Office of the
Communications Security
Establishment Commissioner

Bureau du
Commissaire du Centre de la
sécurité des télécommunications

ANNUAL REPORT
2018
2019

Canada

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

Tel.: 613-992-3044
Fax: 613-992-4096

Website: www.ocsec-bccst.gc.ca

Catalogue No. D95E-PDF
ISSN 1700-0874

Communications Security
Establishment Commissioner

The Honourable Jean-Pierre Plouffe, CD

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, CD

June 2019

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, 2018, to March 31, 2019, 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

This past year, I accepted a reappointment, starting in October, for 18 months. This extension provides continuity at a critical time, and allows me to lead the Office of the CSE Commissioner through the transition to a new role expected when Bill C-59, An Act respecting national security matters, receives Royal Assent and its provisions come into force.

This may, therefore, be the final report of the CSE Commissioner, though we continue business as usual, reviewing CSE activities, until the bill passes. I am honoured to have been in this important role, examining CSE activities through a lens of lawfulness, ever mindful to ensure that Canadians' privacy is protected. This office can be pleased with the part it has played since it came into existence in 1996, in contributing to the overall accountability of CSE to Parliament and the public, and to improvements in CSE practices and policies. Chiefs of CSE have acknowledged that CSE is a better organization because of independent, external review.

Bill C-59 promises to reshape Canada's security and intelligence accountability framework – including my role.

Under the changes proposed by the bill, the Office of the CSE Commissioner would cease to exist. The important responsibility of after-the-fact reviews of CSE activities would be handed over to the proposed National Security and Intelligence Review Agency, including any ongoing review projects. Employees of the CSE Commissioner's office, instead of following their former mandate, would be transferred to the Office of the Intelligence Commissioner being created by the legislation.

As Intelligence Commissioner, I will have a quasi-judicial role of reviewing ministers' decisions authorizing certain activities of both the Communications Security Establishment and the Canadian Security Intelligence Service to determine whether the respective ministers' conclusions to authorize these activities were reasonable and, if so, to approve them. In this new regime, I will become part of the decision-making process for those activities, that is, *before* they can be conducted.

I have examined the proposed legislation based on my experience as CSE Commissioner and as a former long-serving judge of a Superior Court. This has informed my proposals to clarify the wording of the bill and to facilitate the process involving the Intelligence Commissioner with respect to reviewing certain ministerial decisions. I proposed several

amendments to the bill when I appeared last year before the House of Commons Standing Committee on Public Safety and National Security. At the beginning of May 2019, I appeared before the Standing Senate Committee on National Security and Defence examining Bill C-59 and responded to the members' questions regarding the role of the Intelligence Commissioner as set out in the bill.

With these significant changes looming ahead, I am fortunate to have informative and useful exchanges with my counterparts not only in the Five Eyes countries, where there are strong partnerships among the intelligence agencies, but also in other countries. Several of these countries have also undergone, or are undergoing, changes to their legal, policy and operational contexts. The international environment presents us with many challenges, including terrorism and cyber threats, as well as concerns around protecting privacy. Our international contacts are valuable and contribute to informing our respective situations in a constructive way.

Similar to my observations in last year's annual report, this past year continued to be intense – in fact, increasingly so, with the progress of Bill C-59 through Parliament and the concomitant task of preparing for the transition to the new role of the Office of the Intelligence Commissioner, while continuing to conduct reviews of CSE activities. In this context, I am most fortunate to be aided by a very capable, professional and dedicated staff and I am immeasurably thankful to them for their sustained efforts in pursuing the objectives of both my current and proposed mandate.

Finally, there were changes in the office. Last summer, the Executive Director, Bill Galbraith, earned his retirement from public service, after guiding us with his dedication, knowledge and sound judgment for almost 10 years. We are very pleased to welcome his replacement, Guylaine A. Dansereau, who brings an impressive list of accomplishments from her time with the Royal Canadian Mounted Police.

We look forward to the responsibilities of the new role expected with the passage of Bill C-59, and to contributing to strengthening Canada's security through enhanced accountability and greater transparency.

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*:

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 Act also 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 budget for the Commissioner's office is 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 cryptography and other technologies needed to protect government computer systems and networks containing sensitive national and personal information. However, this part of CSE's mandate changed significantly with the creation in October 2018 of the Canadian Centre for Cyber Security. This unit brings under the authority of CSE components

of CSE, the Canadian Cyber Incident Response Centre of Public Safety Canada, and an IT security component of Shared Services Canada.

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 astute. 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 records that document important decisions and activities relating to compliance and the protection of the privacy of Canadians.

REPORTING ON FINDINGS

Classified report on each review to the Minister responsible for CSE: The results of individual reviews are produced as classified reports to the Minister of National Defence 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 – 122 to date – on its website.

OFFICE RESOURCES

In 2018–2019, the Commissioner was supported by 10 full-time positions, together with a number of subject matter experts, as required. The office's expenditures were $2,123,396, 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 (166) of the 175 recommendations made since 1997, including the five recommendations in reports to the Minister 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 is monitoring 10 recommendations that CSE is working to address – five 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 five past recommendations.

Part of CSE's mandate includes providing assistance to federal law enforcement and security agencies. In 2015, the Commissioner's office reviewed CSE's assistance to the Canadian Security Intelligence Service (CSIS) under section 16 of the *Canadian Security Intelligence Service Act*. This section permits CSIS to collect foreign intelligence at the request of either the Minister of National Defence or the Minister of Foreign Affairs. The Commissioner recommended that CSE ensure all policies related to section 16 and the assistance it provides to CSIS are consistent with and reflect the approval process for these activities. CSE fulfilled this recommendation by promulgating an overarching policy on assistance to federal law enforcement and security agencies. CSE will consider additional updates to the policy as a result of a new memorandum of understanding being developed with CSIS concerning these activities.

CSE advised it had implemented a recommendation made in January 2018 from the Commissioner's review of CSE's 2015–2016 disclosures of Canadian identity information. CSE put in place measures to ensure that clients requesting disclosure of Canadian identity information specify both the client's lawful authority and a robust operational justification to receive this information. However, this year, the Commissioner found opportunities for improvement in his review of CSE's 2017–2018 disclosures of Canadian identity information.

A 2017 review examined CSE authorities and participation in a multilateral operational initiative. To ensure clarity for any new activities involving information sharing with foreign entities, the Commissioner recommended that CSE conduct adequate assessments with respect to authorities and measures to protect the privacy of Canadians prior to commencing such activities. The Minister accepted the recommendation and, in response, CSE developed an operational risk framework to examine authorities to participate in new operational activities.

In last year's review of CSE's foreign signals intelligence activities conducted under ministerial authorization, the Commissioner recommended that CSE ensure request memoranda to the Minister of National Defence contain comprehensive information to describe and document the agency's contemplated activities in a thorough manner so as to better support the Minister's decision-making. CSE addressed this recommendation by including additional contextual information in all three ministerial authorizations related to foreign signals intelligence for 2018–2019.

Also last year, the Commissioner recommended that CSE clarify language in ministerial authorizations related to solicitor-client communications. This recommendation applied to CSE's information technology security activities and its foreign signals intelligence collection activities. CSE satisfactorily addressed the recommendation by including the same definition of solicitor-client communication in both types of ministerial authorizations. This definition reflects the legal protection afforded these types of communications.

Overview of 2018–2019 Findings and Recommendations

During the 2018–2019 reporting year, the Commissioner submitted eight classified reports to the Minister on his reviews of CSE activities.

These eight reviews were conducted under the Commissioner's authority under the *National Defence Act*:

- to ensure CSE activities are in compliance with the law; and
- to ensure CSE activities carried out under a ministerial authorization are authorized.

In a review of CSE's targeting practices in the context of a particular foreign signals collection program that is also subject to a ministerial directive, the Commissioner found discrepancies between requirements in the ministerial directive and CSE practices. This resulted in repeating a recommendation made twice in the past that CSE reconcile these discrepancies either to comply with or amend the ministerial directive.

One review resulted in three of the five recommendations the Commissioner made this year. This review related to CSE's assistance to the Canadian Security Intelligence Service's warranted activities for investigating or reducing a threat to the security of Canada using intrusive means, regardless of where that identified threat is situated in the world.

The review of disclosures of Canadian identity information for 2018–2019 focused on ensuring implementation of a previous recommendation that when a client requests disclosure of Canadian identity information, the client must specify its lawful authority and a robust operational justification to acquire that information.

