ICO Annual Report 2019

Office of the Intelligence Commissioner

Bureau du commissaire au renseignement

Canada

Office of the Intelligence Commissioner (ICO)

P.O. Box 1474, Station B
Ottawa, Ontario K1P 5P6
Tel: 613-992-3044
Website: **https://www.canada.ca/en/intelligence-commissioner.html**

Catalogue No. D95-8E-PDF
ISSN 2563-6049

Office of the Intelligence Commissioner
Bureau du commissaire au renseignement

P.O. Box/C.P. 1474, Station/Succursale B
Ottawa, Ontario K1P 5P6
613-992-3044, Fax 613-992-4096

November 2020

The Right Honourable Justin Trudeau, P.C., M.P.
Prime Minister of Canada
Office of the Prime Minister
Ottawa, Ontario
K1A 0A2

Dear Prime Minister,

Pursuant to the provisions of subsection 22(1) of the *Intelligence Commissioner Act*, I am pleased to submit to you this first annual report of my activities for the period of July 12, 2019 to December 31, 2019, for your submission to Parliament.

Sincerely,

The Honourable Jean-Pierre Plouffe, C.D.
Intelligence Commissioner

Canada

Table of Contents

Intelligence Commissioner's Message

I am pleased to present this first annual report of my activities as the Intelligence Commissioner (IC) for 2019. My position and the Office of the Intelligence Commissioner (ICO) were created by statute on July 12, 2019. It is an honour and privilege to serve Canada in this new review function of a quasi-judicial nature.

When the Canadian government reshaped the national security and intelligence accountability framework, it created a novel oversight function, that of the IC. In this new regime, the IC is part of the decision-making process for certain national security and intelligence activities *before* they can be conducted. My mandate is set out in the *Intelligence Commissioner Act* (IC Act). I review conclusions of either the Minister of National Defence or the Minister of Public Safety and Emergency Preparedness, and where applicable the Director of the Canadian Security Intelligence Service to determine whether they are reasonable. These conclusions are the basis on which certain authorizations are issued or determinations are made in relation to some activities conducted by either the Communications Security Establishment (CSE) or the Canadian Security Intelligence Service (CSIS).

I was mindful that the first decisions I rendered as IC would set the tone in applying this new oversight framework. When undertaking this task, I ensured that my decisions were considered and explained clearly and thoroughly. It was important to me that the ministers, along with CSE and CSIS, understood how I interpreted the new statutory framework and how this interpretation guided my decisions.

We live in an uncertain world, challenged by complex national security issues that no single agency or country can manage alone. Collectively, and within this context, security and intelligence oversight and review bodies are essential to ensuring two fundamental principles in democratic societies: accountability and transparency. As part of the Canadian security and intelligence oversight and review community, we benefit greatly from working with our partners forming the Five Eyes Intelligence Oversight and Review Council (FIORC). We have developed strong relationships, shared our expertise, and increased our collaborative efforts, and we will continue to do so in the years ahead.

This year we did face many challenges and going forward, the ICO will continue to evolve. To date, our accomplishments include the establishment of procedures supporting the independence of my role, the creation of a suite of operational policies and working aids, and the introduction of new technologies and capabilities. These achievements would not have been possible without the professionalism and dedication of my staff, as well as the essential support provided by our internal services. I am greatly thankful to them for their sustained efforts in pursuing the objectives of my new mandate.

The pages that follow provide details of my activities, including statistics, during the first six months of operation. I encourage Canadians to read this report to learn more about my office's ongoing efforts to contribute directly to the strengthening of Canada's national security through enhanced accountability and greater transparency.

The Honourable Jean-Pierre Plouffe, C.D.
Intelligence Commissioner

Mandate and Organization

ABOUT THE ICO

The ICO was established in 2019 as part of changes to Canada's national security framework

The IC's mandate is set out in the IC Act

The IC reports annually to Parliament through the Prime Minister

MANDATE

The IC conducts independent oversight of a quasi-judicial nature. The IC must be a retired judge of a superior court appointed on the recommendation of the Prime Minister. The IC performs his duties and functions on a part-time basis. The IC's role and responsibilities are defined and set out in the IC Act, the statute creating this position.

Under this legislation, the IC is responsible for performing quasi-judicial reviews of the conclusions on the basis of which certain authorizations are issued or determinations are made under the *Communications Security Establishment Act* (CSE Act) and the *Canadian Security Intelligence Service Act* (CSIS Act). If the IC is satisfied that the conclusions or reasons underpinning these authorizations or determinations are reasonable, the IC must approve them.

