2023

Annual Report of the Intelligence Commissioner

Office of the Intelligence Commissioner

Bureau du commissaire au renseignement

Canada

Office of the Intelligence Commissioner
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-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 28, 2024

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

Dear Prime Minister,

Pursuant to the provisions of subsection 22(1) of the *Intelligence Commissioner Act*, I am pleased to submit to you an annual report on my activities for the 2023 calendar year, for your submission to Parliament.

Sincerely,

The Honourable Simon Noël, K.C.
Intelligence Commissioner

Canada

TABLE OF CONTENTS

Intelligence Commissioner's Message ::

Welcome to the 2023 Annual Report of the Intelligence Commissioner — the second report since my appointment as Intelligence Commissioner in October 2022.

In introducing last year's Annual Report, I shared my commitment to transparency, at the same time recognizing certain constraints related to national security. With this report, I reaffirm my commitment to public transparency, with an added emphasis on providing details about the role and work of the Intelligence Commissioner.

It is primarily through my written decisions — summarized in this report — that I communicate with Canadians and contribute to the transparency and accountability of Canada's national security and intelligence agencies. I am therefore pleased to note that my decisions rendered in 2023 are available to the public on the Office of the Intelligence Commissioner (ICO) website. I have written these decisions to provide Canadians with as much information as possible about the privacy rights and interests at play when I consider whether to approve — or not approve — certain activities that the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS) wish to undertake.

Having completed my first full year in this role, during which I rendered 13 decisions — the most in any year since the ICO was established — I can confidently say that the work of the Intelligence Commissioner has a significant and tangible impact on Canada's national security and intelligence activities.

Indeed, my decisions hold accountable the ministers who authorize CSE and CSIS activities and have a direct influence on these activities. For example, in the past year I did not approve a ministerial authorization and only partially approved others because the scope of proposed activities was too broad. After considering the rationale for my decisions, the agencies involved submitted revised requests for authorization to undertake certain activities. New ministerial authorizations — setting out a more limited scope of activities and more detailed reasons to justify the activities — were provided for my review and ultimately, approval.

CSE and CSIS are mandated to ensure the protection of Canadians. This is implemented through the granting of broad powers that require, at times, intrusion into our private lives and non-compliance with Canadian laws. To ensure that this kind of intrusion and non-compliance remain the exception and is not undertaken without proper justification, the activities conducted by CSE and CSIS must be carefully reviewed and scrutinized. This is the role of the Intelligence Commissioner.

We live in a turbulent and complex world in which threats come in many forms, and where it can be difficult to identify the source of threats such as cyberattacks. To keep Canadians safe, it is essential that CSE and CSIS have the appropriate tools to protect us. Canadians' confidence that these agencies will use these tools in a reasonable manner rests on independent and effective oversight. This is what I strive to provide in our collective interest.

I would like to express sincere thanks to the staff at the ICO, who continue to support me with diligence and professionalism. Their considerable efforts make it possible for me to fulfill my mandate.

I invite you to read this report to better understand the role of the Intelligence Commissioner and my activities in 2023. I hope it contributes to your confidence that your rights and interests are being considered and protected when it comes to national security and intelligence activities.

The Honourable Simon Noël, K.C.
Intelligence Commissioner

OVERVIEW

Est.
2019

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

The IC reports annually to Parliament through the Prime Minister

IC Act

MANDATE

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

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 another country, or interfere with the privacy interests of Canadians. Any activities of this kind 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. The activities cannot take place without approval from the IC.

In conducting independent oversight of governmental decisions, the IC plays a central role in assuring effective governance of national security and intelligence activities in Canada – the IC holds the government accountable by ensuring that the Minister or Director appropriately balance national security and intelligence objectives with respect for the rule of law and privacy interests.

The IC's function is quasi-judicial in nature — reviewing and analysing ministerial authorizations, applying legal tests to the facts, and writing decisions that are binding on CSE and CSIS. 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
ii. Cybersecurity activities

CSIS requires IC approval for ministerial authorizations related to:

i. Classes of Canadian datasets
ii. Retention of a foreign dataset
iii. Querying a Canadian or foreign dataset in exigent circumstances
iv. Classes of acts or omissions that would otherwise constitute offences

These authorizations are described in the following pages.