Besides the review of CSE disclosures of Canadian identity information, the Commissioner also conducted other annual reviews:

- of ministerial authorizations for foreign signals intelligence activities;
- of one-end Canadian communications (including private communications) acquired, used, retained and destroyed by CSE, which was a spot check examination whose results were reported with the annual review of ministerial authorizations related to foreign intelligence;
- of cyber defence activities conducted under ministerial authorization; and
- of CSE incidents and procedural errors related to privacy.

The review of incidents and procedural errors brought to light a privacy incident that demanded deeper examination. This incident was the subject of its own review.

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.**

The Commissioner made five recommendations to promote compliance with the law and strengthen privacy protection, including that:

1. CSE reconcile discrepancies between requirements in a ministerial directive and CSE practices, either by fulfilling the stipulated administrative obligations or seeking an amendment to the applicable ministerial directive;
2. CSE develop, in collaboration with CSIS, a mechanism to provide CSE minimally redacted judicial decisions relevant to understanding CSIS's warrant authorities;
3. CSE develop, in collaboration with CSIS, a formal notification mechanism to inform CSE of any changes to the warrant template or of any changes to the underlying interpretations of CSIS warrants in the context of the warranted target activities;
4. CSE take measures to ensure that the identification and retrieval of all documentation relevant to a review request are accurate and complete; and
5. CSE take measures to ensure its corporate records regarding the disclosure of Canadian identity information contain detailed and complete information describing and documenting the disclosure, and the status of the disclosure.

BUSINESS AS USUAL UNTIL BILL C-59 RECEIVES ROYAL ASSENT

As of the writing of this annual report, Bill C-59 had not yet been passed. This legislation will eliminate the Office of the CSE Commissioner and move its review functions to the National Security and Intelligence Review Agency. The CSE Commissioner and the staff of the Commissioner's office will take on new duties as part of what will be the Office of the Intelligence Commissioner. Until this legislation is enacted, however, the CSE Commissioner will uphold his commitment to fulfill his mandate under the authority of the *National Defence Act*. All conclusions and references to follow-up reviews in this annual report are written as if the Office of the CSE Commissioner will continue to operate for the foreseeable future. Regarding review reports completed in and reviews carrying over into the new fiscal year, Bill C-59 states that all reviews not reported on will be transferred to the National Security and Intelligence Review Agency. Bill C-59 requires this agency to include this information in its first annual report. It is also expected that the National Security and Intelligence Review Agency will continue to monitor issues that the CSE Commissioner has identified in the past.

Highlights of Reports Submitted to the Minister in 2018–2019

CSE'S MISSION POLICY SUITE

During the 2017–2018 fiscal year, CSE achieved its ambitious goal of consolidating all its existing operational policies — more than 60 policy documents — into the Mission Policy Suite that governs its operational activities. The Mission Policy Suite consists of an overarching preamble discussing CSE's authorities, governance and accountability, followed by a separate chapter for each of the three parts of CSE's mandate:

- Part A deals with CSE's foreign signals intelligence mandate;
- Part B deals with CSE's information technology security mandate; and
- Part C deals with CSE's mandate to assist law enforcement and security agencies.

The Mission Policy Suite has already made an imprint on CSE operations: its presence was evident in all the reviews undertaken this year by the Commissioner's office.

1. Review of CSE's Targeting Practices in the Context of a Particular Collection Program

BACKGROUND

CSE conducts foreign signals intelligence collection activities under the authority of the *National Defence Act*. The Act requires that activities conducted under CSE's signals intelligence mandate, including methods of collection, 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 acquire information of potential foreign intelligence value to the government and to ensure that CSE directs its collection activities at foreign entities located outside of Canada, CSE must distinguish those communications that involve foreign entities – i.e., foreign persons, organizations, corporations or machines/networks – located outside Canada from those communications originating or terminating in Canada or involving Canadians. To that end, CSE uses strict criteria and parameters in "targeting" the communications of such foreign entities of interest and applies a number of control mechanisms to ensure compliance with the Act.

CSE conducts a particular intelligence collection program that provides unique access to foreign signals intelligence as well as to metadata in support of target and network analysis; the intelligence and the metadata, in turn, aid subsequent targeting and intelligence collection activities. This program is carried out under specific authorities and ministerial direction.

METADATA

Metadata is information associated with a communication that is used to identify, describe, manage or route that communication. It includes, but is not limited to, a telephone number, an e-mail or IP (Internet protocol) address, and network and location information. Metadata excludes the content of a communication.

Certain risks and sensitivities associated with this program demand that its activities be reviewed periodically to verify whether, in fact, they were carried out in compliance with the law and with all applicable ministerial direction, and whether adequate measures were in place to protect the privacy of Canadians.

This review covered the period from April 1, 2015, to March 31, 2016; however, relevant developments since that timeframe were also taken into consideration. The review also followed up on certain issues raised in previous reviews that were relevant to the current review.

FINDINGS AND RECOMMENDATION

For the particular collection program that is the focus of this review as well as more generally, CSE has operational policies and procedures for its signals intelligence targeting activities that provide sufficient direction to CSE employees on the protection of the privacy of Canadians. Moreover, CSE employees display a high level of policy awareness pertaining to targeting and related activities.

CSE uses an automated rules-based approach to targeting, which helps ensure consistency in the application of its targeting criteria and adds rigour to the targeting process. Centralized validation of targeting requests, by a targeting authority outside the intelligence production chain, reduces the residual risk of inappropriate targeting and adds further rigour to the targeting process. CSE also maintains comprehensive records of its targeting history and has in place a compliance monitoring regime that includes, among other things, mandatory regular revalidation of targets to help ensure compliance as well as appropriate corrective action in the event of a targeting anomaly.

In following up on targeting-related issues that were raised in two previous reviews, the Commissioner found that CSE had addressed all but one. The single outstanding issue related to the ready availability of comprehensive statistics on a particular aspect of targeting that is carried out by CSE either on its own behalf or on the request of a Five Eyes collaborating agency. CSE had previously indicated an intention to enable its targeting management system to provide such statistics; however, the agency has since noted that it does not consider this capability a priority, and consequently nothing has materialized. CSE assured the Commissioner's office, however, that if such statistical information were needed, it could be generated manually. CSE also advised that it is developing a new system that is expected to address any statistical and reporting shortcomings previously identified, although the agency has not yet established a timeline for implementing this new system. The Commissioner's office will monitor progress in this area.

CSE'S FIVE EYES PARTNERS

The Five Eyes partners are CSE and its main international cryptologic 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.

Another issue raised in two other previous reviews, and followed up on in the current review, involved specific long-standing discrepancies between CSE's practices and certain administrative risk-management measures stipulated in the ministerial directive for the intelligence collection program that was the focus of this review. The Commissioner found that these discrepancies continue to exist. The Commissioner **recommended**, once again, and as was also recommended by his predecessor, that CSE reconcile these discrepancies to comply with the ministerial directive by either

fulfilling the stipulated administrative obligations or seeking an amendment to the applicable ministerial directive itself. The Commissioner was pleased to note, however, that the Chief of CSE committed in writing to rectify this situation in a timely manner.

CONCLUSION

As a result of this review, the Commissioner concluded that CSE's targeting activities during the period under review complied with the law and were directed at foreign targets in accordance with Government of Canada intelligence requirements. As well, CSE had satisfactory measures in place to protect the privacy of Canadians when conducting targeting activities. The Commissioner also concluded, however, that long-standing discrepancies remain between CSE's practices respecting the particular collection program that was the focus of the review and certain administrative obligations set out in a ministerial directive. The Chief of CSE subsequently committed to correcting this situation.

2. Review of CSE Assistance to the Canadian Security Intelligence Service for Warranted Target Activities

BACKGROUND

Under its own authorities, CSE is prohibited from directing its foreign intelligence or information technology security activities at Canadians or at any person in Canada. CSE can, however, provide technical and operational assistance to federal law enforcement and security agencies in the performance of those agencies' lawful duties. In this context, the Canadian Security Intelligence Service (CSIS) may request CSE assistance to investigate or reduce a threat to the security of Canada using intrusive means, regardless of where that identified threat is situated in the world.

If CSIS has a judicially authorized warrant, issued under the *Canadian Security Intelligence Service Act,* CSE can support CSIS with the interception of Canadians' communications to investigate or reduce a threat to the security of Canada. When CSE provides operational assistance to CSIS, CSIS remains the owner of the information and of the intercepted communications relating to the subject of the warrant. Further, CSE is subject to any limitations imposed by law on the agency to which it is providing assistance.

