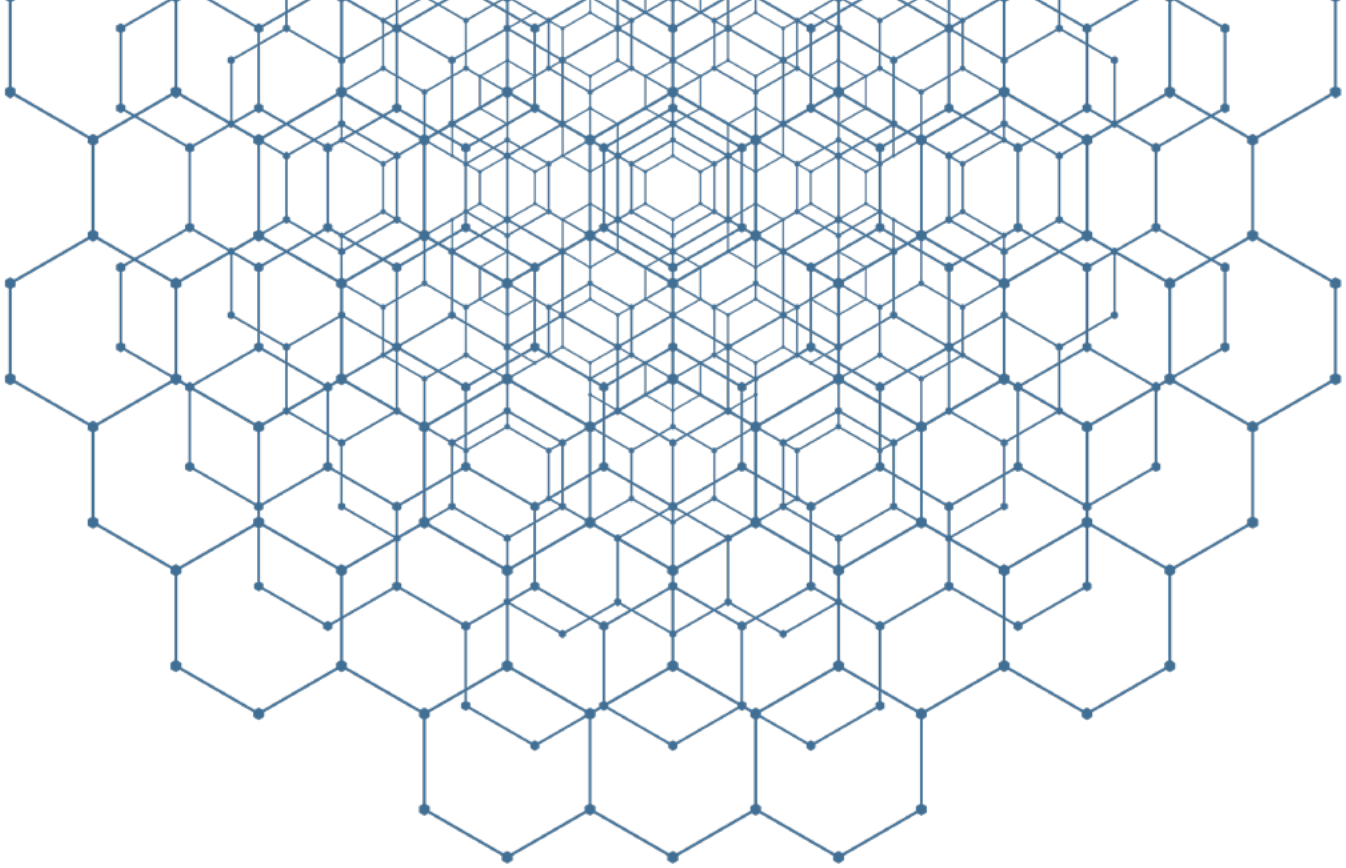


2024

Annual Report of the Intelligence Commissioner

Office of the Intelligence Commissioner
Bureau du commissaire au renseignement

Canada

P.O. Box 1474, Station B
Ottawa, Ontario K1P 5P6
613-992-3044
Info@ico-bcr.gc.ca
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, 2025

Prime Minister of Canada
Office of the Prime Minister
Ottawa, Ontario
K1A 0A2

Dear Prime Minister,

Pursuant to the provisions of subsection 22(1) of the *Intelligence Commissioner Act*, I am pleased to submit to you an annual report on my activities for the 2024 calendar year, for your submission to Parliament.

Sincerely,

The Honourable Simon Noël, K.C.
Intelligence Commissioner

Canada

Table of Contents

MESSAGE OF THE INTELLIGENCE COMMISSIONER

I am pleased to present my 2024 Annual Report. This report provides an overview of my activities as Intelligence Commissioner during the past year, as well as details of the oversight process I undertake when deciding whether to approve – or not approve – national security and intelligence activities authorized by the Minister of National Defence, the Minister of Public Safety, or the Director of the Canadian Security Intelligence Service (CSIS). The report also highlights the impact of my decisions in strengthening the governance of these activities in Canada.

Due to their classified nature, the activities of the Communications Security Establishment (CSE) and CSIS that require my approval cannot always be made public. As a result, representing the interests of Canadians through oversight of these activities is a fundamental aspect of my role as Intelligence Commissioner. Through my decisions, I seek to ensure that the extraordinary powers granted to our national security and intelligence agencies are exercised in a manner that is acceptable to Canadians.

In practice, this means that in deciding whether to approve a ministerial authorization issued by the decision maker, I consider important legal questions. These range from determining whether the proposed activities are authorized by law to ensuring the decision maker's authorization shows how the requirements set out in legislation have been met.