Oversight Process ::

The IC conducts oversight of ministerial authorizations by applying the "reasonableness" standard of review.

WHAT IS A MINISTERIAL AUTHORIZATION?

A ministerial authorization is a written document which gives CSE or CSIS permission to carry out certain specified activities in support of their responsibilities in protecting Canada's national security and collecting foreign intelligence. 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, since it allows these agencies to undertake activities that contravene the laws of Canada or another country, or potentially infringe on the privacy interests of Canadians and persons in Canada. Before CSE or CSIS can carry out the activities included in a ministerial authorization, the authorization must be approved by the IC. Ministerial authorizations are valid for up to one year following IC approval, except for a ministerial authorization to retain a foreign dataset collected by CSIS, which is valid for up to five years.

While the content of ministerial authorizations is not publicly available, the CSE Act and the CSIS Act, as well as IC decisions published on the ICO website provide details on the information that is included:

- the facts that gave the Minister or the Director the information they needed to decide that the authorization met the legislative requirements for it to be issued
- the reasons explaining how the legislative requirements have been met
- detailed explanations of the activities to be carried out and how they fit into the permitted categories set out in legislation
- examples illustrating the full scope of the activities being authorized or the classes being determined
- any terms and conditions considered advisable in the public interest
- policy measures and procedures in place to protect Canadian privacy interests and ensure respect for the rule of law
- reporting requirements
- the proposed period for which the authorization would be valid

STANDARD OF REVIEW

When issuing an authorization, the Minister of National Defence, the Minister of Public Safety, or the Director of CSIS — the decision makers — must provide conclusions to explain and justify why they authorized the types of activities CSE or CSIS would like to conduct. The IC reviews those conclusions to determine whether they are reasonable.

While the term "reasonable" is not defined in the IC Act, the CSE Act or the CSIS Act, it is a familiar standard in administrative law that is applied by courts when reviewing decisions made by governments or decision makers acting on their behalf. The IC's decisions recognize that Parliament intended that the IC apply the reasonableness standard as it is applied in administrative law jurisprudence. In essence, a reasonable decision is one that is justified, transparent and intelligible.

In determining whether the decision maker's conclusions supporting a ministerial authorization are reasonable, the IC must determine whether they are justified given the facts at issue and the legal context. To do so, the IC takes into account the roles and responsibilities of the decision maker, their own role as IC, as well as the overall objectives of the IC Act, the CSE Act and the CSIS Act.

The IC focuses on the reasons on which the decision maker has based their conclusions, rather than on the IC's own interpretation of the law and the facts. That means the decision maker's reasons must not be assessed against a standard of perfection or include the outcome or details that the IC believes should have been included.

Applying the reasonableness standard in this way ensures that accountability for the national security and intelligence activities subject to IC review remains with the respective Minister or Director of CSIS. While the IC is responsible for determining whether the decision maker's justification supporting the conclusions is reasonable, the responsibility for allowing CSE or CSIS to conduct the activities in the first place belongs to the Minister or Director who issued the authorization.

Sharing information with the IC outside the context of an authorization under review

The IC Act (section 25) allows the IC to receive information from the Minister of Public Safety, the Minister of National Defence, CSIS and CSE outside the context of an authorization under review. The information cannot be directly related to a specific review. Its purpose is to assist the IC in the exercise of his or her duties.

To that end, the IC occasionally 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 IC does not request to be briefed on specific topics. Rather, 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, except Cabinet Confidences.

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.

The ministerial authorization is valid only if approved by the IC. CSE or CSIS may then carry out the activities.

AUTHORIZATIONS REVIEWED AND DECISIONS RENDERED IN 2023

2023 Results
at a glance

AUTHORIZATIONS:

13
RECEIVED

8
APPROVED
(61%)

4
PARTIALLY APPROVED
(31%)

1
NOT APPROVED
(8%)

100%
DECISIONS RENDERED
in accordance with legislated timeframe

37
REMARKS
made by the IC

2023 IC Decisions and Authorizations Reviewed ::

Minister of National Defence/ CSE activities	RECEIVED	APPROVED	PARTIALLY APPROVED	NOT APPROVED	IC REMARKS
Foreign Intelligence	3	-	3	-	8
Cybersecurity – Federal Infrastructures	1	1	-	-	5
Cybersecurity – Non-Federal Infrastructures	2	2	-	-	5
Total	**6**	**3**	**3**	**0**	**18**

Minister of Public Safety/ CSIS activities	RECEIVED	APPROVED	PARTIALLY APPROVED	NOT APPROVED	IC REMARKS
Classes of Canadian datasets	2	1	-	1	6
Retention of a foreign dataset	3	3	-	-	6
Classes of acts or omissions	2	1	1	-	7
Total	**7**	**5**	**1**	**1**	**19**

Summaries of the 2023 decisions follow the description of each ministerial authorization.

