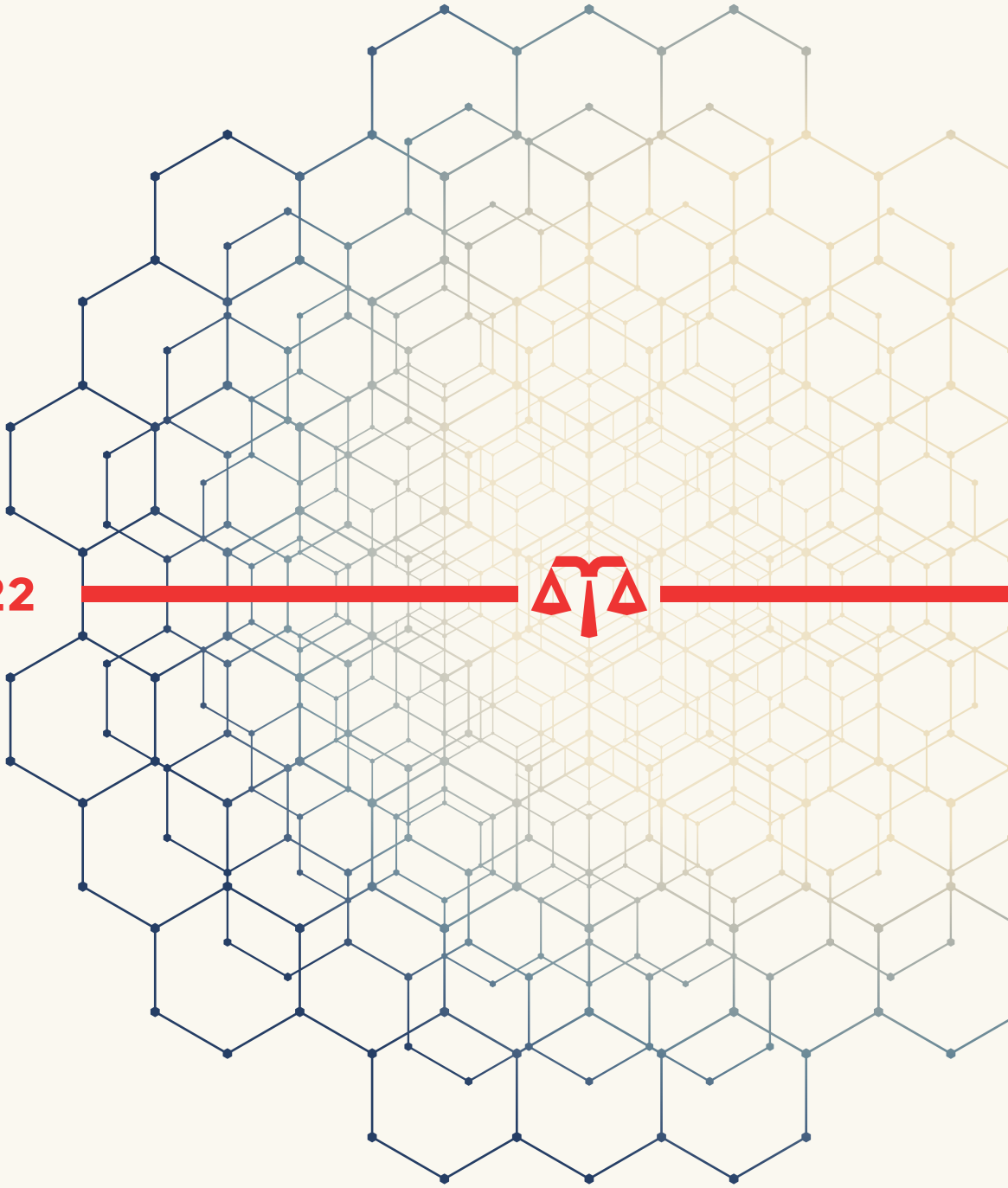
Annual Report

2022



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 (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

March 31, 2023

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 the activities for the 2022 calendar year, for your submission to Parliament.