Beyond the legal considerations, since the agencies carry out the activities at the operational level, I must also assess practical issues. For example, I examine whether the proposed activities are described clearly enough to ensure the employees who will conduct them understand their limits – reducing the risk they may go beyond what is approved – and whether the agencies have safeguards in place to minimize potential impacts on Canadians.

My oversight continues to show the importance of information flow for effective decision making. For example, before approving the activities set out in a ministerial authorization, I must be certain that the decision maker has fully considered the potential implications for the rule of law and what impact the activities may have on the rights and privacy interests of Canadians. To enable this full consideration, it is essential that CSE and CSIS provide all relevant information to their respective decision makers. Since my appointment as Intelligence Commissioner in October 2022, I have insisted in my decisions that both agencies implement specific measures to improve the sharing of information with their decision makers. I am pleased to report noticeable and ongoing improvement in this area. There is no question that the better informed decision makers are, the more thoroughly they will be able to assess the impacts of their decisions – and the more confident Canadians can be in those decisions.

While my decisions and reasons are my primary means of communicating with the Canadian public, in the past year I was invited to appear before parliamentary committees to comment on planned amendments to existing security-related legislation as well as proposals for new legislation. My message to parliamentarians in these appearances was clear: Canadians must feel confident that our national security and intelligence agencies have the appropriate tools to conduct activities effectively and within the bounds of the law. Rigorous oversight, like that provided by the Intelligence Commissioner, is essential to providing this assurance.

In this regard – and notwithstanding their commitment to diligence in carrying out activities – CSE and CSIS sometimes make mistakes. Prompt reporting of potential compliance concerns allows me to ensure any negative effects are addressed quickly, and to assess potential impact on existing or future authorizations. In my 2024 decisions, I continued to emphasize the need for the agencies to be transparent about compliance incidents, to the fullest extent possible without compromising national security.

This need for transparency is particularly important as challenges to national security continue to evolve. In turn, the role of the Intelligence Commissioner also continues to evolve in response to new and emerging challenges. In 2024, for example, I determined that an authorization related to malicious cyber activities called for urgent action on my part. After reviewing the *Intelligence Commissioner Act*, I concluded that it allowed me to issue an immediate decision approving the authorization, with my written reasons to follow. This novel approach allowed CSE to provide cybersecurity support to the affected non-federal entities without delay. Also in 2024 – and for the first time since the role of the Intelligence Commissioner was created in 2019 – I attached a condition to a foreign dataset authorization, without which the Director's conclusions would not have been reasonable.

These developments reflect the ongoing need for adaptability in oversight. Effective national security and intelligence activities require meaningful scrutiny. The evolution of my role within the existing legislative framework is necessary to fulfill the important function played by the Intelligence Commissioner in the governance of these activities.

In conclusion, I wish to express my sincere thanks to the staff of my office for their professionalism and dedication in supporting my mandate. Their support is essential to ensuring I can fully represent the interests of Canadians in carrying out this important and independent oversight of governmental decisions.

The Honourable Simon Noël, K.C.
Intelligence Commissioner

ROLE OF THE INTELLIGENCE COMMISSIONER

IC

- mandate is set out in the IC Act
- conducts independent oversight
- is appointed by order in council for a fixed term
- must be a retired judge of a superior court
- performs his duties and functions on a part-time basis
- submits annual report to Parliament through the Prime Minister

ICO

- supports the fulfillment of the IC's independent oversight mandate
- 2024–25 Operating Budget is $2,575,853

Mandate

The Intelligence Commissioner's (IC) mandate is to approve – or not approve – certain national security and intelligence activities planned by the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS).

In the interest of national security and intelligence collection, these agencies may sometimes engage in activities that could involve breaking the laws of Canada, or interfere with the privacy interests of Canadians. These activities must first be authorized in writing by the Minister responsible for the agency involved or, in some cases, by the Director of CSIS. The ministerial authorization must include the conclusions – effectively the reasons – supporting the activities that are being authorized.

The IC reviews the conclusions given for authorizing the activities to determine whether they meet the test of "reasonableness" as recognized by Canadian courts. If so, the IC approves the ministerial authorization, and the agency can proceed with the planned activities. All decisions are published on the Office of the Intelligence Commissioner (ICO) website.

The activities that require approval by the IC are set out in the *Intelligence Commissioner Act* (IC Act), the *Communications Security Establishment Act* (CSE Act), and the *Canadian Security Intelligence Service Act* (CSIS Act).

In the case of CSE, IC approval is required for ministerial authorizations related to:

i. Foreign Intelligence activities; and

ii. Cybersecurity activities.

CSIS requires IC approval for ministerial authorizations related to:

i. Classes of Canadian datases;

ii. Retention of a foreign dataset;

iii. Searching a Canadian or foreign dataset in exigent circumstances; and

iv. Classes of acts or omissions that would otherwise constitute offences.

These authorizations are described in the following pages with additional information available on the ICO website.

Oversight process

The IC conducts independent oversight of governmental decisions by confirming that the Minister or Director of CSIS appropriately balances national security and intelligence objectives with respect for the rule of law and privacy interests.

WHAT IS A MINISTERIAL AUTHORIZATION?

A ministerial authorization gives CSE or CSIS permission to carry out certain specified activities in support of their respective responsibilities of collecting foreign intelligence and protecting Canada's national security. For CSE, a ministerial authorization is issued by the Minister of National Defence. For CSIS, a ministerial authorization is issued by the Minister of Public Safety or, in some cases, the Director of CSIS.

