ICO

Annual Report 2021

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

© Her Majesty the Queen in Right of Canada as represented by the Office of the Intelligence Commissioner, 2022.

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

March 31, 2022

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 an annual report on my activities for the 2021 calendar year, 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 third annual report of my activities as the Intelligence Commissioner for 2021. I trust that Canadians will have confidence in the strong accountability measures that have been instituted through this unique quasi-judicial function in Canada's national security accountability framework."

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

I am pleased to present this annual report of my activities as the Intelligence Commissioner for 2021. I am honoured to serve Canada in this review function of a quasi-judicial nature.

My mandate is set out in the *Intelligence Commissioner Act*. The IC is an integral part of the decision-making process for certain national security and intelligence activities before they can be conducted. This is a unique function in Canada. I review the conclusions of the Minister of National Defence and the Minister of Public Safety, 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 or the Canadian Security Intelligence Service.

I trust that after almost three years of experience, this regime of oversight is functioning as it was intended by Parliament. Indeed, it has contributed to the strengthening of Canada's national security through enhanced accountability and greater transparency.

We continued to benefit greatly from working with our domestic and international partners in the security and intelligence oversight and review community. In 2021, the Five Eyes Intelligence Oversight and Review Council meeting was held virtually. While the meeting was a success, we look forward to resuming our in-person collaboration as we explore mutual issues and concerns and share best practices.

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

This past year, the COVID-19 pandemic continued to cause significant disruptions. I am pleased to report that I met all statutory time limits for rendering decisions and other mandatory reporting requirements. These achievements would not have been possible without the significant efforts of my staff. I am grateful for their dedication and professionalism. I am appreciative of the foundation they have helped establish and their steady advancement going forward, particularly during a period of such uncertainty.

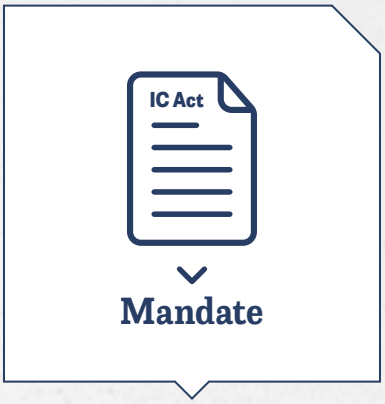
The pages that follow provide details of my activities, including statistics, during 2021. I encourage Canadians to read this report to learn more about my office's ongoing efforts to bolster Canada's national security and public confidence.

Part I

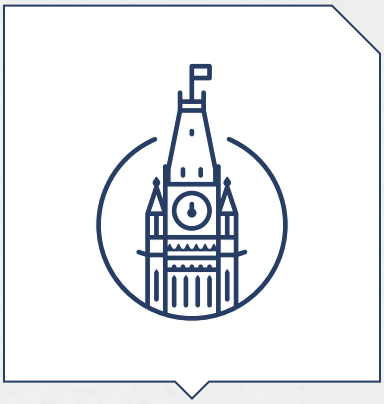
Mandate and Organization

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 INTELLIGENCE COMMISSIONER (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 OR HER DUTIES AND FUNCTIONS ON A PART-TIME BASIS. THE IC'S ROLE AND RESPONSIBILITIES ARE DEFINED AND SET OUT IN THE *INTELLIGENCE COMMISSIONER ACT* (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.

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[1] 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

1 Section 25 of the *Intelligence Commissioner Act* specifies that the IC reviews conclusions of the Minister of Public Safety and Emergency Preparedness. In October 2021, the Prime Minister separated the Public Safety portfolio from the Emergency Preparedness portfolio. The Minister of Public Safety carries out the duties that fall under the purview of the IC. For simplicity, this annual report uses "Minister of Public Safety" in this context, regardless of the timing of the conclusions under review.

- 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 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 once approved by the IC following his or her quasi-judicial review.

DID YOU KNOW?

The IC is an integral part of the decision-making process for certain national security and intelligence activities before they can be conducted.

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.

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, the Minister of National Defence and the Minister of Public Safety, 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 establish whether they are 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.

