorization documents themselves and to CSE activities or class of activities described in the ministerial authorizations; and to assess the impact, if any, of the changes on the risk of non-compliance with the law and on the risk to privacy.

The office examined the status, at the end of the 2015–2016 ministerial authorization period, of the recognized private communications that CSE had acquired, retained or used in carrying out its foreign signals intelligence activities. The office verified CSE's compliance with the law and with all applicable authorizations, ministerial directives and policies, and assessed the extent to which CSE protected the privacy of Canadians. In addition, the Commissioner's office conducted two spot check reviews – with no notice given to CSE – of one-end Canadian communications (which include private communications) used or retained by CSE during the periods of March 1, 2016, to May 31, 2016, and December 1, 2016, to January 15, 2017.

The office examined all foreign intelligence reports produced by CSE that were based in whole or in part on one-end Canadian communications. The office also received briefings on all of the one-end Canadian communications retained, viewed a sample of them directly, and interviewed the foreign intelligence analysts and supervisors concerned – who were working on government intelligence priorities – about their justification for retaining the communications.

FINDINGS AND RECOMMENDATIONS

The Commissioner found that the 2015–2016 and 2016–2017 foreign signals intelligence ministerial authorizations met the conditions for authorization set out in the *National Defence Act*, namely that:

- the interception will be directed at foreign entities located outside Canada;
- the information could not reasonably be obtained by other means;
- the expected foreign intelligence value of the information justifies the interception; and
- satisfactory measures are in place to protect the privacy of Canadians and that the private communications will be used or retained only if they are essential to international affairs, defence or security.

There were no significant changes to the 2015–2016 and 2016–2017 ministerial authorizations and associated request memoranda to the Minister.

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 its operational activities.

Once again this year, 2015–2016, there was a substantial increase in the number of used or retained private communications (3,348, which is almost 3,000 more than in 2014–2015) at the end of the 2015–2016 ministerial authorization period. The increase in the number of used or retained private communications remains a consequence of the technical characteristics of certain communications technologies, and CSE's legal obligations to count private communications in a certain manner.

CSE used 533 of these 3,348 private communications in 20 foreign intelligence reports, and subsequently deleted the remaining private communications. During the two spot check reviews, the office also reviewed a 40 percent sample of one-end Canadian communications that were unintentionally acquired during the specified time frames and subsequently recognized as such. These included both communications marked for retention and those marked for deletion by CSE as not being essential to international affairs, defence or security. The office confirmed that those one-end Canadian communications that were not essential were deleted from CSE systems.

Consequently, the Commissioner found that the current manner in which CSE counts private communications provides a distorted view of the number of Canadians or persons in Canada that are involved in (i.e., are the other end of) CSE interceptions to obtain foreign intelligence under ministerial authorizations. He **recommended**, therefore, that CSE reporting to the Minister on private communications contain additional information to better describe the private communications and explain the extent of privacy invasion.

Based on the information reviewed and the interviews conducted, the Commissioner found that CSE complied with the law and protected the privacy of Canadians. Specifically,

- CSE did not direct its foreign signals intelligence activities at Canadians or persons in Canada;
- one-end Canadian communications recognized by CSE were intercepted unintentionally;
- one-end Canadian communications used and retained by CSE were essential to international affairs, defence or security, as required by the *National Defence Act*;
- CSE deleted non-essential one-end Canadian communications; and
- CSE conducted its foreign signals intelligence activities in accordance with applicable ministerial authorizations and directives and treated one-end Canadian communications in accordance with its policies and procedures – CSE did not retain private communications beyond the retention and disposition periods prescribed by its policy.

SOLICITOR-CLIENT COMMUNICATIONS

During the 2015–2016 ministerial authorization period, CSE reported to the Minister that it used, for the first time, a private communication that it considered to be a solicitor-client communication.

The solicitor-client privilege is a quasi-constitutional right to communicate in confidence with one's legal counsel and is highly protected by the courts. CSE has policy and measures in place to determine whether this type of communication can be used in a report. At the time the communication was obtained, CSE's policy included the requirement of obtaining legal advice from Justice Canada on whether the continued retention and/or use of the solicitor-client communication would be in conformity with the laws of Canada. The requirement to consult Justice Canada in these circumstances is no longer in CSE policy.

The examination of this particular communication was hampered, however, by the lack of documentation of the legal advice obtained or the opportunity to interview the legal counsel purportedly involved. Consequently, the office had to rely on statements of CSE officials. Upon review, the office agreed that the communication did not in fact constitute a solicitor-client communication. It was therefore unnecessary for CSE to have reported this activity to the Minister. Notwithstanding, and while the Commissioner did not have any outstanding questions about CSE's treatment of the communication, he was of the view that CSE should have sought and obtained written legal advice from Justice Canada concerning the privileged nature of the communication and on whether retaining

or using it would be in conformity with the laws of Canada and would not bring the administration of justice into disrepute.