Intelligence Commissioner Act

REVIEW AND APPROVAL

12 The Commissioner is responsible, as set out in sections 13 to 20, for

(a) reviewing the conclusions on the basis of which certain authorizations are issued or amended, and certain determinations are made, under the *Communications Security Establishment Act* and the *Canadian Security Intelligence Service Act*; and

(b) if those conclusions are reasonable, approving those authorizations, amendments and determinations.

The IC reviews the following:

- the conclusions on the basis of which the Minister of National Defence issued or amended a Foreign Intelligence Authorization or a Cybersecurity Authorization for CSE;
- the conclusions on the basis of which the Minister of Public Safety and Emergency Preparedness determined classes of Canadian datasets for which collection was authorized or classes of acts and omissions the commission of which may be justified that would otherwise constitute offences for CSIS; and
- the conclusions on the basis of which the Director of CSIS authorized CSIS to query a dataset in exigent circumstances or to retain a foreign dataset (the Minister of Public Safety and Emergency Preparedness designated the Director of CSIS as the person responsible for authorizing this retention).

Consistent with the IC's oversight role, an authorization or determination is valid only after it is approved by the IC following this quasi-judicial review.

STANDARD OF REVIEW

The IC Act provides that the IC must perform a review of the conclusions reached by decision-makers under the CSIS Act and the CSE Act in order to determine if those conclusions are reasonable.

In accordance with the IC Act, the decision-makers, either the Minister of National Defence or the Minister of Public Safety and Emergency Preparedness, and where applicable the Director of CSIS, must provide conclusions, essentially their reasons, explaining and justifying their decision to issue an authorization or to make a determination. These conclusions are therefore essential to the IC's review.

The term "reasonable" is not defined in the IC Act, the CSE Act or the CSIS Act. In jurisprudence, however, it is a term that has been associated with the process of judicial review of administrative decisions. Review by the IC is not, as such, a judicial review — the IC not being a court of law — even though he or she is a retired judge of a superior court. Rather, the IC is responsible for performing a quasi-judicial review of the decision-maker's conclusions.

However, the IC accepts that when Parliament used the term "reasonable" in the IC Act, in the context of a quasi-judicial review of administrative decisions by a retired judge of a superior court, it intended to give to that term the meaning it has been given in administrative law jurisprudence. In that regard, the IC must be satisfied that the decision-makers' conclusions bear the essential elements of reasonableness: justification, transparency, intelligibility and whether it is justified in relation to the relevant factual and legal contexts.

Moreover, the legitimacy and authority of administrative decision-makers within their proper spheres must be recognized and an appropriate posture of respect is to be adopted.

THE INTELLIGENCE COMMISSIONER'S REVIEW PROCESS

The process begins when CSE or CSIS prepares an application and provides it to its respective decision-maker, either the Minister of National Defence or the Minister of Public Safety and Emergency Preparedness, and where applicable the Director of CSIS. If the decision-maker is satisfied that the legislative requirements are met, he or she issues an authorization or makes a determination. In doing so, the decision-maker must provide conclusions, or reasons, explaining and justifying the decision to issue an authorization or make a determination.

According to the IC Act, the decision-maker must provide the IC with all information that was before him or her when issuing the authorization or making the determination. This includes the application of the intelligence agency, any supporting document or information, written or verbal, that was considered by the decision-maker, the conclusions of the decision-maker and the authorization or determination itself. Together, these documents form the application record for the IC's review.

In each case, the IC, supported by the ICO, undertakes an in-depth analysis of the application records to determine whether the conclusions reached by the decision-maker are reasonable. If the IC is satisfied that they are, the IC must approve the authorization or determination in a written decision that sets out the reasons for doing so.