REVIEW PROCESS

THE PROCESS BEGINS WHEN CSE OR CSIS PREPARES AN APPLICATION AND PROVIDES IT TO ITS RESPECTIVE DECISION-MAKER, THE MINISTER OF NATIONAL DEFENCE AND THE MINISTER OF PUBLIC SAFETY, 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 HIS OR HER DECISION.

According to the IC Act, the decision-maker whose conclusions are being reviewed by the IC must provide the IC with all information, written or verbal, 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 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. The application record may include information that is subject to any privilege under the law of evidence, solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege. However, the IC is not entitled to have access to information that is a confidence of the Queen's Privy Council for Canada, the disclosure of which could be refused under section 39 of the *Canada Evidence Act*.

In each review, the IC, supported by the Office of the Intelligence Commissioner (ICO), undertakes an in-depth analysis of the application record to determine whether the decision-maker's conclusions 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, as required by the IC Act.

The authorization or the determination is valid once approved by the IC.

Review Process Map

2 Minister of National Defence, Minister of Public Safety, Director of CSIS.

Disclosure of Information to the Intelligence Commissioner

Other than information received in the context of reviews, the IC is entitled to receive a copy of reports, or parts thereof, from the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency if they relate to the IC's powers, duties or functions. The Minister of Public Safety, the Minister of National Defence, CSIS and CSE may also, for the purpose of assisting the IC in the exercise of his or her powers and the performance of his or her duties and functions, disclose information to the IC that is not directly related to a specific review.

Intelligence Commissioner Act

DISCLOSURE OF INFORMATION TO COMMISSIONER

25 Despite any other Act of Parliament and any privilege under the law of evidence and subject to section 26, the following persons or bodies may – for the purpose of assisting the Commissioner in the exercise of his or her powers and the performance of his or her duties and functions – disclose to the Commissioner any information that is not directly related to a specific review under any of sections 13 to 19:

(a) the Minister of Public Safety and Emergency Preparedness;

(b) the *Minister*, as defined in section 2 of the *Communications Security Establishment Act*;

(c) the Canadian Security Intelligence Service; and

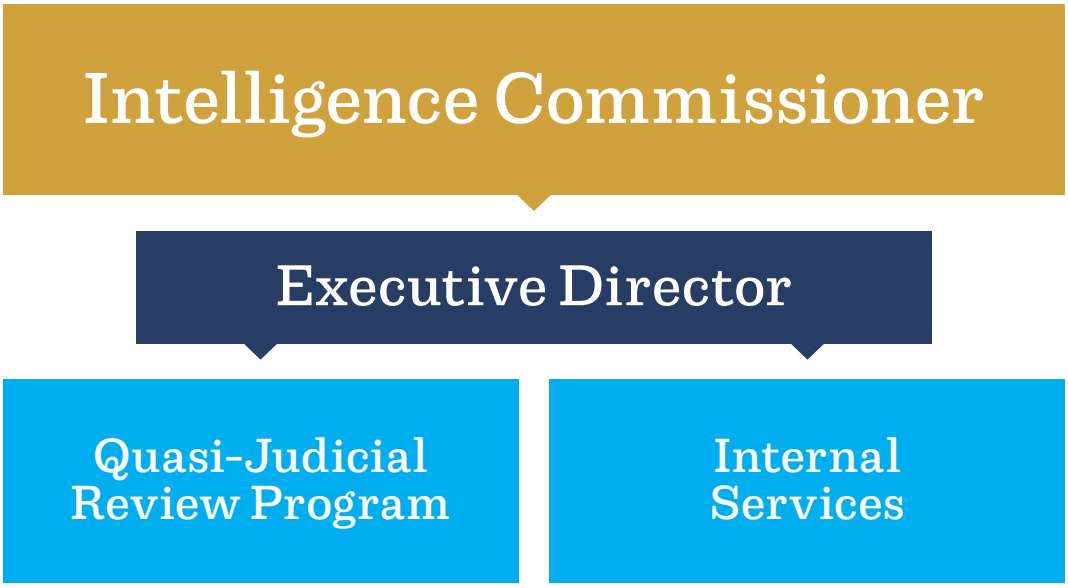
(d) the Communications Security Establishment.

NO ENTITLEMENT

26 The Commissioner is not entitled to have access to information that is a confidence of the Queen's Privy Council for Canada the disclosure of which could be refused under section 39 of the *Canada Evidence Act*.