Because of the quasi-constitutional nature of solicitor-client privileged communications, the Commissioner **recommended** that CSE always seek and obtain written legal advice from Justice Canada concerning the retention or use of an intercepted solicitor-client privileged communication.

CONCLUSION

It is positive that, in recent years, CSE has implemented Commissioners' recommendations to expand privacy reporting to the Minister. Privacy reports now include recognized one-end Canadian communications received by CSE via a Second Party partner or involving a Canadian abroad, both of which are deemed to have a similar privacy interest to that of private communications. In response to another recommendation of the Commissioner, CSE reports on privacy submitted to the Minister now also contain more comprehensive information regarding the retained foreign signals intelligence private communications, including a monthly count of the private communications retained and the rationales for retention.

The Commissioner's office will continue to conduct annual reviews of foreign signals intelligence ministerial authorizations as well as reviews of CSE's foreign signals intelligence collection activities conducted pursuant to the ministerial authorizations. The office will also conduct in-depth spot check reviews of one-end Canadian communications acquired and recognized by CSE, whether collected by CSE or a Second Party partner. In addition, the Commissioner will examine in a follow-up review new foreign signals intelligence activities involving CSE cooperation with the Canadian Armed Forces. Finally, the Commissioner's office will monitor CSE actions to address matters identified in this report, including those related to the use and retention of solicitor-client communications.

COMPLAINTS ABOUT CSE ACTIVITIES

In 2016–2017, 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 2016–2017.

ACTIVITIES OF THE OFFICE

Maintaining the confidence of parliamentarians and Canadians in the work of the office requires openness and transparency, as well as concerted efforts to keep up with ever-evolving technologies and to capitalize on opportunities to share best practices with the office's counterparts in other countries.

CONTRIBUTING TO THE DIALOGUE ON NATIONAL SECURITY AND ACCOUNTABILITY

National security was in the spotlight in the past year, with government-sponsored nation-wide public consultations. The office contributed responses to a series of questions prepared for the consultations about oversight, including existing review bodies, and the proposed committee of parliamentarians on national security. On a more specific issue, the Commissioner wrote to Minister Goodale, who oversees the consultation process, to provide his views to counter a proposal to require CSE to obtain judicial warrants, instead of ministerial authorizations, when CSE unintentionally intercepts a private communication.

Apart from the consultations, the Commissioner appeared before parliamentary committees to present his perspective on legislation that touches on issues related to accountability, CSE and the work of the office:

- **House of Commons Standing Committee on Public Safety and National Security, November 15, 2016**: The Commissioner appeared before this committee in relation to Bill C-22, which proposes to establish a national security and intelligence committee composed of parliamentarians. Encouraged by the additional transparency and accountability such a committee could contribute to national security and intelligence activities, the Commissioner explained how the committee could also be a catalyst for collaboration among review bodies. The Commissioner noted that the committee's broad mandate and the respective roles for review bodies and the proposed committee should be clearly defined to avoid duplication and to ensure complementarity;
- **House of Commons Standing Committee on Access to Information, Privacy and Ethics, December 7, 2016**: The Commissioner discussed the first year of the implementation of the *Security of Canada Information Sharing Act* (SCISA) – which relates to information sharing among Canada's security and intelligence agencies and departments. Although CSE did not share or receive information under SCISA in the first year, the Commissioner echoed the concerns of the federal Privacy Commissioner that the threshold for sharing information does not consider whether personal information is involved, and that personal information in particular should be subject to a higher threshold for sharing;
- **House of Commons Standing Committee on National Defence, March 21, 2017**: The Commissioner outlined four important issues, including changes needed to the *National Defence Act*, clarifications needed to Bill C-22 on how review bodies will work with a proposed committee of parliamentarians, the need to have cooperation among review bodies authorized in legislation, and the value of transparency for security and intelligence agencies, and their respective review bodies, in strengthening overall accountability and enhancing public trust.

Remarks and letters from the Commissioner are posted on the office's website.

OUTREACH, LEARNING AND NETWORKING

The office's review process is built on maintaining an in-depth understanding of CSE policy and operations. In this context, training of the office's review staff includes attending the same CSE courses given to CSE employees. In turn, the office continued to deliver presentations about the role and work of the Commissioner as part of the orientation of new CSE employees.