The power to issue a ministerial authorization is an important responsibility because it allows CSE and CSIS to undertake activities that contravene the laws of Canada, or potentially infringe on the privacy interests of Canadians and persons in Canada. Before CSE or CSIS can carry out the activities specified in a ministerial authorization, it must be approved by the IC.

ON WHAT STANDARD DOES THE IC REVIEW A MINISTERIAL AUTHORIZATION?

As the decision maker, the Minister or Director provides conclusions – essentially reasons – supporting the activities set out in a ministerial authorization and explaining how the legislative requirements have been satisfied. The IC reviews these conclusions to determine whether they are reasonable.

The IC applies the "reasonableness" standard of review as it is applied by Canadian courts: a reasonable decision is one that is justified, transparent and intelligible.

When analyzing a ministerial authorization, the IC considers the roles and responsibilities of the decision maker, the role of IC, as well as the overall objectives of the IC Act, the CSE Act, and the CSIS Act. The IC focusses on the reasons on which the decision maker has based their authorization, rather than on the IC's own interpretation of the law and the facts.

The IC's oversight ensures that the Minister or Director of CSIS remains accountable for the national security and intelligence activities set out in the ministerial authorizations.

WHAT INFORMATION IS SHARED WITH THE IC?

The decision maker must provide the IC with all information that was before them when issuing the authorization, except for Cabinet confidences.

Outside the context of an authorization under review, the IC may receive information that is not directly related to a specific review. Its purpose is to assist the IC in the exercise of his duties. Occasionally, the IC receives briefings from CSE and CSIS on classified contextual and technical information that could help his broader understanding of the national security and intelligence environment. The burden is on the agencies to determine what information is useful or necessary for the IC to fulfill his role.

OVERSIGHT PROCESS MAP

CSE or CSIS prepares an application and provides it to the decision maker (Minister or Director).

If satisfied that the legislative requirements are met, the decision maker issues a ministerial authorization which must include their conclusions supporting their decision.

The IC receives the ministerial authorization and all the information that was before the decision maker.

The IC decides if the conclusions of the decision maker are reasonable and provides a written decision within 30 days or within another agreed timeframe.

If approved by the IC, the authorization is valid and the activities can be conducted.

ACTIVITIES OF THE INTELLIGENCE COMMISSIONER

2024 Results
at a glance

Authorizations

13 Received

11 Approved

1 Approved with conditions

1 Partially approved

100% of decisions rendered in accordance with legislated timeframe

31 Remarks made by the IC

Authorizations reviewed and IC decisions – 2024

Minister of National Defence/ CSE activities	Received	Approved	Not approved	Partially approved*	IC remarks
Foreign Intelligence	3	2	-	1	8
Cybersecurity – Federal Infrastructures	1	1	-	-	4
Cybersecurity – Non-Federal Infrastructures	3	3	-	-	5
Total	**7**	**6**	**0**	**1**	**17**

*Partially approved: The IC determines that the decision maker's conclusions support only some of the activities set out in the authorization, and only those activities are approved.

Minister of Public Safety/ CSIS activities	Received	Approved	Not approved	Approved with conditions+	IC remarks
Classes of Canadian datasets	1	1	-	-	3
Retention of foreign datasets	4	3	-	1	8
Classes of acts or omissions	1	1	-	-	3
Total	**6**	**5**	**0**	**1**	**14**

+Approved with conditions: The IC approves an authorization to retain a foreign dataset with conditions if the Director's conclusions are reasonable once the conditions are attached.

IC remarks: Comments or observations made by the IC raising legal or factual issues of concern, but that do not impact the reasonableness of the conclusions. Remarks are made to improve the content of future authorizations or highlight an issue for CSE or CSIS' consideration.

Authorizations related to CSE activities

Where CSE's foreign intelligence or cybersecurity activities may contravene an Act of Parliament or lead to the acquisition of information that risks interfering with the reasonable expectation of privacy of Canadians or persons in Canada, an authorization from the Minister of National Defence is required.

FOREIGN INTELLIGENCE AUTHORIZATION

(Section 13, IC Act)

What does it authorize?

A foreign intelligence authorization is required before CSE can proceed with gathering intelligence through activities that may violate the laws of Canada, or inadvertently infringe on the privacy of Canadians or persons in Canada.

Why is it required?

As part of its mandate, CSE collects foreign intelligence in accordance with the Government of Canada's intelligence priorities. When carrying out its activities, CSE may acquire, covertly or otherwise, information from or through what is known as the "global information infrastructure" (GII) – basically the Internet, computer and telecommunications networks, and associated devices. Information collected from the GII that has foreign intelligence value is used and analyzed by CSE and shared within the Government of Canada according to its intelligence priorities.

Why is the IC's role important?

The IC ensures that the foreign intelligence activities described in the authorization, that would otherwise fall outside the limits of Canadian law, are conducted in way that is reasonable, proportionate and include measures that limit the impact on the privacy of Canadians.

CYBERSECURITY AUTHORIZATION

(Section 14, IC Act)

What does it authorize?

A cybersecurity authorization allows CSE to conduct unlawful activities and to acquire information that may breach the reasonable expectation of privacy of Canadians or persons in Canada when accessing the information technology (IT) systems of the Government of Canada and non-federal entities designated as being of importance to the Government – such as IT systems in the health, energy and telecommunications sectors.

Why is it required?

CSE provides advice, guidance and services to help protect IT systems from hackers and other cyber threats. To understand the vulnerabilities of these IT systems, CSE must access and collect information from them.

Why is the IC's role important?

The IC ensures that CSE cybersecurity activities specified in the authorization do not have a disproportionate effect on the rights and privacy interests of Canadians and persons in Canada, or on the rule of law. The IC's review also ensures that CSE has appropriate and adequate measures in place to limit any impact on the privacy of Canadians.