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 OR HER DUTIES AND FUNCTIONS ON A PART-TIME BASIS.



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. Legal and review officer positions make up the staff complement of the quasi-judicial review program, providing 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.

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 behaviour 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.

SNAPSHOT OF THE ORGANIZATION

Workforce

10 Full-time equivalents

Cost of operations

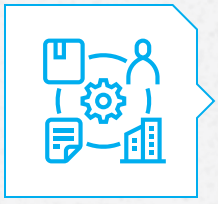
$2,018,296

Salaries and wages

$922,474

Contribution to employee benefit plans

$158,843



Other operating expenses

$936,979

Part II

Results for 2021

RESULTS

THIS REPORT CONTAINS STATISTICS FOR CALENDAR YEAR 2021. DURING THAT PERIOD, THE INTELLIGENCE COMMISSIONER (IC) REVIEWED NINE AUTHORIZATIONS AND DETERMINATIONS. ALL DECISIONS WERE RENDERED WITHIN THE 30-DAY STATUTORY TIME LIMIT AND WERE VALID FOR ONE YEAR, WITH THE EXCEPTION OF AN AUTHORIZATION TO RETAIN A FOREIGN DATASET, WHICH IS VALID FOR FIVE YEARS FOLLOWING THE IC'S APPROVAL.[3]

The IC approved 89% of the authorizations and determinations.

Minister of National Defence	*Intelligence Commissioner Act*	Received	Reasonable	Not Reasonable	Partially Reasonable
Foreign Intelligence Authorizations	Section 13	3	2	–	1
Cybersecurity Authorizations	Section 14	2	2	–	–
Amendments to authorizations	Section 15	–	–	–	–
TOTAL		**5**	**4**	–	**1**

Minister of Public Safety	*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[4]	Section 17	1	1	–	–
Authorizations for the querying of a dataset in exigent circumstances[5]	Section 18	1	1	–	–
Determinations of classes of acts or omissions	Section 19	1	1	–	–
TOTAL		**4**	**4**	–	–

3 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.

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

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

RESULTS – 3 YEARS

Minister of National Defence

Foreign Intelligence Authorizations, Section 13 of the IC Act

2021	2020	2019
3 Received	3 Received	3 Received
2 Reasonable	3 Reasonable	3 Reasonable
1 Partially Reasonable		

Cybersecurity Authorizations, Section 14 of the IC Act

2021	2020	2019
2 Received	3 Received	2 Received
2 Reasonable	3 Reasonable	2 Reasonable

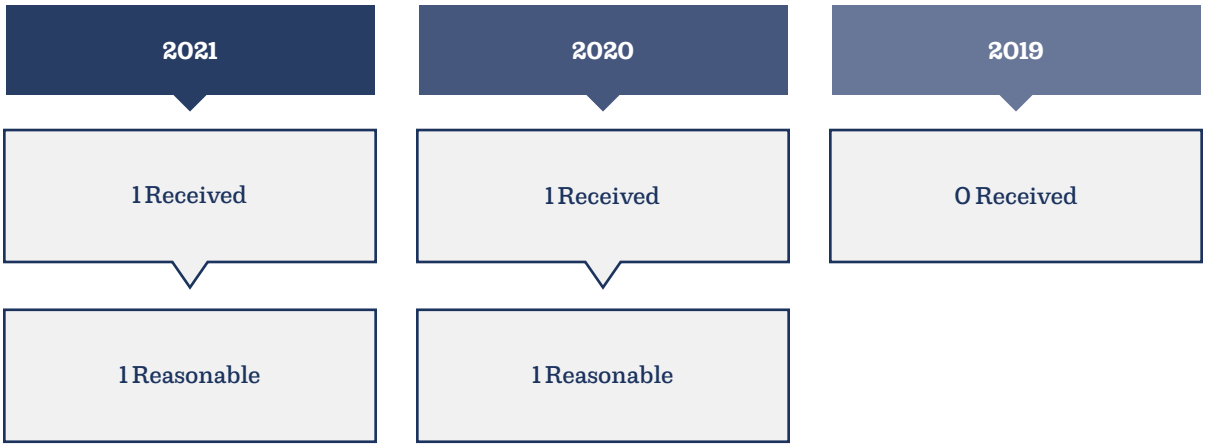
Amendments to Authorizations, Section 15 of the IC Act