Partially Approved

For certain authorizations, the IC may determine that the decision maker's conclusions support some – but not all – of the activities set out in the authorization. The activities that are not supported by reasonable conclusions are not approved.

IC Remarks

Remarks are comments or observations made by the IC at the end of his decisions that reflect potential legal or factual issues of concern raised in the authorization, but that do not impact the reasonableness of the conclusions under review. Remarks are made to improve the content of future applications or to highlight an issue for consideration by CSE or CSIS.

Authorizations Related to CSE Activities ::

FOREIGN INTELLIGENCE AUTHORIZATION

(section 13 of IC Act)

What does it authorize?

A foreign intelligence authorization allows CSE to collect foreign intelligence in ways that would otherwise violate the laws of Canada and breach the reasonable expectation of privacy of Canadians or persons in Canada.

> **Foreign intelligence is defined in the CSE Act as** "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security."

Why is it required?

As part of its mandate related to foreign intelligence, CSE may acquire, covertly or otherwise, information from or through what is known as the "global information infrastructure" (GII). Basically, the GII includes the Internet, computer and telecommunications networks, links and associated devices. Information collected from the GII that has foreign intelligence value is used and analysed by CSE, and shared in accordance with Government of Canada intelligence priorities.

When undertaking any of its activities, CSE must abide by conditions set out in the CSE Act: the 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* (Charter).

However, the legislation recognizes that to effectively collect foreign intelligence, CSE may need to contravene Canadian law. The legislation recognizes as well that CSE may unintentionally collect information that would infringe on the reasonable expectation of privacy of a Canadian or a person in Canada. Therefore, before CSE can proceed with foreign intelligence collection that may violate the laws of Canada, or inadvertently infringe on privacy, it must obtain a foreign intelligence authorization.

Why is the IC's role important?

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

How does CSE obtain it?

The Chief of CSE submits an application to the Minister of National Defence that describes the reasons the authorization is needed and the foreign intelligence activities or classes of activities that CSE wants to conduct. It also identifies Acts of Parliament that may be contravened by CSE when conducting the activities under the authorization.

The Minister issues the authorization when they have reasonable grounds to believe that the authorization is necessary; the proposed activities are reasonable and proportionate considering the purpose and nature of the activities; and all other statutory conditions have been met.

Decisions rendered in 2023

In his three decisions relating to foreign intelligence authorizations, the IC emphasized that the conclusions on which a ministerial authorization is based must demonstrate an understanding of the proposed activities, as well as their effect on the rule of law and Canadian privacy interests.

In the first of three decisions, the IC gave partial approval to the activities authorized by the Minister, finding that most of the activities set out in the authorization were reasonable and proportionate. The Minister's conclusions reflected a proper balance between the need to acquire foreign intelligence and privacy protections. Further, the Acts of Parliament that could potentially be contravened were limited in number and in impact on the Canadian public. The Minister showed an awareness of the privacy interests at issue and laid out the measures in place to protect them.

However, the IC did not approve one of the classes of activities set out in the authorization as it fell outside the scope of the CSE Act. For the Minister's conclusions to be reasonable, the Minister must have the statutory authority to include them in the authorization. Subsection 26(2) of the CSE Act sets out the activities and classes of activities that CSE may carry out under a foreign intelligence authorization. The IC was of the view that this particular class of activities was too broad to fit into the permitted categories set out in the Act.

The IC drew particular attention to paragraph 26(2)(e) of the CSE Act, which states that an authorization may permit CSE to carry out "any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activity, authorized by the authorization." The IC noted that this provision is broadly worded and would appear to allow the Minister to include similarly broad activities in an authorization. However, the IC stated that CSE would have to provide the Minister with the amount of detail needed to develop a clear understanding of the types of activities that would fall under this provision. This level of detail and specificity is necessary to avoid classes of activities that are unreasonably broad.