AMENDED AUTHORIZATION

(Section 15, IC Act)

During an ongoing operation, CSE might discover that it needs to undertake a particular activity not included in an approved ministerial authorization. Review by the IC ensures that CSE has sufficient justification for carrying out the new activity. Since the coming into force of the CSE Act in 2019, the Minister of National Defence has not issued any amended authorizations.

CSE and information related to Canadians

When conducting any of its foreign intelligence or cybersecurity activities, CSE must respect requirements set out in the CSE Act: the activities must not target Canadians or any person in Canada or infringe the *Canadian Charter of Rights and Freedoms* (Charter).

However, when conducting activities pursuant to an authorization, CSE may incidentally acquire information related to Canadians or persons in Canada. Incidentally means that the information acquired was not itself deliberately sought.

CSE can only retain incidentally acquired information relating to Canadians or persons in Canada when it is "essential" to do so. The IC's decisions have found reasonable the following definition of "essential":

- for foreign intelligence authorizations: the information is required to understand the foreign intelligence, or if without it, it would not be possible to provide foreign intelligence that supports the Government of Canada's intelligence priorities.
- for cybersecurity authorizations: without the information, CSE would be unable to identify, isolate, prevent, or mitigate harm to the system.

IC enables rapid response to cyber incident

The IC Act sets out the duties and responsibilities of the IC in considerable detail. However, there are certain aspects of the IC's responsibilities that are not explicitly set out. In **Decision CSE-2024-05**, the IC interpreted the IC Act to facilitate a rapid response to a cyber incident.

The Minister of National Defence issued a cybersecurity authorization related to non-federal entities designated as important to the Government of Canada. Facing malicious activity on their IT systems, these entities had requested CSE's help to protect their systems and information.

Given the context of the malicious activity and the critical role played by the systems that belonged to the non-federal entities, the IC recognized it was in the best interest of all parties – including the non-federal entities, CSE, and Canadians – to issue a decision as quickly as possible.

Under usual circumstances, the IC Act requires the IC to issue a written decision, including the reasons for the decision, within 30 days of receiving the authorization for review. In reviewing the legislation, the IC noted the Act did not specify that he was required to issue his decision and his reasons at the same time.

The IC stated that "*the preparation of my reasons should not delay the implementation of the cybersecurity solutions.*" As a result, he approved the authorization the day after receiving the request, allowing CSE to immediately start helping the non-federal entities secure their systems. The IC's reasons followed within the legislated time frame.

Renewing cybersecurity authorizations: ministerial conclusions must reflect current situation

Authorizing CSE to provide cybersecurity assistance to non-federal entities can be essential to safeguarding their critical IT infrastructure. However, these authorizations also represent an intrusion on Canadians' privacy by enabling CSE, a federal agency, to access information held by other levels of government or the private sector – information that would otherwise be beyond its legal reach. Further, the longer these authorizations are in effect, the greater their potential impact on privacy.

The CSE Act does not specify how long CSE cybersecurity assistance to a non-federal entity can continue, requiring only an annual renewal of the authorization and approval by the IC. In 2024, the IC approved three cybersecurity authorizations for non-federal entities, two of which involved renewing the approval of activities authorized in previous years. When seeking approval for a renewal, the IC emphasized that, to assure transparency and accountability, ministerial conclusions must fully justify and provide a factual basis for the extension being requested.

The Minister's conclusions to renew the first authorization cited ongoing cyber threats and the need for the entity to finish implementing CSE recommendations for strengthening its capacity to protect its systems **(Decision CSE-2024-06)**.

The second authorization related to the renewal of cybersecurity authorizations for Canada's three northern territories **(Decision CSE-2024-07)**. Unlike the reactive nature of the authorization considered in **Decision CSE-2024-06** – responding to a specific, ongoing cyber threat – the Minister's conclusions in this case characterized the renewal as having a preventative purpose. The justification centred on the need to act proactively in a region of strategic importance to Canada's national security.

In approving both renewals, the IC noted the Minister's conclusions may have to evolve to meet the reasonableness standard required for approval. As the IC pointed out, the facts relating to a cyber compromise and its response can change over time. Consequently, when a cybersecurity authorization is renewed, the Minister's conclusions should also change to reflect the different circumstances. This ensures the necessary factual basis required by legislation to allow the CSE to continue its cybersecurity assistance.

> *In contexts where cybersecurity activities are carried out for preventative or proactive purposes, I am of the view that the Minister nevertheless needs to establish a factual basis for CSE's assistance.*
>
> Decision CSE-2024-07

Authorizations related to CSIS activities

THE DATASET REGIME

What is the purpose of the dataset regime?

The dataset regime enables CSIS to collect information that it otherwise could not collect. It provides CSIS with the authority to collect, retain, and use Canadian and foreign datasets that are not directly and immediately related to a threat to the security of Canada, but that may nonetheless be relevant to its duties. Analysing personal information found in datasets enables CSIS to make connections or identify patterns and trends that would not be apparent using traditional investigative techniques.

A **dataset** is a collection of information that is characterized by a common subject matter, stored as an electronic record, contains personal information, and is relevant to the performance of CSIS' duties under sections 12 to 16 of the CSIS Act but cannot be collected or retained under those sections.

Under the dataset regime, CSIS activities related to datasets require a ministerial authorization, and subsequent review by the IC, in three instances:

- the Minister's determination of classes of Canadian datasets;
- the Minister's authorization, or that of a person designated by the Minister, to retain a foreign dataset (the Director of CSIS has been designated for this purpose); and
- the Director of CSIS' authorization to search a dataset in exigent circumstances.