2021	2020	2019
0 Received	0 Received	0 Received

Minister of Public Safety

Determinations of classes of Canadian datasets, Section 16 of the IC Act

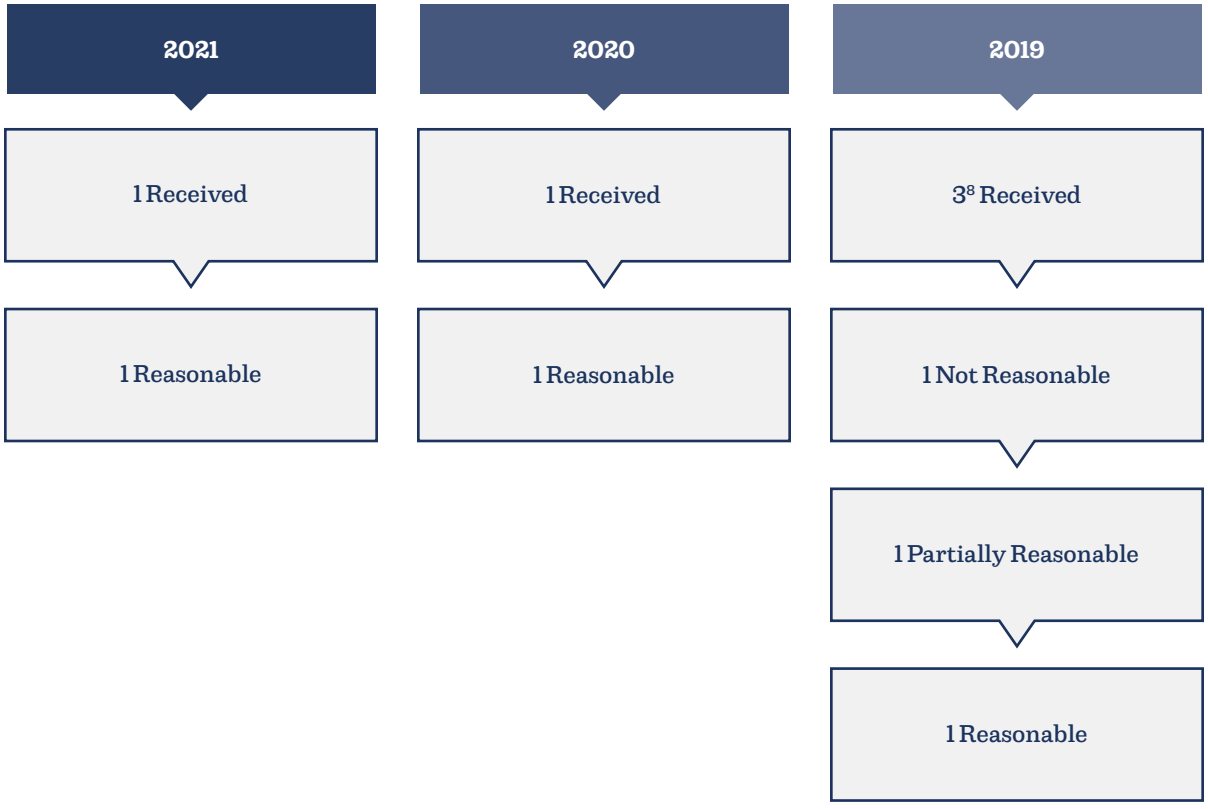
Authorizations for the retention of foreign datasets[6], Section 17 of the IC Act



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

Authorizations for the querying of a dataset in exigent circumstances[7], Section 18 of the IC Act

Determinations of classes of acts or omissions, Section 19 of the IC Act



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

8 In 2019, the Minister of Public Safety 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.

Case Summaries

CASE SUMMARIES

AUTHORIZATIONS ISSUED UNDER THE *COMMUNICATIONS SECURITY ESTABLISHMENT ACT*

I. Summary

In 2021, the Intelligence Commissioner (IC) reviewed five ministerial authorizations issued by the Minister of National Defence related to activities of the Communications Security Establishment (CSE): three Foreign Intelligence Authorizations and two Cybersecurity Authorizations.