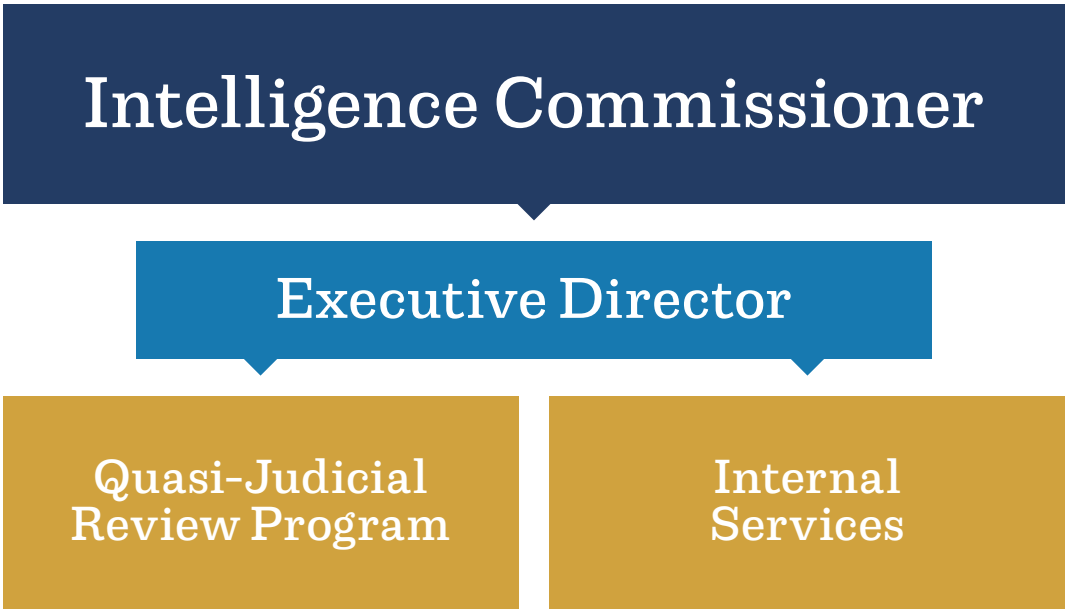
The IC Act requires that the IC's decision be rendered within 30 days after the day on which the IC received notice of the authorization or determination, or within any other period that may be agreed on by the IC and the decision-maker. In the case of an authorization issued by the Director of CSIS for a query of a dataset in exigent circumstances, the IC must render a decision as soon as feasible.

The IC must provide the decision to the concerned Minister or to the Director of CSIS. A copy of all the IC's decisions are subsequently provided to the National Security and Intelligence Review Agency (NSIRA), as required by the IC Act.

The authorization or the determination comes into effect only once it is approved by the IC.

ORGANIZATIONAL STRUCTURE

The IC, appointed by order in council for a fixed term, is the organization's Chief Executive Officer and Deputy Head and reports to Parliament through the Prime Minister. The IC must be a retired judge of a superior court and performs his duties and functions on a part-time basis.



Intelligence Commissioner Act

APPOINTMENT

4 (1) The Governor in Council, on the recommendation of the Prime Minister, is to appoint a retired judge of a superior court as the Intelligence Commissioner, to hold office during good behavior for a term of not more than five years.

RANK OF DEPUTY HEAD

5 The Commissioner has the rank and all the powers of a deputy head of a department and has control and management of his or her office and all matters connected with it.

The IC is supported by an Executive Director who is responsible for the day-to-day activities of the office, consisting of the quasi-judicial review program and internal services. The staff of the quasi-judicial review program is comprised of legal and review officer positions. This complement of positions provides a balance of the legal expertise required to assess the legal standard of reasonableness and the operational expertise required to inform those assessments. The ICO also benefits from internal services support staff to facilitate the performance of the quasi-judicial review program and to conduct day-to-day administrative functions, including human resources, financial management, security, information technology and information management activities.

SNAPSHOT OF THE ORGANIZATION

Workforce

10 full-time equivalents

Budget

$910,475

Salaries, wages and other operating costs	$491,411
Contributions to employee benefit plans	$70,895
Other operating expenses	$348,169

Results for 2019

RESULTS

The IC's position and the ICO were established in July 2019. Accordingly, statistics are provided for only six out of 12 months of operation, from July to December 2019. During those months, the IC reviewed nine authorizations and determinations. All decisions were rendered within the 30-day statutory deadline. All authorizations and determinations received and approved for calendar year 2019 were valid for one year, with the exception of a Cybersecurity Authorization which was valid for six months following the IC's approval[1].