CLASSES OF CANADIAN DATASETS

(Section 16, IC Act)

A **Canadian dataset** predominantly relates to Canadians or persons in Canada, or Canadian companies.

What does it authorize?

A class of Canadian datasets is a category or type of Canadian dataset described and defined in a ministerial authorization. The Minister's determination of classes of Canadian datasets is the initial step that allows CSIS to collect Canadian datasets. CSIS has 180 days to evaluate the dataset and determine if it falls within a class approved by the IC. Retention of Canadian datasets must subsequently be approved by the Federal Court.

Why is it required?

The authorization and oversight by the IC ensure that any collection by CSIS of Canadian-related information that is not related to a threat is reasonable. To collect a Canadian dataset, CSIS must reasonably believe that it falls within a class authorized by the Minister and approved by the IC.

Why is the IC's role important?

The IC ensures that CSIS collects the non-threat-related information in a balanced manner, and that the Minister has given proper consideration to privacy interests of Canadians and persons in Canada. Review by the IC also supports compliance and governance of CSIS activities by ensuring that the classes of datasets are clearly defined and can easily be understood by the CSIS employees responsible for collecting the information.

RETENTION OF FOREIGN DATASETS

(Section 17, IC Act)

A **foreign dataset** predominantly relates to non-Canadians who are outside of Canada or to non-Canadian companies.

What does it authorize?

The ministerial authorization authorizes the retention of the foreign dataset, which enables CSIS to use personal information about non-Canadians who are not in Canada, even if that information is not immediately and directly related to activities that represent a threat to the security of Canada.

Why is it required?

To retain a foreign dataset, the authorization requires CSIS to take the necessary measures to ensure that the dataset predominantly relates to non-Canadians who are outside of Canada or to non-Canadian companies.

Why is the IC's role important?

The IC's oversight confirms that the foreign datasets are relevant to CSIS' duties and do not contain information about Canadians or persons in Canada. The IC also ensures that CSIS has taken appropriate measures to delete any Canadian-related information and is not retaining information that relates to physical or mental health that a person would reasonably expect to remain private.

SEARCH OF A DATASET IN EXIGENT CIRCUMSTANCES

(Section 18, IC Act)

What does it authorize?

The authorization allows CSIS to conduct a search of a dataset where there is an urgent need for information in two instances: to preserve the life or safety of an individual, and to acquire intelligence of significant importance to the security of Canada the value of which would otherwise be diminished or lost.

Why is it required?

Urgent situations may arise in which obtaining an approval to retain a dataset would require too much time and pose a risk.

Why is the IC's role important?

The IC ensures that the Director's rationale for determining that an exigent circumstance exists is sufficiently supported by the factual context. To subsequently retain the dataset, CSIS must obtain the respective approval from the Federal Court or the IC.

While reviewing the Minister's conclusions, I am to carefully examine whether the important privacy and other interests of Canadians and persons in Canada were appropriately considered and weighed as well as to ensure that the rule of law is fully respected.

Decision CSIS-2024-05

Changes to Dataset Regime in 2024

In the years following the introduction of the dataset regime in 2019, CSIS expressed concerns that the regime was limiting its ability to retain and use datasets to investigate national security threats. In May 2024, after a period of public consultation, the government introduced a series of amendments to the CSIS Act – including to the dataset regime – in Bill C-70, *An Act respecting countering foreign interference*.

Appearing before parliamentary committees reviewing the Bill, based on his experience, the IC said that the proposed amendments would enhance CSIS' ability to use both Canadian and foreign datasets effectively, without limiting the role of the IC in providing independent oversight.

In **Decision CSIS-2024-04** – the first since the amendments in Bill C-70 came into effect in June 2024 – the IC noted that while the materials provided for review did not mention the legislative changes, he conducted the review using the updated CSIS Act. In his decision, the IC emphasized that any amendments or legal developments relevant to an authorization, including changes to CSIS policies or practices, should always be noted in the materials considered by the decision maker and provided for the IC's review – if only to confirm they had no impact.

In this decision, as well as in **Decisions CSIS-2024-05** and **CSIS-2024-06**, which both involved foreign datasets, the IC found that the legislative amendments did not affect the reasonableness of the Director's conclusions. Specifically, the IC pointed to subsection 11.1(1) of the CSIS Act, under which CSIS has two ongoing obligations related to foreign datasets.

Continuing obligations of CSIS

1. Deleting information with a reasonable expectation of privacy that relates to the physical or mental health of a person; and

2. Removing information that pertains to a Canadian or a person in Canada.

Before the 2024 amendments, the Act stated that CSIS "shall" delete or remove such information. The Act now says that CSIS "shall take reasonable measures to ensure" the information is deleted or removed.

While the text of the Act no longer demands certainty that this information be deleted or removed, the IC noted that this legislative change is not likely to have an impact in practice. In previous authorizations, the Director relied on measures taken by CSIS to ensure it was meeting its obligations under subsection 11.1(1). The IC's jurisprudence has also established that it is reasonable to rely on such measures since, in imposing a "continuing obligation" on CSIS, the Act recognizes that achieving a perfect result at the outset is not always possible.

CLASSES OF ACTS OR OMISSIONS – JUSTIFICATION FRAMEWORK

(Section 19, IC Act)

What does it authorize?

The ministerial authorization allows CSIS employees that are designated by the Minister, or persons acting under their direction, to carry out activities that would otherwise be against the law in Canada. The authorization specifies the types or "classes" of acts or omissions that are allowed. This is referred to as the "justification framework". The justification framework may also allow for information collected through otherwise unlawful conduct to be considered to have been collected lawfully.

Why is it required?