Office staff members keep abreast of intelligence and security, legal, privacy, and technology issues through attendance and participation in a variety of courses offered by government institutions, professional associations, and universities. Conferences attended by staff over the past year include the International Cyber Risk Conference and the Security Education Conference Toronto. At the 18th Annual Privacy and Security Conference in Victoria, B.C., the Executive Director was moderator and presenter on a panel entitled "Privacy, National Security and Accountability: How Can Public Trust Be Ensured?" Other panel participants included representatives from the media, the Office of the Privacy Commissioner, CSE and a former general counsel for the U.S. National Security Agency.

Other opportunities for learning, networking and outreach included attendance at symposia dealing with international affairs, information technology security, national security, privacy and cyber security. Some host organizations included the International Association of Privacy Professionals, the Smart Cybersecurity Network, the Executive Panel of the Canadian Defence Engagement Program, and the Canadian Association for Security and Intelligence Studies. In January 2017, the office's in-house counsel spoke to University of Ottawa law students on the office's mandate and role. The office also continued to provide support to the Canadian Network for Research on Terrorism, Security and Society (TSAS), a network created by a number of university academics.

CANADIAN AND INTERNATIONAL REVIEW BODIES

The Commissioner and the Chair of the Security Intelligence Review Committee (SIRC), with their senior officials, have continued discussions about cooperation nationally and internationally. They and the Civilian Review and Complaints Commission for the RCMP (CRCC) have also appeared together before parliamentary committees examining Bill C-22 and the *Security of Canada Information Sharing Act*.

Productive discussions with international counterparts marked the fall of 2016. The Commissioner and senior officials met with members of the U.K. Intelligence and Security Committee of Parliament. Discussions included issues of transparency and public trust, and relations between a parliamentary oversight committee such as theirs with existing review bodies. The Chair of the U.K. committee noted that oversight and review bodies in both countries share similar challenges, particularly in monitoring the balance between privacy and security.

Also in the fall, the Commissioner and senior officials from the office met with David Anderson, the U.K. Independent Reviewer of Terrorism Legislation. Among the numerous topics covered was Mr. Anderson's assessment of the 2016 update of the British government's Investigatory Powers Bill, in which he noted the legislation "introduces world-leading standards of transparency" and provides "legal sanction to a range of powers which have already proved their worth." That bill passed into law in November.

Finally, the Commissioner and Executive Director, along with their colleagues from SIRC, discussed issues of common interest with review and oversight bodies from Australia, New Zealand, the United Kingdom and the United States, in a Washington, D.C. meeting. Such meetings will become more important, for learning not only about best practices in review and oversight, but also how the Five Eyes review bodies can more effectively examine the relationships among their intelligence agencies to strengthen public trust in their respective countries.

WORK PLAN – REVIEWS UNDER WAY AND PLANNED

The Commissioner uses a risk-based and preventive approach to reviews, setting priorities of what to review where risk is assessed as greatest for potential non-compliance with the law and risk to the privacy of Canadians. A three-year work plan is updated twice a year. Developing the work plan draws on many sources, including: regular briefings from CSE on new activities and changes to existing activities; the classified annual report to the Minister from the Chief of CSE on priorities and legal, policy, operational and management issues of significance; and issues raised in past or on-going reviews. To learn more about the Commissioner's risk-based and preventive approach to reviews, please visit the office's website.

Four reviews carrying over from 2016–2017 will be completed in 2017–2018: a review of a particular method of collecting foreign signals intelligence conducted under a ministerial authorization and a ministerial directive; a review focused on CSE targeting activities; a separate review started in 2016–2017 that derived from the concluded review of CSE sharing of information with foreign entities; the annual review of disclosures of Canadian identity information to Government of Canada clients, Second Party partners and non-Five Eyes recipients.

A follow-up review will be conducted on CSE assistance to the Canadian Security Intelligence Service (CSIS) under part (c) of CSE's mandate and sections 12 and 21 of the *CSIS Act* (formerly called Domestic Intercept of Foreign Telecommunications and Search warrants); this was planned to start last year but was displaced in priority due to the unplanned review referred to above. Another follow-up review of CSE support to CSIS under part (c) of CSE's mandate regarding a certain type of reporting involving Canadians will also be conducted. A study on CSE's use of social media for intelligence sharing will also be undertaken in the new year.

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. On October 18, 2016, he was re-appointed for a two-year term.

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 from the Regular Force as a Lieutenant-Colonel in 1976, but remained in the Reserve Force until 1996. He 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, advisors, etc.

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

Directions

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

...

Review of authorizations

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

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 disclosure to authorities necessary

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

(*a*) the person has, before communicating of confirming the information, brought his or her concern ... to his or her deputy head or ... the Deputy Attorney General of Canada; and

(*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.