Between 2008 and 2014, the Federal Court rendered several decisions that highlighted gaps in the statutory underpinnings of the domestic interception of foreign telecommunications and search warrant process, as well as issues concerning CSE assistance to CSIS in executing these warrants. In 2015, the CSIS Act was amended by the coming into force of Bill C-44, An Act to amend the Canadian Security Intelligence Service Act and other Acts, and of Bill C-51, Anti-terrorism Act. CSIS is now permitted by statute, when it has a validly obtained warrant, to investigate threats using intrusive means or to reduce threats to the security of Canada, within or outside Canada. To reflect the legislative changes, the term warranted target activities replaced the term domestic interception of foreign telecommunications and search.

Under this regime, CSIS requests for CSE assistance delineate the type of assistance requested and identify CSIS's rationale and authority to request the assistance. CSIS also provides CSE the relevant warrants issued by the Federal Court to demonstrate to CSE that CSIS has the legal standing to receive CSE assistance.

The Commissioner's office reviewed CSE assistance provided in support of all requests for assistance relating to CSIS warrants that were issued and expired between June 1, 2015, and June 1, 2017. The review also examined CSE's processes and practices concerning these activities. CSE provided the Commissioner's office with comprehensive briefings on its warranted target assistance activities. In addition, the office sent requests for information and received written responses from CSE. The Commissioner's office also examined applicable written and electronic records, files, correspondence and other documentation relevant to CSE assistance including policies and procedures, legal guidance, associated warrants, request for assistance documents, and internal correspondence. Furthermore, CSE employees involved in warranted target assistance activities were interviewed.

The Commissioner's office examined the contents of reporting databases to verify information provided by CSE and to ensure conformity with legal and ministerial requirements and associated policies and procedures. For that purpose, all reports and requests for CSE assistance to CSIS warranted target activities during the period under review were assessed. The office also assessed a sample representing over 20 percent of the total selectors used by CSE against various criteria to determine whether warrant conditions were respected.

FINDINGS AND RECOMMENDATIONS

During the period under review, CSE assisted CSIS in investigating threats to the security of Canada, but received no requests related to CSIS activities to reduce threats to the security of Canada.

First, the Commissioner's office assessed CSE's warranted target activities framework. It found that CSE reasonably interpreted the legal framework applicable to warranted target activities. CSE also accurately tracked and accounted for the required documents to conduct such activities. Further, to ensure that guidance was accurately put into practice, the office confirmed that requests for assistance and operational plans reflected legal guidance and warrant language.

Second, the Commissioner's office assessed whether CSE's practices followed the established guidance. It found that CSE respected warrant conditions when assisting CSIS. In addition, CSE's operational activities and handling of relevant data respected established control frameworks.

Third, the Commissioner's office assessed whether CSE adequately identified and managed compliance risks associated with legal, ministerial and policy requirements. It confirmed that CSE managers routinely and closely monitored the reviewed program activities to verify that CSE complied with governing authorities and that internal compliance monitoring and review of warranted target assistance activities by CSE contributed to the identification and mitigation of compliance risks.

Access to warrant-related decisions

The Commissioner's office noted that CSE was not always well apprised of the full scope of judicial decisions involving CSIS warrants. CSE's lack of direct access to minimally redacted warrant-related court decisions increased CSE's legal compliance risk given the fact that CSE may have less ability to form an independent opinion of CSIS's warrant authorities.

Before providing assistance, CSE must independently understand, in depth, the mandate of the organization for which it is approving assistance given that CSE will be acting under that organization's authority. To do so, CSE requires information such as court decisions that interpret CSIS activities. The Commissioner's office was advised that CSE's legal counsel, made up of Justice Canada employees acting in an advisory capacity, have access to unredacted court decisions pertaining to CSIS that are relevant to CSE and its operations. In practice, it is at the discretion of CSE's legal counsel when CSE employees are provided minimally redacted court decisions, or summaries of these decisions. Essentially, CSE employees do not directly receive court decisions relevant to CSIS activities. The fact that CSE is not directly provided general warrant-related decisions may hinder it from fully and independently assessing the risk of accepting requests to provide assistance to CSIS.

CSE would be in a better position to assess its own compliance risk if it was directly provided minimally redacted versions of the related CSIS warrant decisions. The Commissioner **recommended** that CSE develop, in collaboration with CSIS, a mechanism to provide CSE minimally redacted judicial decisions relevant to understanding CSIS's warrant authorities.

Changes in warrant language or interpretation

In addition, during the period of review, CSE did not benefit from a formal notification process of any change in warrant language or underlying interpretation from CSIS. The Commissioner's office believes that CSE should be informed by CSIS when there are changes in warrant language or underlying interpretations of what the language entails, particularly since CSE does not receive minimally redacted Federal Court decisions unless Justice Canada legal counsel at CSE deems them relevant to CSE activities.

While it is positive that CSE has identified both substantive and stylistic changes brought to requests for assistance and warrants over the course of the review period, legal compliance risks are heightened by relying on internal expertise to identify modifications in complex documents. The Commissioner therefore **recommended** that CSE develop, in collaboration with CSIS, a formal notification mechanism to inform CSE of any changes to the warrant template or of any changes to the underlying interpretations of CSIS warrants in the context of the warranted target activities program.

Access to CSE information

Lastly, the Commissioner's office relies on CSE to receive timely, accurate and complete responses to its inquiries in order to determine whether CSE's activities complied with the law. CSE is also expected to provide high-quality responses to other review bodies, such as the National Security and Intelligence Committee of Parliamentarians, and, in the event that Bill C-59 receives Royal Assent and comes into force, the National Security and Intelligence Review Agency.

Over the course of this review, the Commissioner's office noted one instance where internal access controls inhibited efforts by CSE review advisors to retrieve relevant records, leading to incomplete information being initially provided. CSE found that its review advisors had not been granted full access to CSE reporting databases and thus received inaccurate search results. The CSE review facilitation group did not know it lacked the necessary permissions to access the information. CSE ultimately provided the Commissioner's office the complete information. The Commissioner **recommended** that CSE take measures to ensure the identification and retrieval of all documentation relevant to a review request are accurate and complete.

In addition, the Commissioner encouraged CSE to evaluate whether its internal compliance groups have similar access constraints given that their access to information is structured in a similar manner to CSE's review facilitation group. Access to information for internal oversight and review facilitation groups is important. Groups at CSE charged with facilitating both internal and external oversight and review ought to be granted sufficient access to provide review bodies accurate and complete information.

CONCLUSION

In response to the issues identified in this review, CSE has already taken steps to address the recommendation pertaining to the establishment of a formal notification mechanism for changes to warrant language or interpretation. CSE has indicated that since the review period, it has developed a formal mechanism with CSIS to regularly update warrant language. The Commissioner's office will monitor this development.

The Commissioner concluded that CSE's warranted target assistance activities complied with the law, ministerial direction, and CSE's policies and procedures. Furthermore, CSE has satisfactory measures in place to protect the privacy of Canadians when conducting warranted target activities.

3. Annual Review of CSE Disclosures of Canadian Identity Information, 2017–2018

BACKGROUND

This is the 10th annual review of a sample of CSE disclosures of Canadian identity information. This review's objective was to verify that CSE disclosures of Canadian identity information complied with the law, ministerial direction, and CSE policies and procedures, including assessing the extent to which CSE protected the privacy of Canadians.

The Commissioner's office selected and examined a sample of 22 percent (258 requests) of the 1,156 requests from CSE's Government of Canada clients for Canadian identity information contained in CSE and Second Party reports. The requests were received by CSE between July 1, 2017, and June 30, 2018. The sample included all government institutions that made a request during that period. A review of 2015–2016 requests for disclosure found that requests submitted by a particular Government of Canada client typically contained insufficient details. A summary of this review can be found in the Commissioner's 2017–2018 annual report. This sample included all requests submitted by that client.

REQUESTS FOR DISCLOSURE OF CANADIAN IDENTITY INFORMATION IN A REPORT

In collecting foreign signals intelligence in support of the Government of Canada's intelligence priorities, CSE may unintentionally intercept Canadian identity information or information about a Canadian. If the information is used in a report, any Canadian identity information must be suppressed, that is, replaced with a generic term, such as "a named Canadian," to protect the Canadian's identity. When CSE produces a foreign intelligence report that includes suppressed Canadian identity information, CSE clients who can demonstrate they have the legal authority and operational justification can submit a request for disclosure of the information.

Consistent with the approach last year, the office conducted a comparative analysis of requests from various Government of Canada clients. During this review, the Commissioner expected to see evidence of CSE's action on a recommendation made in January 2018 during the 2015–2016 review, that CSE strengthen its procedures to exercise a higher degree of diligence to ensure that all requests stipulate both the lawful authority under which the information is being requested, and a robust operational justification for the need to acquire that information, consistent with the requestor's mandate. The Minister accepted this recommendation and CSE advised it had been implemented.