The CSIS Act recognizes that collecting information and intelligence on potential threats to the security of Canada may occur in settings and situations outside of the boundaries of the law. As an example, the subjects of a CSIS investigation may be engaged in unlawful conduct. If so, CSIS employees working undercover or persons acting under their direction may also be required to participate in the unlawful conduct in order to gain trust, maintain credibility, and develop access. However, the CSIS Act contains important limits on categories of conduct that can never be justified, and further provides that activities under the justification framework cannot infringe rights guaranteed by the Charter.

Why is the IC's role important?

The IC ensures that the acts or omissions that would otherwise be unlawful are restricted to activities related to CSIS duties. The IC also ensures that the classes are well-defined and will be clearly understood by CSIS employees.

Limitations – Section 20.1(18), CSIS Act

Categories of conduct that can never be justified:

(a) causing, intentionally or by criminal negligence, death or bodily harm to an individual

(b) willfully attempting in any manner to obstruct, pervert or defeat the course of justice

(c) violating the sexual integrity of an individual

(d) subjecting an individual to torture or cruel, inhuman or degrading treatment or punishment, within the meaning of the Convention Against Torture

(e) detaining an individual

(f) causing the loss of, or any serious damage to, any property if doing so would endanger the safety of an individual

The justification framework: responsibilities of designated CSIS employees

Once the IC approves classes of acts under the justification framework, designated CSIS employees must determine whether proposed unlawful acts fall within the approved classes. They are also responsible for ensuring that they carry out the acts – or direct them to be carried out – in a way that respects the rule of law. Any failure to understand or exercise this responsibility increases the risk that CSIS employees or persons directed by them could commit unlawful acts that are not legally justified.

It is essential that the Minister and the IC be confident that designated CSIS employees will apply the justification framework within legal boundaries. This is an especially crucial consideration where rights protected by the Charter may be involved. Indeed, the justification framework does not justify committing an act that would infringe a right or freedom guaranteed by the Charter. As indicated by the IC in **Decision CSIS-2024-01**, determining whether a proposed act could violate the Charter is not always a simple exercise. The analysis must be based on the context and facts of the act.

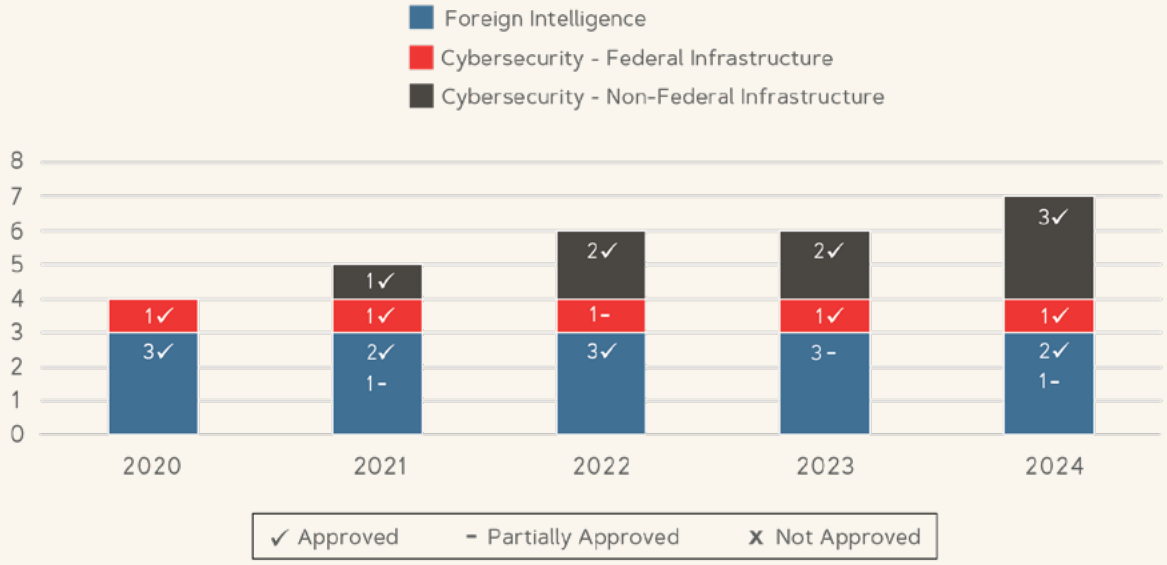
In approving the authorization, the IC emphasized the need for CSIS employees to have a full understanding of the legal principles related to their work. Employees must be able to confirm, for example, that a proposed activity would not interfere with a reasonable expectation of privacy, and is reasonable and proportionate in the circumstances. To support this, the IC stressed the importance of providing CSIS employees with clear guidance – including through training, internal policies, and reporting mechanisms – to ensure acts carried out under the justification framework respect the rule of law.

The IC also noted that – although not explicitly required under the CSIS Act – the Minister may consider how CSIS employees plan to meet the requirements of the framework in practice before authorizing specific classes of acts and omissions.