The IC found that the Minister's conclusions were reasonable in four of the five authorizations and approved them. With respect to one Foreign Intelligence Authorization, the IC found that the Minister's conclusions were reasonable, with the exception of those relating to a specific activity. The IC found that the Minister's conclusions lacked information on the nature of the activity described and on how such activity would be reasonable and proportionate. The IC was of the view that the Minister's conclusions did not bear the essential elements of reasonableness: justification, transparency, intelligibility and did not establish whether they were justified in relation to the relevant factual and legal contexts. This Foreign Intelligence Authorization was partially approved. The IC determined that he must not approve the Foreign Intelligence Authorization relating to this specific activity.

Some improvements and issues noted by the IC are detailed in the section entitled Opportunities for Improvement. The IC issued all of his decisions within the 30-day statutory time limit. 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

22 (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 CSE's mandate is to collect 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. 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 *Communications Security Establishment Act* (CSE Act) permits the Minister of National Defence to issue a Foreign Intelligence Authorization to CSE. This authorization, when approved by the IC, authorizes 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 activities would constitute offences under 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 make up 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. To address this concern, the CSE Act permits the Minister of National Defence to issue a Cybersecurity Authorization to CSE. This authorization, when approved by the IC, authorizes CSE to access the information infrastructure of either a federal institution or a designated non-federal institution to help protect the information infrastructure from mischief, unauthorized use or disruption. Effectively, this allows for the interception of private communications – which would otherwise constitute 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

This year, the IC approved four of the five authorizations provided by the Minister of National Defence. The other authorization was partially approved as the IC found that the Minister's conclusions regarding a specific activity were not reasonable.

In his decisions, the IC raised noteworthy issues that are elaborated here. Overall, these issues were not detrimental to the reasonableness of the Minister's conclusions or the IC's complete or partial approval of the authorizations.

Foreign Intelligence Authorizations

(i) Absence of Ministerial Condition If Contravention of Other Acts of Parliament Not Identified in the Application

The CSE Act stipulates that activities carried out in furtherance of CSE's mandate must not contravene any Act of Parliament unless they are carried out under a ministerial authorization, which must be approved by the IC. CSE identified in its applications Acts of Parliament that may be contravened while conducting activities under ministerial authorization.

In three of the applications for ministerial authorization, the Chief of CSE indicated that CSE may contravene other Acts of Parliament beyond those specifically listed by CSE while conducting the activities under the authorization. Specifically, the Chief of CSE undertook to notify the Minister if another Act of Parliament, including a provision of the *Criminal Code*, not listed in the application, is contravened. Despite this undertaking by the Chief, the Minister did not impose a condition to this effect in the ministerial authorizations. The IC considered that although this may have been an oversight, he expressed the view that such a condition should be included by the Minister in future authorizations.

(ii) Lack of Achieved Outcomes

In two of his decisions, the IC felt that although a good number of contextual examples related to achieved outcomes had been provided in the application records, he found that such examples did not provide a comprehensive overview of achieved outcomes. The IC remarked that achieved outcomes directly contribute to establishing the necessity, as well as, occasionally, the reasonableness and proportionally, of the activities authorized. Stating the achieved outcomes also fosters transparency and supports the Minister in his decision-making.

Although the applications this year provided more concrete examples than the previous year, the IC was of the view that comprehensive and current information on achieved outcomes would bolster the Minister's consideration in determining in his or her conclusions whether the foreign intelligence acquisition activities are necessary, reasonable and proportionate.

Cybersecurity Authorizations

(i) Lack of achieved outcomes

With respect to the Cybersecurity Authorizations, the IC was satisfied that the Minister's conclusions demonstrated that he had reasonable grounds to believe, based on the credible and compelling information found in the application and generally in the record, that the Cybersecurity Authorizations were necessary, and that the conditions for issuing them were met.

However, the IC expressed his opinion on some elements found in one of CSE's applications and the Minister's authorization to inform future applications and authorizations. In particular, notwithstanding the information provided by CSE, the IC reiterated that the inclusion of updated achieved outcomes would better support the facts and statements made in the application, which in turn would bolster the Minister's conclusions that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it, as set out in subsections 34(1) and (3) of the CSE Act, are met.