Minister of National Defence	*Intelligence Commissioner Act*	Received	Reasonable	Not Reasonable	Partially Reasonable
Foreign Intelligence and Cybersecurity Authorizations	Sections 13 and 14	5	5	-	-
Amendments to authorizations	Section 15	0	-	-	-
TOTAL		**5**	**5**	**0**	**0**

Minister of Public Safety and Emergency Preparedness	*Intelligence Commissioner Act*	Received	Reasonable	Not Reasonable	Partially Reasonable
Determinations of classes of Canadian datasets	Section 16	1	1	-	-
Authorizations for the retention of foreign datasets[2]	Section 17	0	-	-	-
Authorizations for the querying of a dataset in exigent circumstances[3]	Section 18	0	-	-	-
Determinations of classes of acts or omissions	Section 19	3[4]	1	1	1
TOTAL		**4**	**2**	**1**	**1**

1 The decision-makers determine the validity period of the authorizations or determinations, which, in most instances, may not exceed one year, as prescribed by legislation.

2 In accordance with the CSIS Act, the Minister of Public Safety and Emergency Preparedness designated the Director of CSIS as the person responsible for authorizing the retention of foreign datasets.

3 Pursuant to the CSIS Act, this authorization is issued by the Director of CSIS.

4 This year, the Minister of Public Safety and Emergency Preparedness made three determinations of classes of acts or omissions. The Minister's original determination was not approved by the IC and partially approved the second time. The third determination was fully approved.

YEAR AT-A-GLANCE

July 12, 2019

Established by legislation

July 19, 2019

First application received

August 2, 2019

First decision rendered

9

Decisions rendered

CASE SUMMARIES

AUTHORIZATIONS ISSUED UNDER THE *COMMUNICATIONS SECURITY ESTABLISHMENT ACT*

I. Summary

When the Minister of National Defence issues an authorization, the IC Act requires the Minister to provide the IC with all of the information that was before the Minister in issuing the authorization. This information constitutes the application record.

Between August 1, 2019, when the CSE Act came into effect, and the end of the calendar year, the IC reviewed five ministerial authorizations issued by the Minister of National Defence.

In each case, the IC found that the Minister's conclusions were reasonable, and he approved the authorization. The IC issued all his decisions within the 30-day statutory deadline. The IC did not receive any amended Foreign Intelligence or Cybersecurity Authorizations to review during this reporting period.

Communications Security Establishment Act

NO ACTIVITIES – CANADIANS AND PERSONS IN CANADA

22 (1) Activities carried out by the Establishment in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate must not be directed at a Canadian or at any person in Canada and must not infringe the *Canadian Charter of Rights and Freedoms*.

[...]

CONTRAVENTION OF OTHER ACTS – FOREIGN INTELLIGENCE

(3) Activities carried out by the Establishment in furtherance of the foreign intelligence aspect of its mandate must not contravene any other Act of Parliament — or involve the acquisition by the Establishment of information from or through the global information infrastructure that interferes with the reasonable expectation of privacy of a Canadian or a person in Canada — unless they are carried out under an authorization issued under subsection 26(1) or 40(1).

II. Background

What are Foreign Intelligence Authorizations and when are they required?

One aspect of the mandate of the Communications Security Establishment (CSE) is to collect signals intelligence on foreign targets located outside Canada – that is, information about the capabilities, intentions or activities of foreign targets related to international affairs, defence or security. These activities must not be directed at a Canadian or at any person in Canada and must not infringe the *Canadian Charter of Rights and Freedoms*. In undertaking these activities, however, CSE might contravene a law or infringe on the reasonable expectation of privacy of a Canadian or a person in Canada.

To address this concern, the CSE Act permits the Minister of National Defence to issue a Foreign Intelligence Authorization to CSE. This authorization allows CSE, despite any other Canadian law or law of any foreign state, to carry out, on or through the global information infrastructure, any activity specified in the authorization to further its foreign intelligence mandate. In practice, such an authorization allows CSE to carry out activities that are consistent with its mandate but that, in the absence of the authorization, would constitute offences. Typically, these would be offences in the *Criminal Code*, such as the interception of private communications, or the conduct of certain activities necessary to enable the acquisition of information for providing foreign intelligence or to keep an activity covert.

Communications Security Establishment Act

CONTRAVENTION OF OTHER ACTS – CYBERSECURITY AND INFORMATION ASSURANCE

22 (4) Activities carried out by the Establishment in furtherance of the cybersecurity and information assurance aspect of its mandate must not contravene any other Act of Parliament — or involve the acquisition by the Establishment of information from the global information infrastructure that interferes with the reasonable expectation of privacy of a Canadian or a person in Canada — unless they are carried out under an authorization issued under subsection 27(1) or (2) or 40(1).