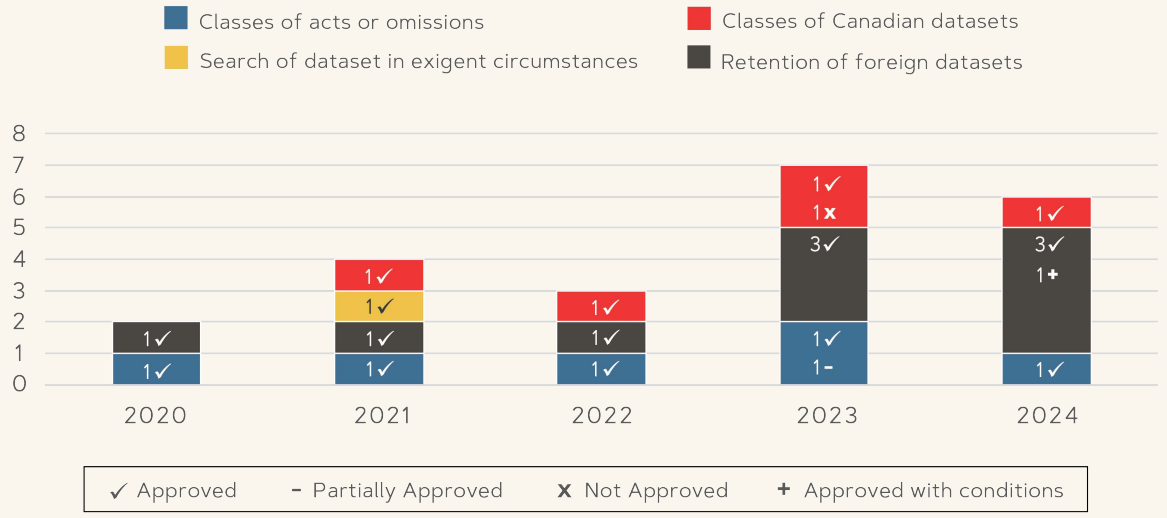
> *The Minister may not want to authorize classes if he is not confident that, once the classes are approved by the Intelligence Commissioner, the Justification Framework would be applied in a way that respects the rule of law…Similarly, this consideration, or the absence of it, in ministerial conclusions could factor into the Intelligence Commissioner's review.*
>
> Decision CSIS-2024-01

Activities – 5 year Overview

Authorizations reviewed by the IC CSE Activities



Authorizations reviewed by the IC CSIS activities



Strengthening ministerial accountability through information sharing

The IC plays a key role in the governance of certain national security and intelligence activities by ensuring that Ministers and the Director of CSIS – the decision makers – have access to all the information needed to make informed decisions.

For the Government of Canada to address national security threats effectively, relevant information cannot be held in silos. Critical details must reach those with the authority and responsibility to respond. Ministerial authorizations, which allow CSE and CSIS to conduct activities that would otherwise be unlawful, depend on this flow of information. This information must be complete and accurate if Ministers and the Director are to be accountable for their decisions.

Through his decisions, the IC enhances the flow of relevant information in two main ways:

1. Oversight of information provided to decision makers

- The IC reviews whether decision makers have been given enough information to fully understand proposed activities and their implications.
- Since the IC reviews the same record as the decision makers, he is well-positioned to assess whether the information was sufficient.
- If the IC finds gaps or insufficiencies in the information, he can refuse to approve the activities.

Decision CSE-2024-01, concerning a foreign intelligence authorization, is an example where insufficient information affected the reasonableness of the Minister's conclusions. In this review, the IC identified uncertainty around how Canadian-related information collected incidentally would be handled. Specifically, it was unclear whether CSE intended to retain all this information. If so, there was no indication how the retention of the Canadian-identifying information satisfied the legal test that it be "essential".

The IC found that the Minister's conclusions did not reflect a full understanding of the activities due to incomplete information from CSE. As a result, the IC found the Minister's conclusions unreasonable with respect to that activity. In his decision, the IC emphasized the importance of sharing all relevant information to ensure accountability.

2. Encouraging greater detail in agency reporting

The IC has frequently suggested that CSE and CSIS provide more detailed information about:

- the types of information collected during authorized activities; and
- how Canadian-related information collected incidentally is handled, including the rationale for retaining any such information.

In certain decisions issued in 2024, the IC observed that the authorizations were effectively requests for renewals: the authorizations included the same activities that the decision maker had authorized – and the IC had approved – in the previous year. The IC emphasized that the record from one year to the next must reflect what is new and distinct. He also emphasized that decision makers need up-to-date information about recent operational activities and their outcomes to make informed decisions. Indeed, the decision makers must be provided with the best available information when determining whether to authorize activities that would otherwise be unlawful.

In his remarks, the IC focused on the information related to the outcomes of activities undertaken in the previous year. This information is an

important tool describing the way in which approved activities have been previously conducted by the agencies – and therefore offers insight into future expected outcomes.

The IC identified categories of information that could be included in reports on outcomes to support the decision maker's conclusions. In particular, the IC specifically requested more detailed reporting on:

- the outcomes of past collection activities, including the types and volume of Canadian-related information collected and retained; and
- how this information was used, and the justification for retaining it.

Getting results

The IC's efforts have led to tangible improvements. The applications provided by CSE and CSIS to their respective Ministers and to the Director now include more detailed accounts of the outcomes of approved activities conducted under previous authorizations. The additional detail on outcomes provides the Ministers and the Director with a greater understanding of the activities carried out by the agencies.

Decision CSE-2024-06, relating to a cybersecurity authorization, is one example. In releasing this decision, the IC noted that,

"This is the first authorization in which there is a precise accounting of retained information. I appreciate and commend CSE for giving effect to past remarks by providing the Minister and myself with additional information on the real-world impacts of the authorizations. I consider this progress for purposes of ministerial accountability as well as for purposes of transparency."

In promoting transparency in the national security and intelligence environment, the IC will look to continue making suggestions to improve the sharing of relevant information with decision makers.

As Intelligence Commissioner, I make my decisions on behalf of Canadians and persons in Canada. A complete record before the Director and myself is necessary for those rights and interests to be appropriately considered.