CASE SUMMARIES

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

I. Summary

The *National Security Act*, 2017, amended the *Canadian Security Intelligence Service Act* (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 the Canadian Security Intelligence Service (CSIS) to collect, retain, query and exploit datasets in the course of performing its duties and functions.

In 2021, the Intelligence Commissioner (IC) reviewed one determination of classes of Canadian datasets and one determination of classes of acts or omissions made by the Minister of Public Safety. One authorization on the query of a Canadian dataset in exigent circumstances and one authorization to retain a foreign dataset, both issued by the Director of CSIS, were also reviewed by the IC.

With reference to both determinations of classes made by the Minister, the IC found that the Minister's conclusions were reasonable, and he approved the determinations. The IC also found the Director's conclusions reasonable and approved the authorization to query a Canadian dataset in exigent circumstances as well as the authorization to retain a foreign dataset. Some improvements and issues noted by the IC are detailed in the section entitled Opportunities for Improvement.

The IC issued all of his decisions within the statutory time limit.

II. Background

What are determinations of classes of Canadian datasets and when are they required?

CSIS has the authority to collect and retain information and intelligence, to the extent that it is strictly necessary, respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. CSIS may also analyze this information. Additionally, CSIS may gather information, in the form of a dataset containing 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 determines, by order, 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 the performance of 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 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 Canadian laws 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 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 Director's authorization comes into effect 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, if the IC is satisfied that the conclusions at issue are reasonable once the conditions are attached.

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 the CSIS Act 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 authorization to retain the dataset; 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 the 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 or she must perform "as soon as feasible."

What are determinations of classes of otherwise unlawful acts or omissions and when are they required?

When carrying out CSIS's information and intelligence collection duties and functions, designated CSIS employees and persons acting under their direction may need to engage in acts or omissions that would be unlawful without an approved determination by the Minister of Public Safety to do so. To that end, 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, as well as in the context of 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 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 two determinations made by the Minister of Public Safety and two authorizations issued by the Director of CSIS. The IC approved both the ministerial determinations and the Director's authorizations. The IC also raised some noteworthy issues in his decisions that are elaborated here. Overall, these issues were not detrimental to the reasonableness of the decision-maker's conclusions or the IC's approval of the determinations and authorizations.

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

The IC reviewed one determination of four classes of Canadian datasets made by the Minister of Public Safety. The IC found that the Minister's conclusions were reasonable and consequently approved the determination of these four classes. The IC also noted that the minor issues he had identified concerning the previous determination had been addressed to his satisfaction.

The Intelligence Commissioner's review of an authorization to retain a foreign dataset

The IC reviewed one authorization to retain a foreign dataset issued by the Director of CSIS as a designated person. The IC was satisfied that the Director's conclusions demonstrated that the legislative requirements were met: the dataset was a foreign dataset; the retention of the dataset was likely to assist CSIS in the performance of its duties and functions; and CSIS complied with its obligations under section 11.1 of the CSIS Act. These obligations are mainly to delete any information containing a reasonable expectation of privacy relating to the physical and or mental health aspect of an individual and to remove any information from the dataset relating to a Canadian or person in Canada. The contents of the Director's authorization also reflected those that are prescribed in subsection 11.17(2) of the CSIS Act. The IC found that the Director's conclusions, which served as a basis for authorizing the retention of the foreign dataset, were reasonable and consequently approved the authorization to retain the foreign dataset. This dataset will be retained for five years.

The IC did note, though, that a review of the record revealed that efforts were made to address most of the remarks and inconsistencies raised in his 2020 decision relating to the retention of a foreign dataset. That being said, the Director's role as administrative decision-maker, in this instance, is one delegated by the Minister pursuant to the CSIS Act. This delegated role is distinct from the Director's duties and functions provided for in statute. In this specific context, the relationship between the Director and CSIS is fundamentally different.