Although CSE made progress in implementing this recommendation, the review of disclosures for the 2017–2018 period still found instances where the lawful authority and/or operational justification provided in certain client requests could be strengthened.

The office also examined all 102 requests from Second Party partners and the 24 requests made by two Government of Canada clients and CSE itself to share specified Canadian identity information with non-Five Eyes entities. When CSE releases such information to Second Party partners or non-Five Eyes recipients, CSE is responsible for determining if this sharing could result in a substantial risk of mistreatment of the Canadian whose information is being released. If CSE discloses the information to other Government of Canada institutions, however, those institutions must conduct the mistreatment risk assessment before they can release the information through their own channels.

FINDINGS AND RECOMMENDATION

The Commissioner found that:

- CSE disclosures of Canadian identity information complied with the law;
- the requesting Government of Canada clients or Second Party partners had the authority to obtain the information; however, some client requests did not always explicitly state the lawful authority or provide robust operational justification;
- there were four instances where CSE's disclosure of Canadian identity information was contrary to its operational policies and procedures; and
- CSE acted in accordance with ministerial direction for addressing risks in sharing information with foreign entities that could result in the mistreatment of an individual.

While the Commissioner found that the disclosure of Canadian identity information complied with the law, 7 percent of the requests analyzed did not stipulate a legislative authority, including a few from the client department whose requests were identified as deficient in the review of 2015–2016 disclosures.

In just over 80 percent of requests for disclosure of Canadian identity information, clients provided robust operational justification. In some instances, however, the Commissioner's office was unable to assess CSE's decision to disclose the Canadian identity information based solely on the written record provided, and had to rely on additional information provided by CSE. The Commissioner's office is of the view that the additional clarification from CSE constituted information that should have been included in the justifications provided in the requests for Canadian identity information or, alternatively, in CSE's records of the rationale for approving the disclosures.

In just under 20 percent of requests, clients provided operational justifications that were generic. CSE explained that generic justifications had been developed in discussion with clients and tested over time. CSE also explained that its analysts learn its clients' mandates, authorities and requirements. However, the Commissioner's office believes these generic requests could not be described as robust, as required by CSE policy, because they did not provide an important element required for approving a client's disclosure request: the requestor's specific reason for the Canadian identity information.

CSE believes these generic requests meet the minimum requirements of policy. However, because the requests contain generic justifications that did not sufficiently outline the requirement for the suppressed information, they failed to meet the Commissioner's office's expectations for justifications of Canadian identity information disclosures. The Commissioner's office will monitor this matter.

In two instances, the operational justifications were inadequate because they did not meet the policy requirements. These two requests came from within CSE itself. During the review, the Commissioner's office noted that these two releases were unproblematic and approved. However, information in CSE's 2017–2018 Minor Procedural Errors File specified that the released Canadian identity information in these cases was in fact subsequently "retracted." Therefore, the CSE corporate records that had been examined by the Commissioner's office contained incomplete information as to the status of these releases.

In light of these findings, the Commissioner **recommended** that CSE take measures to ensure its corporate records regarding the disclosure of Canadian identity information contain detailed and complete information describing and documenting the disclosure, as well as the status of the disclosure.

It is positive that CSE identified these two releases proactively during routine monitoring, resulting in the identity information being retracted.

CSE's Five Eyes partners made 102 requests for disclosure of Canadian identity information in the period under review. The office raised issues with two of these requests. The first related to a request that resulted in Canadian identity information being mistakenly disclosed to a Second Party partner despite a decision that the disclosure was not authorized. Prior to the office's review, CSE was unaware of the disclosure to this agency. The incident was subsequently recorded in CSE's Privacy Incidents File.

The second issue concerned insufficient operational justification being provided by a requesting Five Eyes partner.

The Commissioner encouraged CSE to exercise enhanced diligence when disclosing Canadian identity information outside of Canada and to ensure all policy requirements are met.

CONCLUSION

This review found that CSE disclosures of Canadian identity information complied with the law but there were instances where CSE did not comply with its own policy to require the requesting agency to provide its lawful authority and sufficient operational justification to acquire the information.

The Commissioner **recommended** that CSE take measures to ensure its corporate records regarding the disclosure of Canadian identity information contain detailed and complete information describing and documenting the disclosure, as well as the status of the disclosure. Since the period under review, CSE has advised it has introduced a new tool for receiving, responding to and tracking requests for disclosure of Canadian

identity information. This tool could possibly track the status of a disclosure, including situations where a disclosure decision is retracted. The Commissioner's office will monitor this development.

The integrity of the review process for both CSE and the Commissioner's office depends on the accuracy and completeness of the information provided by CSE. During this review, the Commissioner's office found that the identification and retrieval of some information relevant to the review was incomplete. The Commissioner identified a need for improvement in this area in his recommendation in the review of CSE's assistance to the Canadian Security Intelligence Service for warranted target activities (page 19).

The Commissioner's office will continue to conduct annual reviews of CSE disclosures of Canadian identity information to clients and partners to verify that CSE complies with the law and protects Canadians' privacy.

4. Annual Combined Review of CSE Foreign Signals Intelligence Ministerial Authorizations, 2017–2018 and 2018–2019, and a One-End Canadian Communications Spot Check

BACKGROUND

This summary combines the findings of two reviews:

- **The annual foreign signals intelligence ministerial authorizations review**: The review of foreign signals intelligence ministerial authorizations was executed under the *National Defence Act*, which requires the Commissioner to review CSE activities under ministerial authorizations to ensure they were authorized and to report annually to the Minister on the results of the review. The Commissioner's office also reviewed the status, at the end of the ministerial authorization period, of private communications that were intercepted under these ministerial authorizations and retained or used by CSE.
- **A spot check review of one-end Canadian communications**: The spot check review was conducted under the Commissioner's main mandate to review CSE's activities to ensure that they were in compliance with the law. The review examined one-end Canadian communications retained, used or deleted by CSE during a two-month period in 2018. They included those intercepted by Second Party partners and transmitted to CSE.

PRIVATE COMMUNICATIONS AND ONE-END CANADIAN COMMUNICATIONS

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. The Commissioner reviews such communications whether they were acquired by CSE or by Five Eyes partners and transmitted to CSE.

CSE conducts foreign signals intelligence collection activities under its 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.

The *National Defence Act* also 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. Since 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.

During fiscal year 2018–2019, CSE conducted foreign signals intelligence collection activities under three ministerial authorizations. These were in effect July 1, 2017, to June 30, 2018, and were reissued for a one-year period: July 1, 2018, to June 30, 2019. The office reviewed these six 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 the *National Defence Act* were satisfied;
- to identify any significant changes – for the years 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 2017–2018 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 a spot check review – with no notice given to CSE – of all one-end Canadian communications (which include private communications) used or retained by CSE during a two-month period in 2018.

For both the private communications acquired under ministerial authorization and the one-end Canadian communications that were part of the spot check review, the office examined all foreign intelligence reports produced by CSE that were based in whole, or in part, on these communications. The office also received briefings on all of these communications that were retained, viewed a sample of them directly, and interviewed the foreign intelligence analysts and supervisors concerned – who were working on government intelligence priorities such as terrorism and supporting military operations – about their justification for retaining the communications.

FINDINGS

The Commissioner found that the 2017–2018 and 2018–2019 foreign signals intelligence ministerial authorizations met the conditions for authorization set out in the *National Defence Act*, namely that:

- the interception was directed at foreign entities located outside Canada;
- the information could not have been reasonably obtained by other means;

- the expected foreign intelligence value of the information justified the interception;
- satisfactory measures were in place to protect the privacy of Canadians; and
- private communications were used or retained only if they were essential to international affairs, defence or security.

The 2018–2019 ministerial authorizations and associated request memoranda to the Minister incorporated changes arising from two recommendations that the Commissioner made last year. One recommendation stemmed from a noted reduction in technical and process-related detail that was provided in one of the request memoranda for 2017–2018 compared with previous years, which had resulted in a memorandum to the Minister that was not as informative as it could be. Consequently, the Commissioner had recommended that CSE ensure that future foreign signals intelligence request memoranda contain comprehensive information to describe and document the agency's contemplated activities in a thorough manner to better support the Minister's decision-making. CSE satisfactorily addressed this recommendation by including additional contextual information in all three of its 2018–2019 foreign signals intelligence request memoranda.