Sincerely,

The Honourable Simon Noël, K.C.
Intelligence Commissioner

Canada

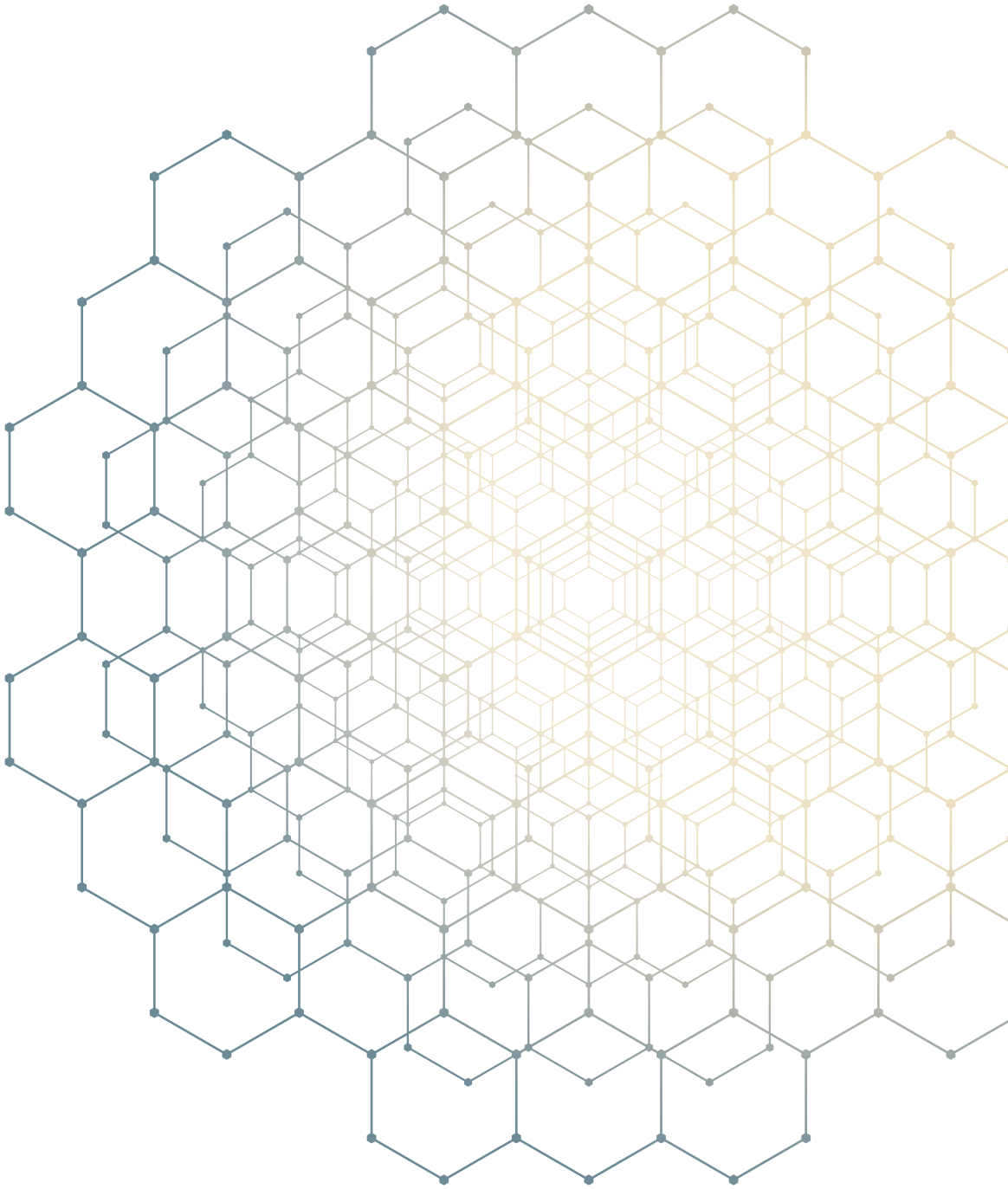


TABLE OF CONTENTS

INTELLIGENCE COMMISSIONER'S MESSAGE

I am of the view that my *raison d'être* as Intelligence Commissioner is to ensure the preservation of the required balance between national security interests on the one hand, and respect for the rule of law, the *Canadian Charter of Rights and Freedoms*, as well as the privacy rights of Canadians and persons in Canada, on the other.

The Honourable Simon Noël, K.C.
Intelligence Commissioner

I am pleased to present my first annual report as Intelligence Commissioner with respect to the activities of the Office of the Intelligence Commissioner for 2022.

Before outlining what I hope to bring to the role of Intelligence Commissioner, I would like to note the significant contribution made by my predecessor, the Honourable Jean-Pierre Plouffe, the first Intelligence Commissioner of Canada. It was under his direction that the Office of the Intelligence Commissioner (ICO) was established pursuant to the *Intelligence Commissioner Act* in 2019 as part of the changes to Canada's national security framework. The decisions, up to September 2022, rendered during his tenure set the tone in applying the new legislation's advance oversight quasi-judicial mandate for reviewing certain national security and intelligence activities before they can be undertaken by the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS).

I would like to thank the staff at the ICO for facilitating my transition to my new role. I look forward to working with them to successfully deliver on my legislative mandate.

On October 1, 2022, I was privileged to be appointed Intelligence Commissioner of Canada. It is a significant responsibility to be asked to play a key role in maintaining the proper balance between national security interests, respect for the rule of law, and the rights and freedoms of Canadians. I accepted the position because I have been involved, in one way or another, in national security and intelligence matters since 1979; I felt that the experience and insights I have gained during those years would enable me to make a useful contribution to this uniquely Canadian function.

The *Intelligence Commissioner Act* requires the Commissioner to review and determine whether the conclusions of the Minister of National Defence, the Minister of Public Safety and, where applicable, the Director of the Canadian Security Intelligence Service (CSIS) which led to the issuance of certain ministerial authorizations or determinations of classes are reasonable.

When determining whether, in the context of national security, such conclusions are reasonable, I believe that I am to carefully consider and weigh the privacy rights and other interests of Canadians and persons in Canada that may be impacted by such authorizations or determinations but also that they are in conformity with the rule of law. I consider this as part of my role as Commissioner, keeping in mind the importance of ensuring the national security of all Canadians.

In the inherently complex world of intelligence and national security, public scrutiny and rising expectations of the activities conducted by the CSE and CSIS are of the utmost importance. Although their mandates require that they operate behind a veil of secrecy, their actions must nonetheless be subject to some objective supervision and control. Fundamental to achieving this goal are greater transparency and enhanced accountability; by ensuring the application of these principles, public trust and confidence in Canada's national security framework will be strengthened. For my part, I commit to provide Canadians access to my decisions by publishing them in a timely fashion on the ICO website, in both official languages, and with the fewest redactions possible. I also intend to be as informative as possible regarding my function so that Canadians are properly informed and understand the work undertaken.

Furthermore, as Intelligence Commissioner, I look forward to maintaining a collaborative working relationship with my counterparts in the Canadian security and intelligence oversight and review community, as well as with Canada's Five Eyes partners in Australia, New Zealand, the United Kingdom and the United States.

I hope this report will give Canadians a better understanding of the mandate of the Intelligence Commissioner, which is essential in the furtherance of national security interests, individual rights and freedoms, and public transparency.

The Honourable Simon Noël, K.C.
Intelligence Commissioner

PART I

MANDATE AND ORGANIZATION

About the Office of the Intelligence Commissionner

Est.
2019

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

The IC reports annually to Parliament through the Prime Minister

MANDATE

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

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
- 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.

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 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.

