ICO

Annual Report 2020

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 2563-6030

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, 2021

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 for tabling in Parliament, my annual report on my activities for the 2020 calendar year.

Sincerely,

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

Canada

Table of Contents

Intelligence Commissioner's Message

"I am pleased to present this second annual report of my activities as the Intelligence Commissioner (IC) for 2020. I am honoured to serve Canada in this review function of a quasi-judicial nature."

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

My mandate is set out in the *Intelligence Commissioner Act* (IC Act). The IC is an integral part of the decision-making process for certain national security and intelligence activities before they can be conducted. I review the 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).

In a period of significant disruption due to COVID-19, this year has presented many challenges, including balancing public health restrictions and operational requirements, as well as, instituting best practices in our first full year of operation. Amid the myriad of obstacles we faced in 2020, I remained steadfast in my commitment to meet all the statutory deadlines 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 continued support, dedication, resilience and flexibility, particularly during such uncertain times.

In addition, I would like to acknowledge that both ministers, as well as CSE and CSIS, displayed a continuous commitment to improving their processes and submissions, despite the challenges and the burden of the pandemic. Although this new oversight framework was only in its second year, I am encouraged by the positive developments of this past year.

Following this year's strategic resource planning exercise, the Office of the Intelligence Commissioner (ICO) received increased funding which will enable my office to acquire modern, effective and secure connectivity; to better meet mandatory security and information technology requirements; and to engage, as required, additional resources having technical or specialized knowledge. Furthermore, work with other government departments and organizations has continued to further strengthen ICO's technical security and internal infrastructure in a manner that is more effective, efficient and sustainable. Overall, ICO will be in a much stronger position to better discharge its mandate going forward, not only in the short term, but the longer term as well.

As part of the Canadian security and intelligence oversight and review community, we benefit greatly from working with our partners, both domestic and international. Although our participation was virtual rather than in person this year, it is more important than ever that we continue to reinforce the collaboration we have all built in the past with our Five Eyes Intelligence Oversight and Review Council colleagues. We have, and will continue, to maintain strong relationships, to explore mutual issues and concerns and to share best practices.

The pages that follow provide details of my activities, including statistics, during our first full year of operation. I encourage Canadians to read this report to learn more about my office's ongoing efforts to strengthen 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

Est.
2019

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

Mandate

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.

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 the Communications Security Establishment (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 the Canadian Security Intelligence Service (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 once approved by the IC following his or her 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 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.

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 their 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 records 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

CSE or CSIS prepares an application and provides it to its respective decision-maker[1]

If the decision-maker is satisfied that the legislative requirements are met, the decision-maker issues an authorization or makes a determination

The IC receives the application record, including the conclusions and all the information that was before the decision-maker when issuing the authorization or making the determination

The IC must provide a decision within 30 days after the day on which the IC receives notice of the authorization or determination, or within any other period agreed on by the IC and the decision-maker

ICO conducts an in-depth analysis of the application record for the IC to determine whether the conclusions reached by the decision-maker are reasonable

If the IC is satisfied that the conclusions reached by the decision-maker are reasonable, the IC must approve the authorization or determination in a written decision that sets out the reasons for doing so

The IC must provide the decision to the decision-maker whose conclusions are being reviewed

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

If the IC is not satisfied that the conclusions reached by the decision-maker are reasonable, the IC must not approve the authorization or determination in a written decision that sets out the reasons for doing so

The IC must provide the decision to the decision-maker whose conclusions are being reviewed

The activities specified in the authorization or the determination cannot proceed as it has not been approved by the IC

1 Minister of National Defence, Minister of Public Safety and Emergency Preparedness, 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 and Emergency Preparedness, 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:

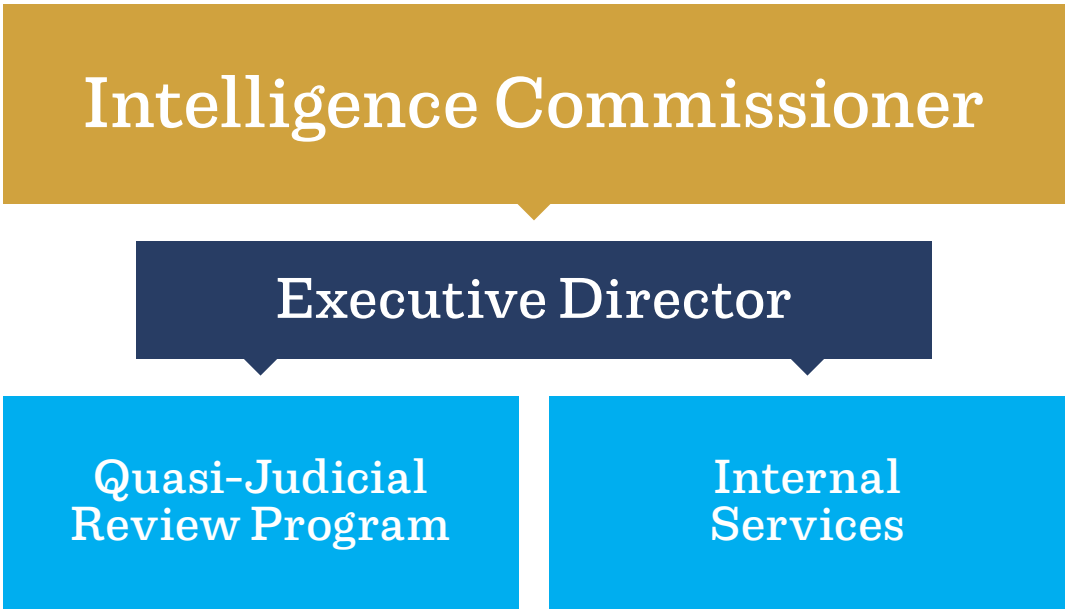
- **(a)** the Minister of Public Safety and Emergency Preparedness;
- **(b)** the *Minister*, as defined in section 2 of the *Communications Security Establishment Act*;
- **(c)** the Canadian Security Intelligence Service; and
- **(d)** the Communications Security Establishment.

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.



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. 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.

SNAPSHOT OF THE ORGANIZATION

Workforce

10 full-time equivalents

Cost of operations

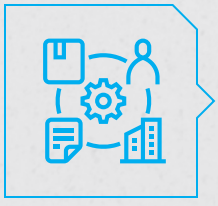
$2,061,805

Salaries and wages

$978,002

Contributions to employee benefit plans

$165,977



Other operating expenses

$917,826

Results for 2020

RESULTS

This report contains statistics for calendar year 2020. During that period, the Intelligence Commissioner (IC) reviewed six authorizations and determinations. All decisions were rendered within the 30-day statutory deadline 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.[2] The IC approved 100% of the authorizations and determinations.

Minister of National Defence	*Intelligence Commissioner Act*	Received	Reasonable	Not Reasonable	Partially Reasonable
Foreign Intelligence Authorizations	Section 13	3	3	-	-
Cybersecurity Authorizations	Section 14	1	1	-	-
Amendments to authorizations	Section 15	0	-	-	-
TOTAL		**4**	**4**	**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	0	-	-	-
Authorizations for the retention of foreign datasets[3]	Section 17	1	1	-	-
Authorizations for the querying of a dataset in exigent circumstances[4]	Section 18	0	-	-	-
Determinations of classes of acts or omissions	Section 19	1	1	-	-
TOTAL		**2**	**2**	**0**	**0**

Over time, the approval of authorizations and determinations by the IC will likely trend upwards, given that decision-makers should submit refined records responding to prior remarks made by the IC.

2 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.

3 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.

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

Case Summaries

CASE SUMMARIES

AUTHORIZATIONS ISSUED UNDER THE *COMMUNICATIONS SECURITY ESTABLISHMENT ACT*

I. Summary

In 2020, the Intelligence Commissioner (IC) reviewed four ministerial authorizations issued by the Minister of National Defence: three Foreign Intelligence Authorizations and one Cybersecurity Authorization.

In each case, the IC found that the Minister's conclusions were reasonable, and he approved the authorization. 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 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

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 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 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 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 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 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 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.