The Commissioner's second recommendation last year was that CSE clarify the language in the ministerial authorizations related to solicitor-client communications. One goal was to accurately reflect the legal protection for such communications recognized in Canadian law; the other goal was to ensure consistency in the definition of this term in policy and in how CSE determines if a communication is a solicitor-client communication in practice in both its information technology security and foreign signals intelligence activities. This recommendation was addressed by clarifying the language in the ministerial authorizations and including a definition of solicitor-client communication that reflects the legal protection afforded these types of communications. In ministerial authorizations, *solicitor-client communication* is now defined as "a communication relating to the seeking, formulating or giving of legal advice between a client and a person authorized to practice as an advocate or notary in Quebec or as a barrister or solicitor in any territory or other province in Canada, or any person employed in the office of such advocate, notary, barrister or solicitor."

PROTECTION OF CANADIANS' PRIVACY

CSE is prohibited from directing its foreign signals intelligence and cyber defence (i.e., information technology security) 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 unintentionally 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.

Over the course of the 2017–2018 ministerial authorization period, the number of recognized private communications unintentionally intercepted by CSE increased modestly (0.6 percent); however, the number of these private communications deemed essential to international affairs, defence or security, and hence retained, increased markedly, by close to 120 percent (from 954 in 2016–2017 to 2,093 in 2017–2018). Of these 2,093 private communications, 402 were used in 20 foreign intelligence reports produced during this period. These reports addressed valid intelligence priorities, and the retention and use of the private communications was found to be reasonable and justified.

The remaining 1,691 private communications were retained for ongoing analysis, and all but one was subsequently deleted. The one remaining private communication was retained for further analysis and possible use. None of the recognized private communications were identified as solicitor-client communications.

As part of the spot check review, the office examined all of the 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 retained one-end Canadian communications, viewed them, and interviewed the CSE officials concerned. The office confirmed that all one-end Canadian communications that were not deemed essential had been deleted from CSE's systems.

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.

EVOLVING LEGAL LANDSCAPE AND ITS IMPACT ON CSE ACCOUNTING

In last year's review of the ministerial authorizations for foreign signals intelligence activities, the Commissioner noted that the Supreme Court of Canada had considered two cases (*R v Marakah*, 2017 SCC 59 and *R v Jones*, 2017 SCC 60) that addressed the concepts of "intercept" and "search" in the context of evolving technology. These cases were of potential relevance to the treatment of one-end Canadian communications within the context of CSE's foreign intelligence program. Ultimately, they did not impact CSE's operations; however, the evolving legal landscape has prompted CSE to expand the scope of its accounting for, and reporting on, a particular type of one-end Canadian communication that it acquires during the course of its foreign signals intelligence collection activities, whether the communications are in transit or at rest. This type of one-end Canadian communication will now be counted as a private communication.

In February 2011, then CSE Commissioner Décary recommended that CSE report to the Minister the number of this particular type of one-end Canadian communication, in a manner similar to what CSE does for recognized private communications intercepted under the other foreign signals intelligence collection programs. Although this recommendation was accepted by the Minister, CSE has not undertaken this reporting consistently throughout the years. CSE's new approach should not only ensure consistency in how private communications are annotated and counted, but also provide better accountability to the Minister. The office will continue to monitor any legal developments and their possible effect on CSE activities.

CONCLUSION

The Commissioner concluded that both the 2017–2018 and 2018–2019 foreign signals intelligence ministerial authorizations met the conditions for authorization set out in the *National Defence Act*. CSE made no significant changes to the ministerial authorizations or conduct of its foreign intelligence collection activities that adversely affected the risk of non-compliance with the law or to privacy, and the Commissioner's office found no evidence that CSE conducted collection activities contrary to legislative, ministerial or policy requirements. With respect to the interception, use and retention of private communications, the Commissioner concluded that CSE complied with the law and protected the privacy of Canadians.

Two previous recommendations made by the Commissioner – one proposing the inclusion of more comprehensive technical and process-related information in CSE request memoranda for ministerial authorizations, and the other citing a need for clearer and more consistent language in defining solicitor-client communications – were satisfactorily addressed by CSE. **No recommendations** resulted from either this year's annual review of CSE's foreign signals intelligence ministerial authorizations or the spot check review.

The Commissioner's office will continue to conduct these reviews.

5. Annual Review of CSE Cyber Defence Activities Conducted Under Ministerial Authorization, 2017–2018

BACKGROUND

CSE conducts cyber defence activities under the authority of the *National Defence Act*. CSE helps protect electronic information and information infrastructures of importance to the Government of Canada. These activities 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.

To detect and protect against sophisticated cyber threats, CSE may, on receiving a written request from a Government of Canada institution to conduct cyber defence activities, deploy equipment to collect and analyze data from that client's system or network. Because cyber defence activities risk the interception of private communications, CSE must conduct these activities under the authority of a ministerial authorization.

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

This review covered the cyber defence ministerial authorization in effect from July 1, 2017, to June 30, 2018. The purpose of the review was to assess whether CSE's cyber defence activities complied with the law and to assess the extent to which CSE protected the privacy of Canadians. In conducting this review, the Commissioner's office examined CSE's 2016–2017, 2017–2018 and 2018–2019 memoranda to the Minister of National Defence, the associated ministerial authorizations, as well as the 2017–2018 CSE Year-End Ministerial Authorization Report to the Minister. The office received onsite briefings, conducted interviews, reviewed CSE databases, systems and legal opinions, and examined various types of reports, both internal and external. The office examined a sample of cyber incidents that included private communications.

At the onset of this review, CSE advised of potential delays in responding to the Commissioner's office's questions as a result of the creation of the Canadian Centre for Cyber Security, which was officially launched in October 2018.

FINDINGS

The Commissioner found that the 2017–2018 cyber defence ministerial authorization met the conditions for authorization set out in the *National Defence Act*. CSE made no significant changes to the ministerial authorization or conduct of cyber defence activities that affected the risk of non-compliance with the law or to privacy. There were no significant amendments to policy instruments for cyber defence activities conducted under ministerial authorization during this review period. However, in June 2018 CSE promulgated a new policy suite that consolidated all operational policies and instructions into a single instrument. The Commissioner's office found this to be a positive change, effectively reducing the complexity of CSE's policy framework.

The Commissioner found that CSE complied with the law and conducted its activities in accordance with legislative, ministerial and policy requirements. Based on an examination of recognized private communications, the Commissioner found that CSE did not direct its cyber defence activities at Canadians or any person in Canada. The recognized private communications examined were related to malicious traffic or activity and suspicious anomalies for cyber threat detection. The private communications retained and used in reports were essential to identify, isolate or prevent harm to Government of Canada

computer systems or networks. There were no significant technology changes to cyber defence systems or the overall cyber defence program for this period.

In reviewing the ministerial authorizations, the Commissioner's office found some changes in terminology and reporting elements. CSE confirmed that during the 2017–2018 ministerial authorization period it defined cyber defence terms used in ministerial and operational reporting in a way that easily corresponds to counts generated by cyber defence tools. Specifically, the 2017–2018 ministerial authorization Year-End Report now reports on the number of *events* instead of *incidents* as was done in previous years. This change in terminology was to align more closely with that used in cyber threat reporting regularly released by CSE. Also, the 2017–2018 ministerial authorization request memorandum to the Minister now speaks to the number of *malicious events* detected by CSE, instead of the number of *compromises*, as used in previous requests. This change in terminology better aligns with a statistic that can be easily and consistently generated by CSE's systems for reporting. Both of these changes are positive developments that promote consistency in CSE's reporting.

EVENTS *(MALICIOUS EVENTS)*, INCIDENTS AND COMPROMISES

An **event** is a single count of observed malicious activity based on a set of criteria — for example, a malware download. The term *event* and *malicious event* are interchangeable.

An **incident** is a group of one or more events related to the same topic.

A **compromise** is the circumvention of the confidentiality, integrity and availability of a resource. CSE assesses the number of compromises by analyzing the number of devices that have been affected in concert with the observed events.

CYBER DEFENCE PRIVATE COMMUNICATIONS

For the 2017–2018 review period, the Commissioner's office selected and examined a sample of cyber defence data, including private communications intercepted by CSE. To facilitate this examination, a number of queries were executed against CSE databases. This resulted in a smaller sample than the office's usual selection of 20 percent. The queries were, however, considered to provide a more representative sample than the usual selection method because under the latter, the majority of incidents are automatically retained and not likely to reveal the variety of circumstances under which a private

communication could be acquired by CSE. An example of such a query was a selection of an on-the-spot sample of data with *incidental private communications* from both the 2016–2017 and 2017–2018 authorization periods to confirm whether or not data was still in CSE's systems after the retention period had expired. Last year the Commissioner's office first learned of the existence of incidental private communications, and committed to continue monitoring the handling of these files in its annual reviews. As expected for the 2016–2017 period, this query generated zero results because the 12-month retention limit had passed. Some results were returned for the 2017–2018 period. However, this was consistent with the permissible retention period.