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

"In order to better understand the role of the Intelligence Commissioner, I would like to quote from the Minister of Justice's *Charter* Statement which was prepared when Bill C-59 was tabled.

> *In addition, Part 2 of Bill C-59, the Intelligence Commissioner Act, would establish an independent quasi-judicial Intelligence Commissioner, who would assess and review certain Ministerial decisions regarding intelligence gathering and cyber security activities. This would ensure an independent consideration of the important privacy and other interests implicated by these activities in a manner that is appropriately adapted to the sensitive national security context.*
>
> ...
>
> *A key change proposed in Bill C-59 is that the activities would also have to be approved in advance by the independent Intelligence Commissioner, who is a retired superior court judge with the capacity to act judicially."*

The Honourable Simon Noël, K.C.
Intelligence Commissioner

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, this term has been associated with the process of judicial review of administrative decisions. While the IC must be a retired judge of a superior court, he or she is not a court of law. Review by the IC is not, as such, a judicial review. Rather, the IC is responsible for conducting a quasi-judicial review of the decision maker's conclusions.

In decisions rendered, the IC accepted that when Parliament used the term "reasonable" in the IC Act, it intended to give to that term the meaning it has been given in administrative law jurisprudence. This means the IC must be satisfied that the decision makers' conclusions bear the essential elements of reasonableness: justification, transparency and intelligibility. The IC must also determine whether the conclusions are justified in relation to the relevant factual and legal contexts. 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 IC must conduct reviews in accordance with the appropriate administrative law principles, which includes taking into consideration the roles of the decision maker and the IC, as well as the overall objectives of the IC Act, the CSE Act and the CSIS Act.

"When conducting a quasi-judicial review, it is important to refer to the objectives of Bill C-59 the *National Security Act, 2017*, SC 2019, c 13 and its Preamble, which led to the creation of the IC Act, the CSE Act, and made important amendments to the CSIS Act. I consider the following to be directly related to my role as Intelligence Commissioner:

Whereas a fundamental responsibility of the Government of Canada is to protect Canada's national security and the safety of Canadians;

Whereas that responsibility must be carried out in accordance with the rule of law and in a manner that safeguards the rights and freedoms of Canadians and that respects the Canadian Charter of Rights and Freedoms;

Whereas enhanced accountability and transparency are vital to ensuring public trust and confidence in Government of Canada institutions that carry out national security or intelligence activities;

Whereas those institutions must always be vigilant in order to uphold public safety;

Whereas those institutions must have powers that will enable them to keep pace with evolving threats and must use those powers in a manner that respects the rights and freedoms of Canadians."

The Honourable Simon Noël, K.C.
Intelligence Commissioner

Review Process ::

The IC's review process begins with an application that CSE prepares and provides to the Minister of National Defence, or that CSIS prepares and provides to the Minister of Public Safety or, where applicable, the Director of CSIS. If the above mentioned decision maker is satisfied that the application meets legislative requirements, they:

- issue an authorization, that is:
  - a Cybersecurity Authorization (federal or non-federal infrastructure) for CSE;
  - a Foreign Intelligence Authorization for CSE;
  - an Amendment to a Cybersecurity or a Foreign Authorization for CSE;
  - an authorization for CSIS to retain a foreign dataset; or
  - an authorization for CSIS to query a Canadian or a foreign dataset in exigent circumstances; or
- make a determination of:
  - classes of Canadian datasets collected by CSIS; or
  - classes of acts or omissions that would otherwise constitute offences when carried out by CSIS.

In doing so, the decision maker must provide conclusions, or reasons, explaining and justifying their decisions.

The IC's review is to determine whether the Minister's conclusions, on the basis of which the authorization or the determination was issued, are reasonable.

According to the IC Act, the decision maker whose conclusions are being reviewed, 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 Cabinet confidence.

In each review, the IC, supported by the Office of the Intelligence Commissioner, 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.

"I recognize that my independent quasi-judicial review must take into consideration the reasonableness of the Minister's conclusions as they relate to the privacy interests of Canadians and persons in Canada as well as other relevant and important interests in the context of national security, keeping in mind the legislative texts at play."

The Honourable Simon Noël, K.C.
Intelligence Commissioner

Review Process Map ::

CSE or CSIS prepares an application and provides it to its respective decision maker[2]

::

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 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

::

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

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.

It must be done at a time when no application is being reviewed by the IC. This transfer of knowledge is essential to ensure that classified contextual or technical information is known to the IC, which in turn helps to enhance the quality of future decisions.

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* [the Minister of National Defence];

(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 [King'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

::

EXECUTIVE DIRECTOR

::

Quasi-Judicial Review Program

::

Internal Services

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

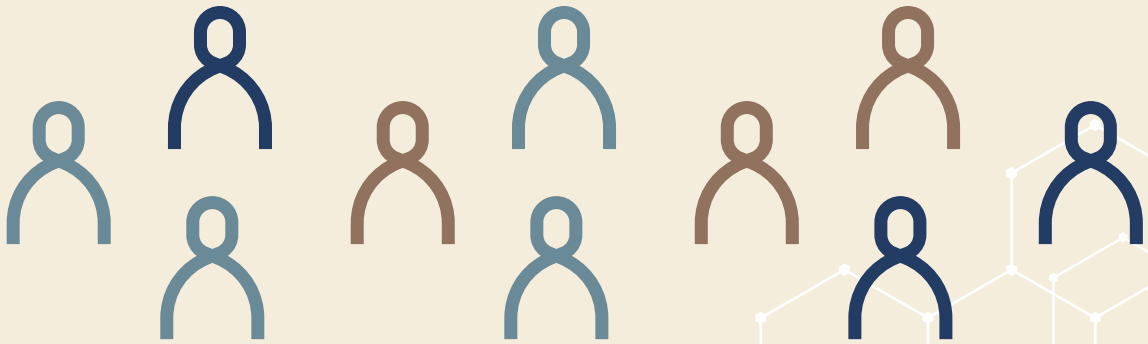
APPOINTMENT

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

$2,278,497

Cost of operations

Salaries and wages

$1,072,859

Other operating expenses

$1,065,829

Contribution to employee benefit plans

$139,809

PART 2

RESULTS

This report contains statistics for calendar year 2022. During that period, the Intelligence Commissioner (IC) reviewed nine authorizations and determinations (seven by Commissioner Plouffe and two by Commissioner Noël).[3] 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.[4]

The IC approved 89% of the authorizations and determinations.