This same concern was apparent in the second and third foreign intelligence decisions in which the IC also only partially approved the activities set out in the authorizations. In both decisions, the IC did not approve a class of activities that copied the broad wording found at paragraph 26(2)(e) of the CSE Act, noted above. Further, the description of this class of activities indicated that if CSE conducted activities that fell outside the scope of the other activities listed in the authorization — and therefore fell within this broadly defined class of activities — the Minister would be notified by CSE. The IC concluded that the Minister was effectively issuing a blanket authorization for activities that fall "outside the scope" of the other activities explicitly set out in the authorization — while simply asking to be notified after the fact should they be conducted.

The IC was of the view that being notified of an activity after the fact meant that the Minister would have been unaware of the nature of the activity before CSE carried it out. Further, if the activity is "outside the scope" of the authorized activities, approval from the IC — an integral part of the authorization process — would not have been obtained.

Simply replicating the wording of paragraph 26(2)(e) of the CSE Act as a "catch-all" clause in an authorization did not provide the Minister with enough information to understand the activities that would be "outside the scope" of other activities in the authorization. The Minister's conclusions did not provide insight into what these activities could be.

Notable remarks in the decisions

Reports containing Canadian Identifying Information

The CSE Act recognizes that, in the course of collecting information about foreign entities, CSE may inadvertently also collect information about Canadians.

To obtain a better understanding of the impact of CSE activities on Canadian privacy interests, the IC noted that it would help if CSE provided the Minister with more detail about the types of information related to Canadian privacy interests included in CSE reporting. Even general examples of the information being collected and CSE's reasons for retaining the information would help to increase the awareness of the real impact on privacy interests of Canadians.

Threshold for determining whether a target is not a Canadian or a person in Canada

The Minister's conclusions state that to carry out the activities being authorized, CSE must have reasonable grounds to believe that the target of the activities is not a Canadian, and that a foreign entity being targeted is located outside of Canada. These limits minimize the risk that information related to Canadians will be acquired incidentally. Nevertheless, the IC noted that, considering CSE is prohibited from directing its activities at Canadians or persons in Canada, it may be appropriate to have a higher legal threshold than "reasonable grounds to believe"— which may be somewhat less rigorous than the absolute ban on targeting Canadians or persons in Canada found in the CSE Act.

"[I]ssuing an authorization is a ministerial responsibility that cannot be delegated. It is a heavy responsibility because authorized activities could contravene Canadian laws and intrude on the privacy interests of Canadians. Parliament is asking the Minister no less than to personally confirm that CSE is justified in carrying out unlawful activities. [...] Parliament is also asking the Minister to confirm that activities that could amount to a search or seizure are compliant with the Charter."

—IC Decision, 2200-B-2023-06, paragraphs 57-58

CYBERSECURITY AUTHORIZATION

(section 14 of IC Act)

What does it authorize?

A cybersecurity authorization allows CSE to access the information technology (IT) infrastructures of federal entities, as well as non-federal entities that have been designated as being of importance to the Government of Canada. It also authorizes CSE to acquire information that is stored on or passing through this infrastructure in a way that may contravene Canadian laws and breach the reasonable expectation of privacy of Canadians or persons in Canada.

Why is it required?

CSE provides advice, guidance and services to help protect Government of Canada IT systems from hackers and other cyber threats. The CSE mandate includes providing these same services to non-federal entities that have been designated by the Minister of National Defence as being of importance to the Government of Canada — the health, energy and telecommunications sectors, for example.

To understand where and how these important IT systems may be vulnerable, CSE must access and collect information from their infrastructure. While the aim is to protect the IT systems from cyber threats, these activities might nevertheless be contrary to Canadian laws. CSE activities — especially acquiring information — may risk infringing on the reasonable expectation of privacy of a Canadian or of a person in Canada. The CSE Act requires CSE to obtain a cybersecurity authorization from the Minister of National Defence prior to conducting the potentially unlawful activities.

Why is the IC's role important?

The IC ensures that CSE cybersecurity activities do not have a disproportionate effect on the rights and privacy interests of Canadians and persons in Canada or respect for 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.