Communications Security Establishment Act

REPORT

52 (1) Within 90 days after the last day of the period of validity of an authorization issued under subsection 26(1), 27(1) or (2), 29(1), 30(1) or 40(1), the Chief must provide a written report to the Minister on the outcome of the activities carried out under the authorization.

COPY OF REPORT TO COMMISSIONER AND REVIEW AGENCY

52 (2) The Minister must provide the Commissioner and the Review Agency with a copy of a report on the outcome of the activities carried out under an authorization issued under subsection 26(1), 27(1) or (2) or 40(1).

III. Opportunities for Improvement

This year, the IC approved all four authorizations provided by the Minister of National Defence.

In his decisions, the IC noted that most of the inconsistencies raised in 2019 in the Foreign Intelligence and the Cybersecurity Authorizations were addressed. However, the IC raised other noteworthy issues that are detailed here. Overall, these issues were not detrimental to the reasonableness of the Minister's conclusions or the IC's approval of the authorizations.

Provision of information to the Intelligence Commissioner

Within 90 days after the last day of the period of validity of a Foreign Intelligence or a Cybersecurity Authorization, CSE must provide a written report to the Minister of National Defence on the outcome of the activities carried out by CSE under the Authorizations. A copy of this report is to be provided to the IC. In 2020, the IC received two reports for a Foreign Intelligence Authorization and one report for a Cybersecurity Authorization.

When the Minister of National Defence issues an authorization, the *Intelligence Commissioner Act* (IC Act) requires the Minister to provide the IC with all of the information that was before the Minister when issuing the authorization. This information constitutes the application record. This year, each application record submitted to the IC included a list of enclosed documents and a confirmation from the Minister that all information that was before him was included.

However, in one instance, the IC highlighted the fact that an application record referenced two CSE foundational governance documents that were not included in the application record. Given that it appeared that these documents established and formalized fundamental controls for CSE and that the Minister referred to them in his conclusions and authorization, the IC was of the view that such documents, or at minimum their relevant parts, ought to have been included in the application record and explained in the Minister's conclusions.

Foreign Intelligence Authorizations

In the case of the three Foreign Intelligence Authorizations, the IC raised some issues and identified some improvements in all of his decisions.

For example, in one instance, it was unclear whether or not a CSE activity was authorized, given a lack of information and clarity on the matter. The IC indicated that, if CSE intends to conduct this activity over the course of the authorization period, it ought to inform the Minister of National Defence in order to determine whether an amendment to the authorization is necessary.

In addition, the IC also found that the application records did not contain descriptions of achieved outcomes. Achieved outcomes contribute to establishing the reasonableness and proportionality of the activities to be authorized, foster transparency, and support the Minister in his decision making.

In another instance, the Minister did not provide conclusions supporting a specific activity he authorized. The Minister's conclusions also did not adequately address the legislative requirement concerning how unselected[5] information could not reasonably be acquired by other means.

In each case, however, the application record contained sufficient information for the IC to find that the Minister's conclusions were reasonable.

Cybersecurity Authorization

Contrary to CSE's 2019 Cybersecurity Authorization application records, but like this year's Foreign Intelligence Authorization application records, the 2020 application record did not contain descriptions of achieved outcomes. Also, some of the examples provided of activities undertaken were outdated and repetitive from last year. Further, the IC found that the application record did not indicate what cybersecurity services each client opted to receive.

Since ministerial authorizations preclude civil or criminal liability for authorized activities, the IC emphasized that CSE should inform the Minister of National Defence when planned activities for the future are authorized and deployed for the first time during the authorization period. This would provide the Minister with the opportunity to determine if the deployed activities conform to the activities described in the application record, or whether an amendment to the authorization is necessary. The IC also stated that the Minister of National Defence should be informed if CSE contravenes an Act of Parliament not listed in its application during the authorization period.

The application record, however, contained sufficient information for the IC to find that the Minister's conclusions were reasonable.

5 Section 2 of the CSE Act defines the term *unselected*, with respect to information, as meaning "that the information is acquired, for technical or operational reasons, without the use of terms or criteria to identify information of foreign intelligence interest."