INCIDENTAL PRIVATE COMMUNICATIONS

In the context of CSE's cyber security mandate, **incidental private communications** are private communications that are *not* essential to the protection of Government of Canada systems that are captured in raw files during network interception and, due to technical limitations, cannot be separated from those private communications that are deemed to be essential. The files are kept for up to 12 months, in accordance with the authorized ministerial authorization period, after which they are automatically deleted regardless of whether they also contain those private communications deemed essential.

Change in interpretation of a private communication and counting method

In March 2015, the Commissioner completed a review of CSE's 2009–2012 cyber defence operations conducted under ministerial authorization. He raised an issue relating to CSE's practice, while conducting authorized cyber defence operations under ministerial authorization, of treating all unintentionally intercepted one-end in Canada communications as private communications as defined in the *Criminal Code*.

At the time, and since then, the majority of private communications intercepted by CSE and examined by the Commissioner's office, consisted of unsolicited e-mails sent from a cyber threat actor to a Government of Canada employee that contain 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 Government of Canada employee. The Commissioner believed then, and continues to believe, that a communication where it is reasonable to expect that

the purpose of sending it is to compromise Government of Canada computer systems or networks by inserting malware within it, is not a private communication within the meaning of the *Criminal Code*, which is referred to in the *National Defence Act*.

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.

Until this year, CSE counted every e-mail containing malicious code sent to a Government of Canada employee as a private communication because at least one end is in Canada. Those e-mails used or retained by CSE have been included in the number of private communications reported to the Minister in accordance with the cyber defence ministerial authorization, for accountability purposes. This results in a large number of communications that CSE treats as private communications, thus distorting the privacy risk implications of CSE's cyber defence activities. The Commissioner therefore recommended in March 2015 that CSE reporting to the Minister on private communications unintentionally intercepted under ministerial authorizations should highlight the important differences between one-end Canadian communications intercepted under cyber defence operations and private communications intercepted under foreign signals intelligence activities, including the lower expectation of privacy attached to the private communications intercepted under cyber defence operations.

This year, CSE clarified its interpretation of the definition of a private communication in a cyber security context, making it consistent with the Commissioner's 2015 legal interpretation. Based on this new analysis, CSE implemented a new method of counting intercepted private communications.

Throughout the 2017–2018 ministerial authorization period, CSE identified both the automatically generated number of retained private communications (which do not necessarily contain substantive content, such as spam) and the number of private communications manually recognized by an analyst based on the proposed new interpretation of a private communication (which do contain substantive content). Analysts conducting cyber defence ministerial authorization activities were manually tracking the number of private communications with substantive content that are opened (viewed or recognized) and subsequently used or retained. CSE reported there were

no solicitor-client communications used or retained pursuant to this ministerial authorization and that there were 45 recognized private communications with substantive content. The Commissioner's office confirmed this based on the sample reviewed. All private communications with substantive content related to malicious cyber activity.

By the end of the 2017–2018 ministerial authorization period, analyst training was concluded, CSE's new interpretation of a private communication was reflected in its new policy suite, and technical changes had been implemented to support a new counting methodology. The Commissioner's office will examine these implemented changes in next year's review.

PRIVATE COMMUNICATIONS AND SUBSTANTIVE CONTENT

In the context of CSE's new interpretation of a private communication in a cyber security context:

Private communications are communications that contain recognized substantive content, as identified by personnel operating under CSE's cyber security mandate. "Substantive content" is a discourse between persons, involving the passing of thoughts, ideas, words or information from one person to another.

A communication containing recognized **substantive content** is a communication that is sent without malicious intent, but may contain malicious content. For example, an e-mail sent by a non-malicious originator that, unbeknownst to the originator, contained a malicious component such as a malicious link or embedded malicious code, may still contain recognized substantive content.

CYBER DEFENCE REPORTS

The Commissioner's office selected and examined a sample of reports representing eight types of cyber defence reporting. The sample reviewed included reports containing recognized private communications with substantive content and a random selection of other reports. These were examined for three elements: private communications, report dissemination and approvals. Where private communications were used in reports, the office confirmed they were essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. Dissemination was within Canada, predominantly to clients in the Government of Canada and among the Five Eyes partners, and approval levels were consistent with policy requirements.

CSE COMPLIANCE MONITORING

This year, the Commissioner's office examined CSE's compliance monitoring activities and found that they were being carried out regularly. CSE has established a compliance monitoring program in accordance with its policy, to assess the compliance of cyber security operational activities with policy and legal requirements and to ensure the protection of the privacy of Canadians. General compliance activities conducted over the period under review pertained to: data retention and disposition, conditions imposed by ministerial authorizations, and data handling requirements. The Commissioner's office found that CSE was consistent in its compliance activities and that follow-up remedial action is being taken where compliance incidents are observed. Remedial action included employee removal from an authorized access list for raw cyber defence data and the recording of non-compliance incidents where applicable.

FOLLOW-UP IN RELATION TO PAST REVIEWS

Last year, the cyber defence ministerial authorization specified the measures to be taken when a CSE analyst recognized a communication between a client and a *Canadian* solicitor. The Commissioner believed that the inclusion of this qualifier was misleading. Upon examination, the Commissioner also believed that there were inconsistencies in the definition of solicitor-client communication found in the ministerial authorization, CSE policy and how CSE determines if a communication is a solicitor-client communication in practice. The Commissioner therefore recommended that CSE clarify the language in the cyber defence and foreign signals intelligence ministerial authorizations to accurately reflect the legal protection for solicitor-client communications recognized in Canadian law, and ensure consistency with language in policy and with practice. While CSE did address this recommendation to make consistent its definition of solicitor-client communications in this year's cyber defence ministerial authorization, the Commissioner's office noted the policy did not follow suit. The new CSE policy suite has some minor discrepancies in the definition and continues to use the *Canadian* qualifier. Despite CSE's explanation that the policy reference to the term 'Canadian solicitor' is supported by a clear definition that is consistent with the definition found in the 2018–2019 ministerial authorization, the Commissioner found the reference should be removed for consistency and to avoid future misinterpretation. CSE was encouraged to do this for all relevant parts of its policy suite.

The Commissioner's office also noted last year a CSE internal use record that contained unsuppressed Canadian identity information. The office committed to monitor the inclusion of Canadian identity information in future internal use records. The Commissioner's office examined 17 incidents that included internal use records. The Commissioner's office concluded that none of the selected sample had any private

communications and that the inclusion of Canadian identity information, where applicable, was relevant to the protection of Government of Canada systems.

CONCLUSION

The Canadian Centre for Cyber Security established in 2018 amalgamates three distinct organizations with cyber security functions (Public Safety Canada's Canadian Cyber Incident Response Centre, Shared Services Canada's Government of Canada Security Operations Centre and CSE's own Information Technology Security group) under a single centre within CSE. This represents a significant change for cyber defence activities in Canada. The centre's impact to CSE cyber defence activities conducted under ministerial authorization will be examined in next year's review.

This year's annual review encountered significant delays. In explaining these delays, CSE noted competing priorities including the implementation of the new centre and various other high-profile initiatives such as activities involving the upcoming federal election. As a result of these delays, and despite CSE's best efforts, the review process was hindered because the Commissioner's office was pressed for time to conclude its review and limited in its follow-up and validation activities. However, the Commissioner's office acknowledges that the establishment of the Canadian Centre for Cyber Security is exceptional and it is expected that CSE will soon resume its timely support of the Commissioner's review function.

The Commissioner made **no recommendations**.

6. Annual Review of Privacy Incidents and Minor 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 to 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), Second Party Incidents File (SPIF) and 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 that 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 have been 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 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.

The period under review was from July 1, 2017, to June 30, 2018.

The office examined all 75 privacy incidents in the PIF (44) and SPIF (31) and subsequent corrective actions taken by CSE to address them. The office also examined all minor procedural errors (11) documented by CSE during the period under review.

FINDINGS

The privacy incidents in both the PIF and SPIF 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 of, 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, the relevant entities no longer targeted, and any associated intercepted communications and reporting deleted.

However, one targeting incident reported in this year's PIF caused the Commissioner sufficient concern that it was examined in depth. CSE supported the office in the examination of this matter and the Commissioner's findings regarding this specific incident were issued separately and follow, under *Review of a Targeting Privacy Incident*.

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, IP (Internet protocol) addresses and passport numbers. CSE suppresses Canadian identity information in its reports, replacing it with a generic term, such as "a named Canadian," to protect a Canadian's identity.