How does CSE obtain it?

The Chief of CSE submits an application to the Minister of National Defence. The application sets out, among other things, the reasons the cybersecurity authorization is needed, as well as the activities or classes of activities that CSE wants to carry out. It also identifies Acts of Parliament that may be contravened by CSE when conducting the activities under the authorization. When the authorization relates to accessing a non-federal IT infrastructure, the application must also include a written statement from the owner or operator of the infrastructure requesting CSE to carry out the activities included in the authorization.

The Minister issues the authorization when they have reasonable grounds to believe that the authorization is necessary; the proposed activities are reasonable and proportionate considering the purpose and nature of the activities; and all other statutory conditions have been met.

Decisions rendered in 2023

In his three decisions reviewing cybersecurity authorizations, the IC emphasized the importance for CSE to have appropriate measures in place to protect the privacy interests of Canadians, especially given that Canadian-related information could be collected in an incidental manner when conducting cybersecurity activities.

Federal infrastructures

The IC approved the cybersecurity authorization for activities aimed at helping to protect federal IT infrastructures. In reaching this decision, the IC analysed whether the activities authorized by the cybersecurity authorization could include actions to mitigate the risk to federal systems posed by cyber attacks. This issue required analysis because subsection 27(1) of the CSE Act, which sets out the types of activities that can be included in a cybersecurity authorization, does not explicitly mention mitigation actions. The IC found that the cybersecurity and information assurance aspect of CSE's mandate specifically includes providing "services to help protect" federal systems, and there could be no cybersecurity without mitigation actions.

The IC explained that in the context of CSE's cybersecurity mandate as set out in the CSE Act, it is justified to interpret the terms "access", "acquire" and "for the purpose of helping to protect" found in subsection 27(1) as giving CSE the authority to conduct mitigation actions. In addition, the IC indicated that, to the extent that mitigation actions may contravene an Act of Parliament or infringe privacy interests of Canadians or persons in Canada, they should be included in the authorization to ensure ministerial accountability and independent oversight by the IC. Indeed, ministerial authorizations, and reviews by the IC, are mechanisms to ensure that there is proper justification and accountability for any breach of a law or of privacy interests.

Non-federal infrastructures

The IC approved the activities in both decisions concerning cybersecurity authorizations in relation to non-federal IT infrastructures. The IC recognized that the Minister relies on the application from the Chief of CSE to make conclusions with respect to the state of the non-federal entity's systems as well as the effectiveness of the proposed cybersecurity activities. The IC confirmed this to be reasonable as he did not expect the Minister, nor is it the Minister's role, to have that level of technical expertise. Indeed, the CSE Act states specifically that the Chief's application "must set out the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it are met" (subsection 33(2), CSE Act). At the same time, to be seen as reasonable, a ministerial conclusion within the authorization framework must be justified and intelligible. This means that, even where the Minister adopts the Chief's conclusions as their own, the Minister must still show an understanding of the rationale for their conclusions. The IC was of the view that the Minister's conclusions exhibited that understanding. There was a clear rational connection between CSE's proposed cybersecurity activities and their objective, which was to help protect non-federal IT infrastructures.

In the first of these two authorizations, the IC determined that CSE policies and practices indicate the seriousness with which the agency approaches the retention, analysis and use of information relating to a Canadian or a person in Canada. They also supported the Minister's conclusions that this information will only be used, analysed or retained if it is judged essential to identify, isolate, prevent or mitigate harm to the non-federal entity's systems.

In the second decision, the IC indicated that conducting cybersecurity activities on non-federal systems necessarily involves acquiring information related to Canadians or persons in Canada — the systems are located in Canada and the information stored on the systems, by its nature, relates to Canadians and persons in Canada. Further, in this authorization, it was noted that the information on the systems was not limited to the information of the employees of the entity that owned the non-federal infrastructures, but could also include information from members of the Canadian public who, for example, communicate by email with the owner of the infrastructures.

The IC was satisfied that the facts in the record supported the Minister's conclusion that the activities carried out by CSE focused on acquiring information about cyber threats, not information about Canadians. The activities respected the legislative prohibition against targeting Canadians. Indeed, the Minister's conclusion aligned with subsection 23(3) of the CSE Act which states that — despite the prohibition on directing activities at Canadians or persons in Canada — CSE may carry out activities on systems in order to identify or isolate malicious software, prevent malicious software from harming the systems, and mitigate any harm. The Minister's conclusion was also in line with the cybersecurity and information assurance aspect of CSE's mandate that can only be fulfilled by accessing systems in Canada.