What are Cybersecurity Authorizations and when are they required?

CSE is Canada's technical authority for cybersecurity and information assurance. For this aspect of its mandate, CSE provides advice, guidance and services to help protect Government of Canada electronic information and information infrastructures from cyber threats. In addition, CSE is also mandated to provide similar services to help protect electronic information and information infrastructures that are designated by the Minister of National Defence as being of importance to the Government of Canada and whose owner or operator has requested CSE's assistance in writing. Such designation generally pertains to organizations and companies falling within those sectors that comprise Canada's critical infrastructure, for example, energy, finance, and information and communications technology.

These cybersecurity activities must not be directed at a Canadian or at any person in Canada, and must not infringe the *Canadian Charter of Rights and Freedoms*. However, in undertaking these activities, CSE might contravene a Canadian law or risk infringing on the reasonable expectation of privacy of a Canadian or of a person in Canada. Under the CSE Act, the Minister of National Defence may issue a Cybersecurity Authorization to CSE that allows it to access either a federal institution's or a designated non-federal institution's information infrastructure to help protect the information infrastructure from mischief, unauthorized use or disruption. Effectively, this allows for the interception of private communications, which would otherwise be an offence under the *Criminal Code*, as long as that interception happens as part of activities that meet the objectives of CSE's cybersecurity mandate and that are explicitly outlined in a Cybersecurity Authorization.

III. Opportunities for Improvement

The IC is responsible to review the conclusions, or reasons, on the basis of which the Minister of National Defence issued an authorization and, if those conclusions are reasonable, to approve the authorization.

In some instances, the IC determined that the ministerial conclusions were insufficient or non-existent. In the context of quasi-judicial review, the IC applied administrative law principles in deciding to supplement the Minister's conclusions in these cases. Generally, the IC found that the contents of the application record provided insight for the Minister's reasoning for his decision. Therefore, the IC was able to supplement the Minister's conclusions to include the information found in the application record. In other cases where there were inconsistencies between the application record and the authorization, the IC also recognized the Minister's expertise in authorizing activities.

Some of the issues noted by the IC are detailed as follows.

Provision of information to the Intelligence Commissioner

Pursuant to the IC Act, the person whose conclusions are being reviewed by the IC, in this case the Minister of National Defence, must provide the IC with all information that was before him in issuing the authorization. Each application record submitted to the IC included a list of the enclosed documents that constituted the application record. However, in most cases, the Minister did not specifically state that the documents enclosed constituted all the information that was before him in issuing the authorization. Notwithstanding, each application record provided to the IC appeared to be complete, and the IC thus rendered his decision regarding the reasonableness of the Minister's conclusions despite the absence of a confirmation.

Inconsistencies – Foreign Intelligence Authorizations

The IC found some inconsistencies in the application records for Foreign Intelligence Authorizations. Notably, the Minister's conclusions did not address certain authorized activities and some authorized activities were not supported by facts in the Chief of CSE's written application.

In addition, a condition imposed by the Minister in one of the authorizations was neither addressed in his conclusions nor rationalized elsewhere in the application record.

Inconsistencies – Cybersecurity Authorizations

The IC also found two inconsistencies in the application records for Cybersecurity Authorizations. Notably, an activity was not explicitly addressed in the Minister's conclusions despite being described in the Chief of CSE's application. Further, a condition imposed by the Minister in his authorization was neither explained in his conclusions nor supported by information found in the application record.

AUTHORIZATIONS ISSUED AND DETERMINATIONS MADE UNDER THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*

I. Summary

The *National Security Act, 2017*, amended the CSIS Act to provide a justification, subject to certain limitations, for the commission of acts or omissions that would otherwise constitute offences and create a regime for CSIS to collect, retain, query and exploit datasets in the course of performing its duties and functions.

Between July 13, 2019, when the amendments to the CSIS Act came into effect, and the end of the calendar year, the IC reviewed four determinations made by the Minister of Public Safety and Emergency Preparedness: one determination of classes of Canadian datasets and three determinations of classes of acts or omissions.

The IC found that the Minister's conclusions in the determination of classes of Canadian datasets were reasonable and he approved the Minister's authorization to collect these datasets.