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 2020, the Intelligence Commissioner (IC) reviewed one determination of classes of acts or omissions made by the Minister of Public Safety and Emergency Preparedness and one authorization issued by the Director of CSIS on the retention of a foreign dataset.

In the case of the determination of classes of acts or omissions, the IC found that the Minister's conclusions were reasonable and he approved the determination. The IC also found the Director's conclusions reasonable and approved 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 his decisions within the 30-day statutory deadline. During this reporting period, the IC did not receive for review any determinations of classes of Canadian datasets, or authorizations 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?

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 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 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.

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 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 the IC perform "as soon as feasible."

What are determinations of classes of otherwise unlawful acts or omissions and when are they 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 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 sections12, 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 one determination made by the Minister of Public Safety and Emergency Preparedness and one authorization issued by the Director of CSIS. The IC approved both the determination and the authorization. The IC also raised some noteworthy issues. Overall, these issues were not detrimental to the reasonableness of the decision-makers' conclusions or the IC's approval of the determination and authorization.

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

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

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 also identified a minor matter: the Minister's conclusion regarding a particular class did not reflect this year's title of the class, but reflected last year's title instead. The IC was satisfied that this inconsistency was essentially an oversight. Although this did not affect the IC's review of the reasonableness of the Minister's conclusions, this could be improved in future determinations.

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

This was the IC's first review of an 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 to delete any information containing a reasonable expectation of privacy relating to the physical or mental health of an individual and to remove any information from the dataset relating to a Canadian or a person in Canada. The contents of the Director's authorization also met the requirements prescribed by subsection 11.17(2) of the CSIS Act. The IC found that the Director's conclusions were reasonable and consequently approved the authorization to retain the foreign dataset. This dataset will be retained for five years.

Timeline

The following explains the legislative deadline relating to the evaluation of the foreign dataset and some of the matters the IC raised when reviewing the application record. These matters did not affect the IC's review of the reasonableness of the Director's conclusions.

The dataset requested for retention was an existing CSIS dataset that was deemed to be collected on the day that the modifications to the CSIS Act came into force on July 13, 2019. From then, CSIS had 90 days to evaluate the dataset, confirm that the dataset was foreign and bring the dataset to the attention of the Director so as to enable him, as the designated person, to authorize its retention. CSIS did so and provided a request for the retention of the dataset to the Director on the due date, October 11, 2019, thus respecting the legislative requirement of the CSIS Act. The Director authorized the retention of the dataset in November 2020. The CSIS Act does not impose a timeframe for the decision-maker to authorize the retention after the dataset has been brought to his or her attention.

During the one-year period it took the Director to make his authorization, he met with CSIS concerning its written request and considered the interpretation of the "likely to assist" threshold, found in paragraph 11.17(1)(*b*) of the CSIS Act, as well as obtained technical explanations. During this period, CSIS was also operationally impacted by the COVID-19 pandemic.

Remarks

The IC expressed his opinion on some aspects of the application record to inform future requests and authorizations. The IC is responsible to review the conclusions, or reasons, on the basis of which the Director of CSIS issued an authorization for the retention of a foreign dataset. The IC determined that there were some matters where the Director's conclusions were insufficient or non-existent. In the context of his quasi-judicial review, the IC applied administrative law principles and considered the application record as a whole in order to infer information in the Director's conclusions. The application record provided insight on the Director's reasons on these matters. In instances where there were insufficient or non-existent conclusions, the IC deferred to the Director's expertise concerning the handling of dataset backups, as well as his expertise in determining that the information contained in the dataset would likely assist CSIS in the performance of its duties and functions.

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 2020, 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.

LOOKING FORWARD

In the year ahead, the ICO will explore the possibility of publishing redacted and translated versions of the IC's decisions on the ICO website.

The ICO will undertake research and consultations regarding best practices from the national and international security and intelligence community. Looking forward, these insights will help contribute to ongoing efforts to strengthen Canada's national security through greater transparency.

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 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 Related to the Intelligence Commissioner's Mandate

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.