Minister of National Defence	*Intelligence Commissioner Act*	Received	Reasonable	Not Reasonable	Partially Reasonable	IC Remarks[5]
Foreign Intelligence Authorizations	Section 13	3	3	-	-	-
Federal Infrastructure Cybersecurity Authorizations	Section 14	1	-	-	1	-
Non-federal Infrastructure Cybersecurity Authorizations	Section 14	2	2			6
Amendments to authorizations	Section 15	-	-	-	-	-
Total		6	5	-	1	6

Minister of Public Safety	*Intelligence Commissioner Act*	Received	Reasonable	Not Reasonable	Partially Reasonable	IC Remarks[5]
Determinations of classes of Canadian datasets	Section 16	1	1	-	-	1
Authorizations for the retention of foreign datasets[6]	Section 17	1	1	-	-	1
Authorizations for the querying of a dataset in exigent circumstances[7]	Section 18	0	-	-	-	-
Determinations of classes of acts or omissions	Section 19	1	1	-	-	2
Total		3	3	-	-	4

3 Commissioner Plouffe's term ended September 30, 2022 and Commissioner Noël was appointed October 1, 2022.

4 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.

5 Remarks are pertinent comments made which reflect directly on the authorization/determination under review. Remarks are made to improve the content of further applications but also to include some areas of concern. Remarks are included in the "Case Summaries" section of the Annual Report.

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.

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

Results – 4 years ::

MINISTER OF NATIONAL DEFENCE

Foreign Intelligence Authorizations, Section 13 of the IC Act

2022	2021	2020	2019
3 Received	3 Received	3 Received	3 Received
::	::	::	::
3 Reasonable	2 Reasonable	3 Reasonable	3 Reasonable
	::		
	1 Partially Reasonable		

Cybersecurity Authorizations for activities to help protect federal infrastructures, Section 14 of the IC Act

2022	2021	2020	2019
1 Received	1 Received	1 Received	1 Received
::	::	::	::
1 Partially Reasonable	1 Reasonable	1 Reasonable	1 Reasonable

Cybersecurity Authorizations for activities to help protect non-federal infrastructures, Section 14 of the IC Act

2022	2021	2020	2019
2 Received	1 Received	0 Received	1 Received
::	::		::
2 Reasonable	1 Reasonable		1 Reasonable

Amendments to Authorizations, Section 15 of the IC Act

2022	2021	2020	2019
0 Received	0 Received	0 Received	0 Received

MINISTER OF PUBLIC SAFETY

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

2022	2021	2020	2019
1 Received	1 Received	0 Received	1 Received
::	::	::	::
1 Reasonable	1 Reasonable		1 Reasonable

Authorizations for the retention of foreign datasets[8], Section 17 of the IC Act

2022	2021	2020	2019
1 Received	1 Received	1 Received	0 Received
::	::	::	
1 Reasonable	1 Reasonable	1 Reasonable	

Authorizations for the querying of a dataset in exigent circumstances[9], Section 18 of the IC Act

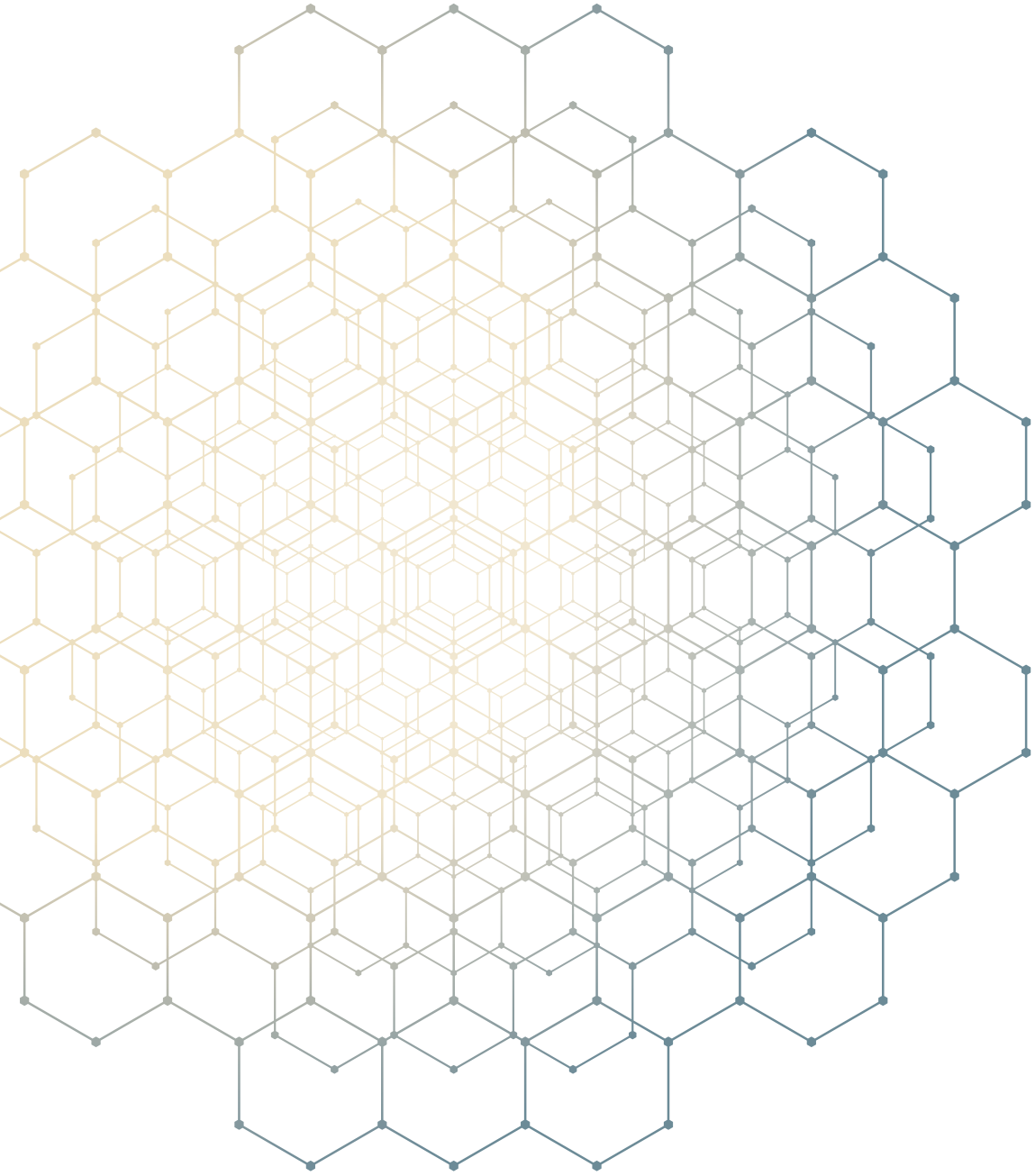
2022	2021	2020	2019
0 Received	1 Received	0 Received	0 Received
	::		
	1 Reasonable		