In the case of the determination of classes of acts or omissions, the Minister made three determinations. For the first determination, the IC found that the Minister's conclusions were unreasonable and did not approve the determination. The Minister's conclusions were found partially reasonable in the second determination and reasonable in the third.

The IC issued all his decisions within the 30-day statutory deadline. During this reporting period, the IC did not receive for review any authorizations for the retention of foreign datasets or for the querying of a dataset in exigent circumstances.

II. Background

What is a determination of a class of Canadian datasets and when is it required?

Under section 12 of the CSIS Act, CSIS has the authority to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada." In accordance with the dataset regime referred to in section 11.02 of the CSIS Act, CSIS may gather information, in the form of a dataset inasmuch as it contains personal information, that does not directly and immediately relate to activities that represent a threat to the security of Canada. According to the CSIS Act, a dataset is "a collection of information stored as an electronic record and characterized by a common subject matter." Through amendments to the CSIS Act enacted in 2019, Parliament legislated specific controls on CSIS's use and retention of datasets to increase accountability and transparency and to better protect the privacy of Canadians, while enabling CSIS to deliver on its mandate. One of these controls involves a ministerial determination of *classes of Canadian datasets*.

A Canadian dataset is defined in the CSIS Act as a dataset that "predominantly relates to individuals within Canada or Canadians." CSIS can lawfully collect a Canadian dataset if it belongs to an approved class of Canadian datasets. At least once every year, the Minister shall, by order, determine classes of Canadian datasets for which collection would be authorized. The Minister may determine that a class of Canadian datasets is authorized to be collected if the Minister concludes

that the querying or exploitation of any dataset in the class could lead to results that are relevant to CSIS's duties and functions, namely, to collect intelligence regarding threats to the security of Canada, to take measures to reduce threats to the security of Canada or to collect foreign intelligence within Canada.

The Minister's determination comes into effect only on the IC's approval.

To lawfully retain a collected Canadian dataset, CSIS must obtain a judicial authorization from the Federal Court of Canada.

What are authorizations to retain a foreign dataset and when are they required?

CSIS collects and analyzes information to fulfil its various duties and functions such as investigating and reducing threats to the security of Canada, performing security screening investigations, and collecting foreign intelligence within Canada. This information may include foreign datasets. A foreign dataset predominantly relates to individuals who are not Canadians and who are outside Canada or to corporations that were not incorporated or continued under the laws of Canada and that are outside Canada. CSIS cannot retain a collected *foreign dataset* without an authorization to do so issued by the Minister of Public Safety and Emergency Preparedness or a person designated by the Minister. In 2019, the Minister delegated his responsibility to authorize the retention of foreign datasets to the Director of CSIS and provided a copy of this delegation to the IC.

The authorization comes into effect only on the IC's approval. The IC's approval can specify conditions respecting the querying or exploitation of the foreign dataset or its retention or destruction.

What are authorizations to query a dataset in exigent circumstances and when are they required?

In exigent circumstances, the Director of CSIS may authorize CSIS to query a dataset it has not yet received permission to retain. Exigent circumstances are defined in legislation as those necessary to preserve the life or safety of any individual or as an opportunity to acquire intelligence of significant importance to national security that would otherwise be lost. For a Canadian dataset this means that the query would take place before CSIS obtains the Federal Court's permission to retain the dataset, while for a foreign dataset it means that the query would take place before CSIS obtains the IC's approval to retain the dataset.

To request an authorization to query a dataset in exigent circumstances, CSIS submits a written application to the Director of CSIS. If satisfied that legal requirements are met, the Director can authorize the query. In the authorization, the Director must provide written conclusions, or reasons, supporting the decision to issue the authorization. The authorization comes into effect on its review and approval by the IC, which the legislation requires that he perform "as soon as feasible."

What is a determination of a class of otherwise unlawful acts or omissions and when is it required?

When collecting intelligence, CSIS might need to engage in acts or omissions that would be unlawful without an approved determination by the Minister of Public Safety and Emergency Preparedness to do so. The Minister shall make, by order, a determination of classes of otherwise unlawful acts or omissions at least once a year after concluding that the commission of those acts or omissions would be reasonable in the context of CSIS's information and intelligence collection duties and functions and any threats to the security of Canada that may be the object of information and intelligence collection activities. The Minister's determination comes into effect only on the IC's approval.

Canadian Security Intelligence Service Act

CLASSES – CANADIAN DATASETS

11.03(1) At least once every year, the Minister shall, by order, determine classes of Canadian datasets for which collection is authorized.