In that sense, although the Intelligence Commissioner's role in representing interests of the Canadian public may not engage principles of natural justice with respect to a particular applicant, I am of the view that it engages broader principles of procedural fairness with respect to Canadians and persons in Canada. Indeed, if information that has a bearing on the rights of Canadians is not presented to, or considered by, the Director, their interests are not being fully considered.

Decision CSIS-2024-05

What if CSIS or CSE fail to comply with a ministerial authorization?

In most cases, ministerial authorizations allowing CSIS or CSE to conduct specific classes of activities expire after one year. When presented with a renewal and deciding whether to approve the authorization, knowing how agencies conducted activities in the previous year or years is an important consideration. The Minister and the IC must have confidence that agencies will act in accordance with internal policies, legislation, and the Charter. Past practice is helpful in making that determination.

To ensure he has this information, the IC asks to be informed promptly of any failure to comply with the terms of an approved ministerial authorization. This could include retaining information longer than permitted under an authorization, for example, or failing to suppress Canadian-related information in reporting. In addition to prompt reporting of any compliance incidents – including steps taken to prevent a recurrence – the IC also expects decision makers to identify any potential compliance issues when seeking IC approval for a new or renewed authorization.

While some compliance incidents are isolated and quickly remedied with no impact on the reasonableness of the decision maker's conclusions, others may be relevant to the IC's decision. They can even have a direct impact on whether the IC approves the authorization.

In **Decision CSIS-2024-06**, the IC reviewed an authorization to retain a foreign dataset. The information provided to the IC indicated that the dataset had been "checked" outside of the parameters of the evaluation process set out in the CSIS Act. The Act sets out that prior to obtaining the IC's approval, a foreign dataset can only be searched by CSIS employees in the context of the evaluation process, during which the employees confirm the dataset's contents and usefulness. The IC approved the authorization, but noted that he did not have enough information to determine whether the "checking" of the dataset constituted an unauthorized search. The IC pointed out that the Director of CSIS had not identified this issue as a potential compliance concern in the conclusions supporting the authorization. He requested that CSIS provide him and the Director with additional information to clarify the matter.

In **Decision CSIS-2024-05**, a compliance incident had a direct influence on the IC's decision regarding the retention period for a foreign dataset.

In the context of previous foreign dataset authorizations, CSIS had informed the IC that it had discovered working documents in its holdings relating to foreign datasets. These working documents – some of which contained information related to Canadians or persons in Canada – had been used to evaluate the foreign datasets. Contrary to CSIS' legislative obligation, the working documents had not been deleted at the end of the evaluation period. Upon discovery of their existence, CSIS deleted them and indicated to the IC that CSIS would include information about the incident when relevant to any authorization sought in the future. Indeed, the IC had received a memorandum about the incident as part of the record in the context of a different foreign dataset that had been approved.

Although the record provided did not include any information about the earlier incident, after a thorough analysis of its content, the IC concluded that the foreign dataset CSIS was seeking to retain was in fact related to the now-deleted working documents. Absent information about the past incident, the IC found that the record was incomplete.

The IC could not confirm whether the absence of information about the earlier compliance incident could have had an impact on the Director's decision. As a result, the IC approved the authorization with a condition: the dataset could be retained only for one year instead of the five years requested.

The IC can only include conditions to an approval of an authorization when the authorization relates to a foreign dataset (paragraph 20(2)(b), IC Act). This marked the first time the IC imposed a condition in an approval, highlighting for CSIS the expectation that all relevant information should be included in future applications. As the IC stated, "*Canadians expect CSIS to have adequate tools to carry out its activities, but also that information relevant to their interests will be considered when CSIS seeks authorization to conduct activities.*"

In any compliance incident, a primary concern for the IC is seeing that action to mitigate its effects is taken as quickly as possible. In 2024, CSE informed the IC that it had shared information collected under ministerial authorizations with international partners without removing Canadian identifying information. In addition to requesting periodic updates from CSE on how it was addressing the incident, the IC also advised CSE that, where relevant, information relating to the incident should be reflected in future applications for approval of ministerial authorizations. The IC also encouraged CSE to be publicly transparent about the incident when possible.

CSE has provided the IC with the requested updates on its efforts to mitigate the effects of this incident, continues to assess its impact, and has indicated it will share the results of its investigation with the IC.

Transparency

As a retired judge, the IC is deeply committed to fostering transparency.

In addition to the annual report, the primary means the IC communicates with the Canadian public is through his written decisions. The ICO continues to publish all decisions on its website with as few redactions as possible to promote transparency and ministerial accountability. The ICO website was also updated in 2024 to include additional information about the IC's mandate and activities.

Additionally, IC Noël appeared this year before parliamentary committees studying Bill C-70, *An Act respecting countering foreign interference* as well as Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*. His remarks focused on the themes of ensuring that national security and intelligence agencies have the appropriate tools and legislation to be effective; the importance and impact of oversight in the national security environment; and the protection of privacy.

Collaboration

The IC receives a copy of reports prepared by National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians that relate to the IC's powers, duties or functions. In 2024, the IC received one report from NSIRA in relation to activities carried out by a federal department related to national security or intelligence.

The ICO continues to benefit from its membership in the Five Eyes Intelligence Oversight and Review Council by exchanging best practices and new developments, and participated in the 2024 annual meeting.

Biography of the Honourable Simon Noël, K.C.

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

Mr. 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 Concerning Certain Activities of the Royal Canadian Mounted Police* (1979–1981) and co-chief counsel 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 King's Counsel in 1992; Commissioner to the Commission des services juridiques du Quebec in 1993; and 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.

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*.

From 1979 to 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 of the Federal Court where files that have a national security component are managed and heard (2006 to 2017). He became a supernumerary judge in September 2017, and retired August 31, 2022.