8 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.

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

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

2022	2021	2020	2019
1 Received	1 Received	1 Received	3 Received[10]
::	::	::	::
1 Reasonable	1 Reasonable	1 Reasonable	1 Reasonable
			::
			1 Not Reasonable
			::
			1 Partially Reasonable



10 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* ::

1. SUMMARY

The mandate of the Communications Security Establishment (CSE) has five aspects. Two of them relate to the jurisdiction of the Intelligence Commissioner (IC): cybersecurity and information assurance; and foreign intelligence.

The IC conducts a quasi-judicial review pursuant to the *Communications Security Establishment Act* (CSE Act) in three types of instances. These instances relate to the conclusions reached by the Minister of National Defence when issuing:

- a Cybersecurity Authorization, which can be related to a federal or non-federal infrastructure;
- a Foreign Intelligence Authorization; or
- an Amendment to a Cybersecurity or Foreign Intelligence Authorization.

These authorizations are explained in the "Background" section.

In 2022, the IC reviewed, in the first three months of his mandate, two non-federal Cybersecurity Authorizations issued by the Minister of National Defence related to activities of the CSE.

In both instances, the IC determined that the Minister's conclusions were reasonable. The IC also made remarks to inform future applications and authorizations, which are detailed in the "Cybersecurity Decisions Rendered" and "Foreign Intelligence Decisions Rendered" sections.

During his nine-month tenure in 2022, the former IC reviewed four ministerial authorizations issued by the Minister of National Defence in relation to activities carried out by CSE: one Cybersecurity Authorization for federal infrastructure and three Foreign Intelligence Authorizations.

With respect to the Cybersecurity Authorization, the former IC found that the Minister's conclusions were reasonable, except for those relating to a specific activity. The former IC determined that the Minister's conclusions lacked information on how the authorized activity is covered by subsection 27(1) of the CSE Act. The former IC was of the view that the Minister's conclusions did not bear the essential elements of reasonableness: justification, transparency and intelligibility, and did not establish whether the authorized activity was justified in relation to the relevant factual and legal contexts. This Cybersecurity Authorization was therefore partially approved.

For the three Foreign Intelligence Authorizations, the former IC was satisfied with the Minister's conclusions and approved them.

All six decisions of the respective ICs made under the CSE Act were rendered within the 30-day statutory time limit.

During this reporting period, no amended Cybersecurity or Foreign Intelligence Authorizations were submitted for review.

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

1) What are Foreign Intelligence Authorizations and when are they required?

One aspect of CSE's mandate – foreign intelligence – is to collect signals intelligence on foreign targets located outside of Canada. This information is about the capabilities, intentions or activities of foreign targets in relation to international affairs, defence or security. These CSE 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 Canadian law, a law of any foreign state, or infringe on the reasonable expectation of privacy of a Canadian or a person in Canada.

To address this concern, the CSE Act permits the Minister of National Defence to issue a Foreign Intelligence Authorization to CSE. When approved by the IC, this authorization allows CSE to carry out, on or through the global information infrastructure, any activity specified in the authorization to further its foreign intelligence mandate.

In practice, a Foreign Intelligence Authorization issued by the Minister and approved by the IC authorizes CSE to carry out activities that are consistent with its mandate. In the absence of such authorization, however, some activities undertaken by CSE would constitute offences under the *Criminal Code*. They include, for example, the interception of private communications, or the conduct of certain activities necessary to keep an activity covert or to enable the acquisition of information for providing foreign intelligence.

2) What are Cybersecurity Authorizations and when are they required?

In another aspect of its mandate, cybersecurity and information assurance, CSE provides advice, guidance and services to help protect Government of Canada electronic information and information infrastructures – that is, federal 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 – that is, non-federal infrastructures – assistance in writing. Such designation generally pertains to organizations and companies falling within those sectors that make up Canada's critical infrastructure. Non-federal infrastructures can involve, for example, energy, finance, and information and communications technology.

Cybersecurity activities carried out by CSE 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 entity or a designated non-federal entity to help protect the information infrastructure from mischief, unauthorized use or disruption. For example, should CSE's cybersecurity activities result in the interception of private communications – which would otherwise be an offence under Part VI of the *Criminal Code* – the interception is permitted, as long as it 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

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).