CRITERIA

(2) The Minister may determine that a class of Canadian datasets is authorized to be collected if the Minister concludes that the querying or exploitation of any dataset in the class could lead to results that are relevant to the performance of the Service's duties and functions set out under sections 12, 12.1 and 16.

Canadian Security Intelligence Service Act

COLLECTION, ANALYSIS AND RETENTION

12 (1) The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

III. Opportunities for improvement

During this reporting period, the IC reviewed a total of four determinations made by the Minister of Public Safety and Emergency Preparedness: one determination of classes of Canadian datasets and three determinations of classes of acts or omissions. The IC approved two of those determinations, partially approved one and did not approve another. The IC also raised some noteworthy issues. Overall, these issues were not detrimental to the reasonableness of the Minister's conclusions or the IC's approval of the determinations.

The Intelligence Commissioner's review of a determination of classes of Canadian datasets

The IC reviewed one determination of four classes of Canadian datasets made by the Minister of Public Safety and Emergency Preparedness.

The IC found that the Minister's conclusions were reasonable and consequently approved the determination of these four classes. The IC also identified minor improvements that could be made to future determinations.

The Intelligence Commissioner's reviews of determinations of classes of otherwise unlawful acts or omissions

The IC reviewed three determinations for classes of otherwise unlawful acts or omissions made by the Minister of Public Safety and Emergency Preparedness. The IC also identified minor matters that could be improved in future determinations.

First determination

The Minister is statutorily required to write conclusions to support his determination of classes of acts and omissions that would otherwise constitute offences, that is, his conclusions must explain his reasons for arriving at a given determination. However, the Minister's first determination for classes of otherwise unlawful acts or omissions did not include any ministerial conclusions. Consequently, the IC was not satisfied that the conclusions were reasonable and he did not approve the determination.

Second determination

The second determination included ministerial conclusions and identified seven classes of otherwise unlawful acts or omissions.

In relation to all but one of the seven classes, the IC found that the Minister's conclusions were reasonable, and the IC consequently approved the determinations of those six classes. However, the IC found the ministerial conclusions that were the basis of the seventh class were not reasonable, and did not approve that class.

Third determination

The third determination for seven classes of otherwise unlawful acts or omissions addressed the essential matters identified by the IC in the two previous determinations. The IC found the Minister's conclusions were reasonable, and consequently approved the determination of all seven classes.

SHARING OF DECISIONS AND REPORTS

The IC Act legislates the sharing of decisions and reports between the IC and the National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP).

The IC must provide a copy of his decisions to NSIRA in order to assist it in fulfilling its review mandate. In addition, the IC is entitled to receive a copy of certain reports, or parts of the reports, prepared by NSICOP and NSIRA, if they relate to the IC's powers, duties or functions.

INTERNATIONAL COLLABORATION

The ICO is a member of the Five Eyes Intelligence Oversight and Review Council (FIORC). FIORC was created in the spirit of the existing Five Eyes partnership, the intelligence alliance comprised of Australia, Canada, New Zealand, the United Kingdom and the United States. The FIORC members exchange views on subjects of mutual interest and concern and compare best practices in review and oversight methodology.

The ICO participated in the 2019 FIORC meeting, held in the United Kingdom and hosted by the Investigatory Powers Commissioner's Office. The IC, as well as the ICO's Executive Director and Senior Legal Counsel, attended the meeting.

Biography of the Honourable Jean-Pierre Plouffe, C.D.

Annex A

BIOGRAPHY OF THE HONOURABLE JEAN-PIERRE PLOUFFE, C.D.

The Honourable Jean-Pierre Plouffe became the first Intelligence Commissioner by virtue of the coming into force of the *National Security Act, 2017* in July 2019.

Previously, he was the Commissioner of the Communications Security Establishment since October 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 Québec 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, Québec, 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 Québec 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 Québec 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.

List of Legislation Related to the Intelligence Commissioner's Mandate

Annex B

LIST OF LEGISLATION RELATED TO THE INTELLIGENCE COMMISSIONER'S MANDATE

Intelligence Commissioner Act, SC 2019, c 13, s 50.

National Security Act, 2017, SC 2019, c 13.

Communications Security Establishment Act, SC 2019, c 13, s 76.

Canadian Security Intelligence Service Act, RSC 1985, c C-23.