With regard to the minor procedural errors entered in the MPEF, the Commissioner agreed with CSE that all entries were minor and did not constitute "privacy incidents." These procedural errors included, for example: unopened files that may have contained Canadian identity information that were kept beyond the allowed retention period; a list that controlled access to certain types of information that technically malfunctioned and temporarily did not disable access to persons whose credentials were no longer valid; and a misconfigured routing tool that risked making Canadian Eyes Only information temporarily accessible to Second Party partners. The privacy impact of these incidents is considered less severe since they were contained internally and addressed prior to the information being accessed by anyone outside CSE.

CANADIAN EYES ONLY

"Canadian Eyes Only" is a dissemination control marking used to identify classified information that may not generally be released to foreign governments, foreign nationals or non-Canadian citizens. For example, a report marked as Canadian Eyes Only cannot be shared with Second Party partners such as the United States' National Security Agency or the Australian Signals Directorate. However, the report could be shared with Canadian departments or agencies such as Global Affairs Canada or the Canadian Security Intelligence Service.

Based on a review of the three files, answers to questions posed to CSE and an examination of the 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.

The Commissioner also found that CSE did not always follow a consistent approach to counting and categorizing incidents. According to CSE, the inconsistencies stem mainly from two issues: first, multiple teams may report various aspects of privacy incidents anchored in the same factual scenario, at different times; second, responsibility for the PIF, SPIF and MPEF files has changed within CSE over the past year. The Commissioner encouraged CSE to standardize its methodology for logging PIF, SPIF or MPEF entries and will monitor developments.

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 and SPIF for this period under review did not constitute material privacy breaches.

CONCLUSION

This review did not identify any material privacy breaches or systemic deficiencies. 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 period under review.

The recording and reporting of privacy incidents and minor procedural errors continue 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.

While the Commissioner made **no recommendations** and was satisfied that the contents and form of the PIF, SPIF and MPEF records contained sufficient details, he encouraged CSE to standardize its methodology for logging PIF, SPIF or MPEF entries and will monitor developments.

7. Review of a Targeting Privacy Incident

BACKGROUND

In reviewing CSE's 2017–2018 privacy incidents and procedural errors files, the Commissioner indicated that there was one targeting incident reported in CSE's Privacy Incidents File that had caused him sufficient concern that he decided to examine it in-depth in order to determine whether CSE complied with the law. CSE was forthcoming in providing information and supporting the Commissioner's office as it examined this matter.

FINDINGS

According to CSE, a privacy incident occurs when the privacy of a Canadian is put at risk in a manner that runs counter to, or is not provided for, in its operational policies. Typically, reporting of privacy incidents does not amount to findings of non-compliance with the law given the importance of encouraging proactive disclosure and mitigation of privacy incidents. Since the Commissioner's office began reviewing privacy incidents in 2011, the Commissioner made no non-compliance findings relating to Privacy Incidents File reviews given that CSE has typically adequately mitigated any privacy incident within a reasonable timeframe after the incident was discovered and reported.

In this particular instance, the Commissioner's office questioned whether CSE's targeting, for several years, of a possible Canadian who was ultimately confirmed to hold Canadian citizenship constituted a breach of CSE's policies and of the law because the incident was not adequately mitigated at the time it was discovered. Following the Commissioner's examination of the facts, he concluded that CSE complied with the law.

The law prohibits CSE from directing its activities against Canadians anywhere in the world and imposes on CSE the duty to establish measures to protect the privacy of Canadians in the use and retention of intercepted information. The law does not impose on CSE the obligation to avoid directing its activities at *possible* Canadians or to protect the privacy of *possible* Canadians. However, even if it is not required, it is CSE's practice to protect entities identified as possibly Canadian in the same manner as entities whose Canadian citizenship is confirmed. In such cases, CSE will apply privacy protection measures such as: cancelling or correcting reports with identities properly suppressed, no longer targeting the relevant entities, deleting any associated intercepted communications and reporting, and identifying the entity as "protected" in CSE's targeting database to prevent future targeting.

In this incident, a foreign national identified as possibly holding Canadian citizenship in 2010 remained targeted by CSE from 2010 to 2015. The incident was discovered, reported and fully mitigated in 2018, when a Second Party inquiry drew CSE's attention to the fact that this issue had not been fully addressed in 2010, when the person's possible Canadian citizenship was first discovered. In 2018, CSE obtained the necessary information to confirm that the targeted person was indeed Canadian.

Given that the identity of the targeted entity was only *confirmed* to be Canadian in 2018, the Commissioner was satisfied that CSE's mitigative actions following the confirmation of the entity's citizenship were adequate and undertaken in a timely mannor, like other matters in CSE's Privacy Incidents File.

The Commissioner found that CSE analysts did not knowingly target the Canadian while the entity's status remained unconfirmed and that a series of factors led to CSE not appropriately protecting the Canadian's privacy in 2010. Some contributing factors identified included that the incident was discovered over a holiday; that separate targeting teams responsible for different technical aspects of collection did not properly coordinate their response to the incident; and that CSE failed to identify the possible Canadian as such in CSE's targeting database.

Although the Commissioner concluded that CSE's conduct in this instance complied with the law, this incident highlighted gaps in CSE's information management, entity protection procedures and policy guidance relating to targets that *may* be Canadian but whose status has not been confirmed.

CONCLUSION

Since this incident occurred, CSE introduced a number of measures to enhance the protection of the privacy of Canadians and to reduce the risk of inadvertently targeting Canadians. The risk of such an error re-occurring is low given that CSE has adopted new targeting tools, redeveloped policies and procedures, updated its organizational structure to further reduce compliance risks, improved how it manages information storage and knowledge sharing, and improved its incident handling systems and protocols.

In addition, CSE has committed to implementing other improvements to its policies and procedures to further reduce the risk of inadvertently targeting a Canadian, notably by creating clear operational policy requirements for protecting entities identified as possibly Canadian; by consolidating accountability for de-targeting in one area; and by conducting an internal evaluation of the coordination between key stakeholders to ensure that necessary actions are taken in response to privacy incidents and to identify other potential gaps in procedures.

The Commissioner was satisfied with CSE's response to the incident and made **no recommendations**.

Complaints About CSE Activities

In 2018–2019, 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 required 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 – on the grounds that it is in the public interest. No such matters were reported to the Commissioner in 2018–2019.

Activities of the Office

This past year, the Commissioner and his officials continued to devote significant efforts to examining Bill C-59, An Act respecting national security matters, as part of the government's work to strengthen the accountability of national security activities of federal government departments and agencies. With respect to the CSE Commissioner's office, this bill will dissolve the office and create the new role of Intelligence Commissioner. The CSE Commissioner, his staff and the budget, will transition to the new Intelligence Commissioner's office.

The Intelligence Commissioner's mandate will be to review ministers' conclusions to authorize certain activities of CSE and of the Canadian Security Intelligence Service (CSIS), to determine whether these conclusions were reasonable and, if so, to approve them. As of the writing of this report, the bill was adopted, as amended, at third reading in the Senate and was expected to be passed before Parliament adjourns for the summer and the federal election takes place in the fall. The Commissioner appeared before the Standing Senate Committee on National Security and Defence to respond to members' questions to clarify aspects of the Commissioner's proposed new role and seek his opinion on various points in the bill. One amendment proposed by the Commissioner, to make explicit that the Intelligence Commissioner would issue an annual report, was accepted by the House of Commons committee examining the bill and has been incorporated in the bill.

As part of his examination of the bill, the Commissioner met with the ministers of National Defence and Public Safety, the National Security and Intelligence Advisor to the Prime Minister, the Chief of CSE and the Director of CSIS. The Commissioner's staff held numerous meetings with officials from CSE, CSIS, Public Safety Canada, the Privy Council Office, the staff of the Security Intelligence Review Committee (SIRC), and the secretariat of the National Security and Intelligence Committee of Parliamentarians. All these exchanges aimed to ensure that the processes set out in the bill for the Intelligence Commissioner's role will create as smooth a transition as possible.

OUTREACH, NETWORKING AND LEARNING

Because CSE must operate largely in secret, the Commissioner and the office strive to contribute to a better understanding of the role of accountability for intelligence and security activities in Canada. Providing transparency to the extent possible is accomplished in part through this public annual report, as well as through appearances before parliamentary committees, speeches and participation at conferences and symposia, and presentations to various groups.

Throughout the year, office staff attended conferences dealing with international affairs, information technology security, artificial intelligence, national security, privacy, cyber security and the law. In the context of the anticipated new role for the office, staff members received briefings from CSE, CSIS and SIRC, and in turn gave briefings to SIRC on review methodology and a primer on CSE's mandate and activities. Staff members also took courses related to access to information and privacy, and specialized technical subjects. Conferences and seminars were organized by such organizations as the Smart Cybersecurity Network, the Canadian Association of Security and Intelligence Studies, the Canadian Military Intelligence Association, the Canadian Bar Association, the International Association of Privacy Professionals, the Carleton Centre for Security, Intelligence and Defence Studies, and various academic institutions.