III. CYBERSECURITY DECISIONS RENDERED

This year, the IC approved two Cybersecurity Authorizations for non-federal infrastructures provided by the Minster of National Defence. In the two decisions, the IC made some remarks, which did not alter his findings regarding the reasonableness of the Minister's conclusions.

For his part, the former IC partially approved one federal Cybersecurity Authorization, finding that the Minister's conclusions regarding a specific activity were not reasonable.

1. First Cybersecurity Authorization for a non-federal infrastructure

In 2022, a non-federal entity made a request to CSE asking that it deploy cyber defence solutions to assist in the protection of the electronic information and information infrastructure under its control and supervision. This non-federal entity holds information of importance to the Government of Canada, including personal information of Canadians and persons in Canada. Satisfied that the legislative requirements were met, the Minister issued a Cybersecurity Authorization. Following his quasi-judicial review, the IC determined that the Minister's conclusions were reasonable and approved the Cybersecurity Authorization.

In his decision, the IC made four remarks regarding the importance of obtaining substantive information as part of the documentation submitted in support of a ministerial authorization to be reviewed. The IC was of the view that to assess whether a ministerial authorization is reasonable, he must be provided with substantive information.

The first remark pertains to a statement contained in the ministerial authorization allowing CSE to use the cyber threat information acquired under this Cybersecurity Authorization in other aspects of its mandate. The IC was of the view that the information provided to him neither provided an explanation for CSE to proceed this way nor did it provide the legal authority for doing so.

The second remark was in relation to the retention periods for information that CSE may acquire. In reference to the retention period of unassessed information, the IC suggested that the record should contain more specific information and concrete examples supporting CSE's explanation to retain such information.

As for the retention period of information assessed to be necessary or essential, the IC recognized that it follows identified policy and legislative requirements. Nonetheless, the IC would like to be provided with specific details of the identified requirements. As noted by the IC, some of the information retained by CSE will include information for which a Canadian or a person in Canada may have a reasonable expectation of privacy.

The third remark relates to solicitor-client communications. As required by legislation, within 90 days after the last day of the period of validity of a ministerial authorization, the Chief of CSE must provide the Minister with a written report on the outcomes of the activities carried out under the authorization. This includes the number of recognized solicitor-client communications used, analyzed, retained or disclosed. Including such information in CSE's application would have been of interest to the Minister as a reminder of the number of instances where solicitor-client communication was acquired and what became of such information. Furthermore, this information would have assisted the IC in answering any questions or concerns he may have had with the potential acquisition and use of solicitor-client communications. The IC was of the view that waiting up to 90 days after the expiration of an approved ministerial authorization is simply not adequate, keeping in mind the utmost importance of solicitor-client privilege, which is itself a principle of fundamental justice.

Finally, the fourth remark concerns the timing of when the IC ought to be advised of the contravention of other acts of Parliament. In the Cybersecurity Authorization, the Minister imposed specific conditions regarding this issue. The IC stated that should such a situation occur, he would expect to be advised of any contravention of other acts of Parliament prior to providing his approval of the ministerial authorization, as well as his reasons for doing so. As a result, any such contravention would be included in the materials before the Minister and the IC.

2. Second Cybersecurity Authorization for a non-federal infrastructure

CSE received information about a cyber threat to a non-federal entity that holds information of importance to the Government of Canada, including personal information of Canadians and persons in Canada. Shortly after being informed by CSE, the non-federal entity requested CSE's help to conduct cyber defence activities to assist in the protection of the information and information infrastructure under its control and supervision.

The Chief of CSE then submitted an application to the Minister of National Defence requesting approval of a Cybersecurity Authorization to carry out activities that may contravene acts of Parliament or that may risk interfering with the reasonable expectation of privacy of Canadians or a person in Canada. The application explained that the non-federal entity's current posture could not sufficiently identify and counter the cyber threat. CSE proposed solutions that would ensure that gaps are identified and that the non-federal entity's posture would be well positioned to protect critical information.

The Minister had reasonable grounds to believe that the ministerial authorization was necessary and that the conditions set out the CSE Act were met. Consequently, she issued a Cybersecurity Authorization.

In conducting his quasi-judicial review, the IC determined that the Minister's conclusions were reasonable with respect to the proposed cybersecurity activities described. The IC rendered his decision, approving the ministerial authorization and made two remarks.

The first remark deals with the lapse of time between the occurrence of the compromise and its reporting to CSE. The IC was of the view that the lack of information on this issue raised questions regarding the urgency for CSE to provide the non-federal entity with assistance. Obtaining more detailed information would have been beneficial to the Minister and the IC. Should CSE not been able to account for the lapse of time, an explanation should have been provided to the Minister and included in her conclusions.

The second remark relates to the information provided on the cyber threat actor. The IC acknowledged that he was provided with substantial and useful information on the issue. Going forward, the IC requested that all documents submitted in support of the ministerial authorization be dated. The IC also requested that all information pertaining to the activities of the cyber threat actor be as current as possible to assist the Minister and the IC in his review of the matter. If the information was not available, the Minister should have been informed, and provided an explanation in her conclusions.

3. Cybersecurity Authorization for a Federal Infrastructure

With the exception of one activity, the former IC approved the Cybersecurity Authorization for a federal infrastructure. He was satisfied that the Minister's conclusions demonstrated that she had reasonable grounds to believe, based on the credible and compelling information found in the application and generally in the record, that the authorization was necessary, and that the conditions for issuing it were met.

As for the activity that was not approved, the former IC determined that there was a lack of information in the Minister's conclusions and in the record establishing how the authorized activity is covered by subsection 27(1) of the CSE Act.