Although the IC was satisfied that there was a general understanding of the Director's distinct role as a designated decision-maker, he noted that a review of some documents in the record may give the impression or the perception that the request from CSIS was being dealt with as an internal matter, and not as a request that CSIS is making to the Minister's delegate. As a designated person, the Director plays a role similar to the one exercised by the Minister. The Minister has a clearly defined arm's-length relationship in reality and in appearance, through a certain formality in the documentation CSIS submits to the Minister. Adding some formality to the process of submitting a request to the Director as a designated decision-maker would help clarify the Director's role. In addition, this way of proceeding would help to establish the necessary distance between CSIS as the applicant and the Director as the decision-maker, as well as, give the appearance of such a distance. This would, in turn, strengthen the Director's role as a designated administrative decision-maker.

The Intelligence Commissioner's review of an authorization to query a Canadian dataset in exigent circumstances

This was the IC's first review of an authorization to query a Canadian dataset in exigent circumstances. Based on his review of the Director of CSIS's authorization and of all the information provided on the record, the IC was satisfied that the conclusions at issue were reasonable. Consequently, he approved the query of a Canadian dataset in exigent circumstances. Nonetheless, the IC identified matters that could be improved in future authorizations, particularly how some of the Director's conclusions would have benefited from greater clarity.

Canadian Security Intelligence Service Act

QUERY OF DATASETS – EXIGENT CIRCUMSTANCES

11.22(1) The Director may authorize a designated employee to query a Canadian dataset that is not the subject of a valid judicial authorization issued under section 11.13 or a foreign dataset that is not the subject of a valid authorization under section 11.17 that has been approved by the Commissioner under the *Intelligence Commissioner Act*, if the Director concludes

(a) that the dataset was collected by the Service under subsection 11.05(1); and

(b) that there are exigent circumstances that require a query of the dataset

(i) to preserve the life or safety of any individual, or

(ii) to acquire intelligence of significant importance to national security, the value of which would be diminished or lost if the Service is required to comply with the authorization process under section 11.13 or sections 11.17 and 11.18.

The Intelligence Commissioner's review of the determination of classes of otherwise unlawful acts or omissions

The IC reviewed one determination made by the Minister of Public Safety for seven classes of otherwise unlawful acts or omissions.

The IC was satisfied that the Minister's conclusions demonstrated that the commission or directing of the acts or omissions in the identified classes was reasonable, having regard to CSIS's information and intelligence collection duties and functions, as well as any threats to the security of Canada that may be the object of such activities or any objectives to be achieved by such activities. The IC found that the Minister's conclusions were reasonable and consequently approved the determination of the seven classes.

The IC remarked, however, that the Minister should include a condition requiring to be notified in the event that other offences, which have neither been identified nor contemplated, are committed based on the acts or omissions defined in the approved classes. Furthermore, given the very specific nature of some of the unlawful acts or omissions, the IC was of the view that a further ministerial condition should be included requiring that the Minister be notified in the event that such an act or omission be committed during the authorized period.

Sharing, Collaboration and Looking Forward

SHARING OF DECISIONS AND REPORTS

The *Intelligence Commissioner Act* (IC Act) legislates the sharing of decisions and reports between the Intelligence Commissioner (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 or her 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 reports, prepared by NSICOP and NSIRA, if they relate to the IC's powers, duties or functions. In 2021, the IC received one such report from NSIRA.

INTERNATIONAL COLLABORATION

The Office of the Intelligence Commissioner (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 comprising Australia, Canada, New Zealand, the United Kingdom and the United States. 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 2021 FIORC meeting, held virtually and hosted by the New Zealand's Inspector-General of Intelligence and Security. The IC, as well as the ICO's Executive Director and Senior Legal Counsel, attended the meeting.

LOOKING FORWARD

As part of its support of the Government of Canada's ongoing commitment to transparency, the ICO has made considerable efforts to publish the IC's decisions on the ICO website. The ICO is working towards having the decisions available online as soon as feasible.

In light of the upcoming legislative review of the *National Security Act, 2017*, the IC is looking forward to sharing his viewpoint on the quasi-judicial function he has performed in the last three years, as part of Canada's national security accountability framework.

Biography

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 had been 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 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 Court of Québec 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

Annex B

LIST OF LEGISLATION RELATED TO THE INTELLIGENCE COMMISSIONER'S MANDATE

Intelligence Commissioner Act, S.C. 2019, c. 13, s. 50.

National Security Act, 2017, S.C. 2019, c. 13.

Communications Security Establishment Act, S.C. 2019, c. 13, s. 76.

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