In November, the Special Legal Advisor accompanied by the Executive Director made a presentation to a civil law class at the University of Ottawa on Bill C-59 and its implications.

In February 2019, the Executive Director attended the 20th Annual Privacy and Security Conference in Victoria, British Columbia, with the opportunity to learn about the most recent developments in technology that affect both privacy and security. With the theme *Looking Back and Leading Forward in a Digital World*, this event once more brought together government, industry and academia to hear about and discuss the latest developments in Canada and internationally in technology, security and privacy. It was encouraging to see that the head of the recently created Canadian Centre for Cyber Security, which comes under the authority of CSE, was a keynote speaker and participated in a four-member panel – Is Canada a Global Leader in Cybersecurity? – which was moderated by the office's former Executive Director.

It is through training and learning opportunities that the office improves its ability to deliver on the Commissioner's mandate. Through training, office staff maintained and enhanced professional standards in various fields, including the law, access to information and privacy, highly technical computer vulnerabilities and testing, and communications security.

The office also continued to deliver presentations about its work to new CSE employees as part of CSE's foundational learning curriculum. Several office employees attended courses at CSE, grounding them in the same information CSE employees receive.

The office also continued to provide support to the Canadian Network for Research on Terrorism, Security and Society, which has representatives from a number of universities in Canada.

MEETINGS WITH OTHER REVIEW BODIES

The Executive Director has been meeting regularly with her counterparts at SIRC and at the secretariat of the National Security and Intelligence Committee of Parliamentarians, discussing issues of mutual interest and concern, in particular the pending legislative changes and new roles. The objective is to ensure as smooth a transition as possible to the new intelligence and national security accountability framework.

This past year, Australia hosted the Five Eyes Intelligence Oversight and Review Council meeting, which was held in Canberra in October. The two-day meeting was attended by the Commissioner, Acting Executive Director and Legal Counsel. Such meetings are essential at a time when the Five Eyes countries are seeing significant legislative changes that affect accountability structures and create new authorities for security and intelligence agencies. These latest meetings allowed for frank exchanges of views and sharing experiences. Discussions were held on a range of issues of mutual interest and concern to all participants, including: recent developments within respective jurisdictions and legislative changes affecting their work and current main challenges; independence of non-political intelligence review and oversight; keeping up with technology used by the intelligence services and the role of review in the privacy debate concerning the collection of bulk data; and best practices with respect to providing whistleblowers with authorized methods for disclosure of national security information. The keynote address came from the Chief of the Office of Civil Liberties, Privacy, and Transparency with the United States Office of the Director of National Intelligence. The Council members also discussed areas where they could cooperate on reviews and exchanges of employees. The executive secretariat of the Five Eyes Intelligence Oversight and Review Council, the Office of the Inspector General of the Intelligence Community of the United States, prepared an executive summary that can be found on its website.

The Commissioner, accompanied by the Special Legal Advisor, travelled to London, England, in June to meet with his United Kingdom counterpart, Investigatory Powers Commissioner Sir Adrian Fulford. The Investigatory Powers Commissioner was established by legislation in 2016. The purpose of the meeting was to discuss and compare the Canadian and United Kingdom oversight regimes and judicial processes, and share best practices. This included information about the roles of the Judicial Commissioners and the inspectors within the Investigatory Powers Commissioner's Office. The two commissioners compared notes on the progress in implementing the *Investigatory Powers Act* and the prospect of the passage of Bill C-59, An Act respecting national security matters, and the new role of Intelligence Commissioner.

Work Plan – Reviews Under Way

The Commissioner uses a risk-based and preventive approach to reviews, setting priorities of what to review based on where risk is assessed as greatest for potential non-compliance with the law or as a potential threat to the privacy of Canadians. This work plan, projected for three years, is updated twice a year.

Developing the work plan draws on many sources, including: regular briefings from CSE on new technologies, new activities and changes to existing activities; the classified annual report to the Minister from the Chief of CSE on priorities and on legal, policy, operational and management issues of significance; and issues raised in past or ongoing reviews. To learn more about the Commissioner's risk-based and preventive approach to reviews, please visit the CSE Commissioner's office website.

Should Bill C-59, An Act respecting national security matters, pass, the Office of the CSE Commissioner will cease to exist and its mandate of after-the-fact review of CSE activities will become the responsibility of the new National Security and Intelligence Review Agency (NSIRA). The most recent work plan updated by the CSE Commissioner's office will be provided to NSIRA, along with material on any ongoing review projects.

Two reviews are expected to be completed early in the new fiscal year 2019–2020 prior to Bill C-59 receiving Royal Assent and entering into force. The results of these two review reports will, as stated in the bill, be included in NSIRA's first statutory annual report on the activities of CSE, which is to be submitted to the Prime Minister. The first is a review of a particular method of collecting foreign signals intelligence conducted under a ministerial authorization and a ministerial directive. The second concerns a review derived from the concluded 2016–2017 review of CSE disclosures of Canadian identity information.

A third review, a follow-up on CSE support to the Canadian Security Intelligence Service regarding a certain type of reporting involving Canadians, is in its early beginnings.

In Closing

Given that this may be the last annual report of the CSE Commissioner, I would like to take this opportunity to reflect briefly on my almost six eventful years as Commissioner.

It has been a rewarding experience and given me great insights into the important work that CSE does. At the same time, it has highlighted for me the important role that this office played over the past 23 years in helping to ensure the accountability of CSE, an organization that must of necessity work in secret to be successful. But with that secrecy comes the need to ensure that it complies with the law that grants its significant powers and that it does not infringe the privacy of Canadians.

I became Commissioner in October 2013 only a few months after Edward Snowden's unauthorized disclosures of sensitive classified material dominated news headlines. This drew attention in an unprecedented manner to signals intelligence collection, not just by the United States National Security Agency but also by its close allies, including CSE. The incident raised questions in the public mind about the legality of certain activities of the signals intelligence agencies. It equally drew into the spotlight the work of the review bodies, raising questions about their effectiveness. In this intense period, more information than ever before was released to the public. Transparency became a watchword for me and I argued constantly for additional information to be released as a way of allaying suspicions about CSE's activities. It is a fine balance, and I believe we were able to contribute in a positive and constructive way to better informing Parliament and the interested public about the activities of CSE and about my office's approach to, and results of, review. As a result of the significant discussions in the public realm, new legislation was introduced, aiming to fill gaps that were determined to have existed under the current accountability framework. This occurred not just in Canada but in several other countries as well.

About two years later, in 2015, as a result of a lengthy and profound review of CSE metadata activities, I reported to the Minister of National Defence and the Attorney General of Canada that I had found CSE to be in non-compliance with the law. This was the first time that a Commissioner wrote to the Attorney General about non-compliance. My discussions with CSE were frank and the organization cooperated fully with my investigation. I was pleased that both the Minister and the Attorney General accepted my recommendations related to metadata. This also acted as a catalyst in making CSE more transparent about its metadata activities. For the first time, a representative of CSE provided a technical briefing to parliamentarians and then to the media.

One other area that is of great importance to me is the relationship with international colleagues, especially in the context of a changing legislative environment. I was disappointed about the demise of the International Intelligence Review Agencies Conference, which met every two years from 1996 through to 2014. However, officials of review and oversight agencies from the Five Eyes countries are now meeting annually to exchange best practices and discuss issues of mutual interest and concern. This was an important step to sustain international review relationships, given the high level of cooperation among the signals intelligence collection agencies in the Five Eyes countries. Notwithstanding this development, it is also important to maintain exchanges with other international review colleagues, and I have continued to encourage this and keep up with some of those contacts.

Assessing Bill C-59, from the time that it was introduced in Parliament until now, has been a priority. It is the most significant reframing of accountability for Canada's national security intelligence activities in 35 years. I have written elsewhere about participating in the process of assessing this proposed legislation and of proposing amendments to parliamentary committees examining the bill.

I look forward to the prospect of transitioning to the new role of Intelligence Commissioner whenever Bill C-59 is passed by Parliament. And I am truly grateful for the talent, professionalism and dedication of the staff that provide me with sound, judicious advice.

Annex A: Biography of the Honourable Jean-Pierre Plouffe, CD

The Honourable Jean-Pierre Plouffe has been Commissioner of the Communications Security Establishment since October 18, 2013.

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, advisers, etc.

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

Directions

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

...

Review of authorizations

273.65

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

Security of Information Act

Public interest defence

15.

(1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

...

Prior 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 or 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.