With no supporting information, or specific rationale, the former IC determined that the Minister's conclusions did not bear the essential elements of reasonableness: justification, transparency and intelligibility, and did not establish whether they were justified in relation to the relevant factual and legal contexts. Consequently, the specific activity in question was not approved by the former IC, and the Cybersecurity Authorization was partially approved.

IV. FOREIGN INTELLIGENCE DECISIONS RENDERED

This year, the former IC approved three Foreign Intelligence Authorizations issued by the Minister of National Defence.

The CSE Act stipulates with respect to a Foreign Intelligence Authorization that activities carried out in furtherance of CSE's mandate must not contravene any Act of Parliament unless they are carried out under the authorization. The authorization must be approved by the IC. In its applications to the Minister, CSE identified acts of Parliament that may be contravened while conducting activities under the authorization.

In the three applications for ministerial authorization, the Chief of CSE indicated that CSE risks contravening other acts of Parliament beyond those specifically listed by CSE while conducting the activities under the authorization. Specifically, the Chief of CSE committed to notifying the Minister if another Act of Parliament, including a provision of the *Criminal Code*, not listed in the application, is contravened. The Minister also imposed a condition to this effect in the authorizations.

The former IC also noted that the issues he had identified concerning previous authorizations had been addressed to his satisfaction.

CASE SUMMARIES

Authorizations Issued and Determinations Made under the *Canadian Security Intelligence Service Act* ::

1. SUMMARY

The *National Security Act, 2017*, amended the *Canadian Security Intelligence Service Act* (CSIS Act) to 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. The amendments also provide a justification framework, subject to certain limitations, for the commission of acts or omissions that would otherwise constitute offences.

The Intelligence Commissioner (IC) conducts a quasi-judicial review under the CSIS Act in four types of instances. Two relate to the conclusions reached by the Minister of Public Safety when making a determination of: (1) classes of Canadian datasets, or (2) classes of acts or omissions that would otherwise constitute offences (classes are explained in the "Background" section). Once every year, by order, the Minister determines these classes.

The other two instances relate to the conclusions reached by the Director of CSIS when issuing: (1) an authorization, as a person designated by the Minister of Public Safety, to retain a foreign dataset, or (2) an authorization to query a Canadian or foreign dataset in exigent circumstances.

In 2022, the former Intelligence Commissioner (former IC) issued three decisions relating to CSIS:

- one pertained to a determination of classes of Canadian datasets – the former IC found that the Minister's conclusions were reasonable and he approved the determination of classes;
- one was a determination of classes of acts or omissions – the former IC found that the Minister's conclusions were reasonable and he approved the determination of classes; and
- one was an authorization to retain a foreign dataset issued by the Director of CSIS – the IC found the Director's conclusions reasonable and approved it.

For all three decisions, the former IC noted some improvements and issues. that are detailed in the section "Decisions Rendered".

The former IC issued all three decisions within the statutory time limit.

This year, the Director of CSIS did not make a request for an authorization to query a Canadian or foreign dataset in exigent circumstances. However, in 2021 the former IC approved for the first time a ministerial authorization to query a Canadian dataset in exigent circumstances. In November 2021, CSIS made an application to the Federal Court of Canada for judicial authorization to retain two Canadian datasets. In March 2022, the court authorized their retention for two years.

II. BACKGROUND ON ACTIVITIES UNDER THE CSIS ACT

1) 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. The Minister shall at least once a year determine these classes of Canadian datasets and 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.

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

When carrying out its 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 that end, the Minister shall, by order, make 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 of any threats to the security of Canada that may be the subject of information and intelligence collection activities.

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

3) 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.

4) 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, 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 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."

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.

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.

III. DECISIONS RENDERED

During this reporting period, all decisions were rendered by the former IC, who reviewed two determinations of classes made by the Minister of Public Safety and one authorization issued by the Director of CSIS to retain a foreign dataset. The IC approved both ministerial determinations and the Director's authorization. The IC also raised some noteworthy issues in his decisions. Overall, these issues were not detrimental to the reasonableness of the decision maker's conclusions or the IC's approval of the determinations and the authorization.

1) 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 when discussing accountability measures, the Minister's conclusions asked the Director of CSIS to inform him how the classes were used, including examples of how querying or exploiting datasets generated results that were relevant to CSIS' duties and functions. Although the record did not contain specific examples, CSIS did provide potential scenarios depicting the use of the Canadian datasets. The IC recognized that the lack of specific examples may be due to the timing of CSIS' first application for judicial authorization in November 2021, and that specific examples would be available only if the Federal Court authorized the retention of the Canadian datasets. Nonetheless, the IC was of the view that it would have been preferable for the Minister to acknowledge this in his conclusions.

2) 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 eight 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 eight classes.

While satisfied that the Minister addressed both remarks made in the IC's 2021 decision on the determination of these classes, the IC took the opportunity to clarify the remark he made in relation to the proposed ministerial condition that should be included 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 class. He acknowledged that a determinative finding of all applicable and contemplated offences in a given proposed operational plan is not feasible. Consequently, his intent was simply to have the Minister informed, after the fact, if an offence that had not been explicitly contemplated was triggered by an act or omission undertaken by a designated employee or a directed source.

In his 2022 decision, the IC also made two remarks regarding CSIS's application, as well as the Minister's conclusions and determination. The IC noted that subsection 23(1) of the IC Act requires that he be provided with all information that was before the decision maker in making his or her determination, including any verbal information provided to the Minister. The IC was of the view that it would be preferable in those instances to be provided with distinct minutes or records of discussion.

In his second remark, the IC found that the title of the class that had been determined by the Minister was narrower than the acts and omissions described in his conclusions. The IC exceptionally gave deference to the Minister's expertise in determining a narrower class. The IC stated that there should be consistency between the titles of the classes determined by the Minister, the Minister's conclusions and the application presented to the Minister. Ultimately, the IC was satisfied that the inconsistency was an oversight that did not affect the reasonableness of the Minister's conclusions. He trusted that the title of the class would be amended in the next ministerial determination.

3) 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.

In his conclusions, the Director of CSIS informed the IC of a non-compliance incident where some records believed to relate to Canadians or persons in Canada were copied from the foreign dataset prior to its deemed collection as a foreign dataset. The Director of CSIS explained that an internal compliance review will determine the circumstances surrounding the incident and ensure its effective remediation. The results of this review will be shared with the appropriate oversight and review bodies in due course. Also, the National Security and Intelligence Review Agency was advised of the incident.

In the decision, the IC noted his appreciation of being informed by the Director of CSIS of the non-compliance incident. The IC explained that he raised the issue in the decision as it concerned information found in the Director's conclusions, which he is statutorily mandated to review as to their reasonableness. However, after review, it was determined that the incident had no bearing on the IC's quasi-judicial review mandate.

In addition, the IC made a remark regarding the supplemental appendices that were added to the initial request made by CSIS. As explained by the IC, if the appendices substantially modified the initial request, it would have been possible for him to find that CSIS' request was made after the dataset had been held for more than 90 days, which is the prescribed timeline to authorize the retention of the foreign dataset. The IC agreed with the Director, however, that the documents did not substantially modify the initial request. Lastly, the IC also made a remark regarding signed and dated documents. A perusal of the record revealed that efforts were made to address the IC's concerns expressed in earlier decisions. However, the IC expects that documents not included initially in future requests for authorization will also be signed and dated.

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.

IV. JUDICIAL AUTHORIZATION TO RETAIN A CANADIAN DATASET

In October 2021, the former IC approved the first authorization to query a Canadian dataset in exigent circumstances under the dataset regime established in 2019. For CSIS to retain this Canadian dataset longer than 90 days, it must obtain, with the Minister of Public Safety's approval, judicial authorization from the Federal Court of Canada.

In November 2021, CSIS submitted its first application for judicial authorization to retain two Canadian datasets. These Canadian datasets were queried previously in exigent circumstances as approved by the IC.

In March 2022, Justice Richard Mosley of the Federal Court authorized CSIS to retain, with terms and conditions necessary and advisable in the public interest, both datasets for two years (2022 FC 645). The Court was satisfied that the datasets were likely to assist CSIS in the performance of its security, foreign intelligence, and threat reduction 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 2022, 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 2022 FIORC meeting, held in the United States and hosted by the Inspector General of the Intelligence Community. Both, the ICO's Senior Counsel and Legal Counsel attended the meeting. The exchanges amongst members were particularly productive, as this was first in-person meeting since 2019.

Looking forward ::

The ICO is committed to the principles of accountability and transparency, which are vital to ensuring trust and confidence in Government of Canada institutions that carry out national security or intelligence activities. To that end, the ICO will continue its efforts to make the IC's decisions available and accessible to the public on the ICO website as soon as feasible.

The *National Security Act, 2017*, which came into force in 2019 and established the ICO, requires that a comprehensive legislative review be undertaken by Parliament. The IC is looking forward to sharing his perspective and the expertise of the ICO acquired during the past four years on the IC's quasi-judicial function, which is an integral part of the Canada's national security accountability framework.

ANNEX A

BIOGRAPHY OF THE HONOURABLE SIMON NOËL, K.C.

The Honourable Simon Noël was appointed Intelligence Commissioner, October 1, 2022.

The Honourable Simon Noël was born in the City of Québec. He studied law at the University of Ottawa and was admitted to the Quebec Bar in 1975. He was a professor in administrative law at the University of Ottawa from 1977 to 1979. In September 2012, the university's Civil Law Faculty bestowed on Mr. Noël the highest distinction as an Alumnus of the Faculty.

He was a partner at the firm Noël & Associates from 1977 to 2002. As a lawyer, he acted in many fields, including civil litigation, corporate law and administrative law. Notably, Mr. Noël was counsel for the Royal Commission of Inquiry into certain activities of the Royal Canadian Mounted Police (1979–1981) and co-chief prosecutor for the Commission of Inquiry into the Deployment of Canadian Forces to Somalia (1995–1997). He also represented the interests of the Security Intelligence Review Committee for over 15 years.

Some legal achievements included being appointed Queen's Counsel in 1992; being appointed Commissioner to the Commission des services juridiques du Quebec in 1993; and being appointed Fellow of the American College of Trial Lawyers in 2000. He also co-authored the *Supreme Court News / La Cour suprême en bref* from 1989 to 1995.

For a number of years, he has also been a speaker on numerous occasions dealing with national security and the rule of law. He has also authored and co-authored a variety of articles over the years. He coordinated the work of the four authors and others for the book, *The Federal Court of Appeal and the Federal Court: 50 Years of History*.

In his early years (1979–1983), Mr. Noël was in charge of two public affairs programs broadcast on the TVA network. He also actively volunteered for community groups and charitable organizations.

Judicial appointments include Judge of the Federal Court of Canada, Trial Division, and *ex officio* member of the Court of Appeal (August 2002); Judge of the Court Martial Appeal Court of Canada (December 2002), following the coming into force of the *Courts Administration Service Act* in July 2003, he was appointed Judge of the Federal Court (November 2003); Interim Chief Justice (2011); and at the request of the Chief Justice, he acted as Associate Chief Justice (2013 to 2017). He was also Co-ordinator of the Designated Proceedings Section (2006 to 2017). The Designated Proceedings Section of the Federal Court is where all files that have a national security component are managed and heard. He became a supernumerary judge in September 2017, and retired August 31, 2022.

ANNEX B

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

The Honourable Jean-Pierre Plouffe was the first Intelligence Commissioner by virtue of the coming into force of the *National Security Act, 2017* from July 2019 to September 2022.

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 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.

ANNEX C

LIST OF LEGISLATION RELATED TO THE INTELLIGENCE COMMISSIONER'S MANDATE

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.