Notable remarks in the decisions

The retention criterion of "until the information is no longer useful for these purposes"

In his decision relating to federal infrastructures, the IC noted that CSE's objective is to assess information that is acquired through the authorized activities without significant delay, and to retain information deemed to be useful only as long as it continues to be useful. However, the IC noted that it was not clear from the record whether CSE had procedures in place to monitor and periodically review whether Canadian-related information that had been acquired incidentally and retained by CSE continued to be useful. The IC suggested that more information on the procedures in place, including how often the information is reviewed by CSE to determine whether it is still useful in protecting federal systems would be helpful to the Minister and himself. This would allow them to be satisfied that CSE is retaining information in accordance with legislation and internal policies.

CSE addressed the IC's remark in the authorizations related to non-federal infrastructures. CSE noted that operational managers are required to review the information on a quarterly basis to confirm whether it is still useful. Information that is no longer useful must be deleted.

Information related to Canadians or persons in Canada

The IC noted that the record provided to the Minister should include more details concerning information related to Canadians or persons in Canada that could be, and is, acquired under the authorization.

The IC explained that while the record sets out types of information related to a Canadian or a person in Canada that may be collected incidentally and retained, it said nothing about what information had actually been retained. While CSE must record rationales whenever Canadian-related information is retained, no information about these rationales was given to the Minister. The IC was of the view that CSE should have a solid grasp of the nature and volume of information that is retained and used, particularly when information related to a Canadian or a person in Canada is concerned. The IC would expect that CSE would in turn provide the Minister and himself with a greater understanding of the nature, frequency and volume of the retention of information where Canadian privacy interests are involved — since the manner in which an activity is conducted may be a factor in determining whether the activity itself is reasonable and proportional.

Use of acquired information for other aspects of CSE's mandate

The IC raised concerns about a blanket statement in the authorization which stated that CSE can use information acquired under one aspect of its mandate to serve other aspects of its mandate — as long as the information is relevant to the aspect in question and meets any particular requirement of the CSE Act that may need to be followed, such as applying privacy protection measures.

The IC did not disagree that CSE can use information gathered for one purpose to fulfill another aspect of its mandate. However, he raised a concern over what appeared to be the implication that CSE has free rein to use any information it acquires for all aspects of its mandate as long as it is "relevant" to that aspect. This was concerning because the cybersecurity authorization would allow CSE to acquire a large volume of information, including information that would benefit from a reasonable expectation of privacy — and CSE was already aware that some of the information would not be assessed as useful for this specific authorization. According to the general statement, CSE could nevertheless use this information for other aspects of its mandate.

The IC provided a hypothetical example highlighting his concern: it may be reasonable to incidentally acquire a large quantity of information on the basis that it is necessary for effective cybersecurity activities — even if some of the information benefits from a reasonable expectation of privacy and is not likely to be assessed as useful for the purpose of the authorization. However, it may no longer be reasonable if this information will also be used for other purposes or other aspects of CSE's mandate. The Minister's conclusions did not consider the impact of CSE's use of information across the five aspects of its mandate.

However, upon reviewing the record in its entirety — and CSE policies related to access and use of information within the agency in particular — the IC concluded that the general blanket statement found in the authorization was actually limited in practice. It was the IC's understanding that any access to and use of information acquired under a cybersecurity authorization — and not yet determined to be useful — is limited by CSE policies and must be consistent with the cybersecurity aspect of its mandate. Further, information related to a Canadian or a person in Canada cannot be retained unless it is found to be essential to identify, isolate, prevent or mitigate harm to non-federal IT infrastructures.

Regardless, the IC stated that any future use of a similar general blanket statement should reference these limitations, as it is imperative for both the Minister and the IC to understand how CSE is acting within limits imposed by the law.

AMENDED AUTHORIZATION

(section 15 of IC Act)

What does it authorize?

An amended authorization allows CSE to carry out activities that were not included in the original foreign intelligence or cybersecurity authorization.

Why is it required?

During ongoing activities, CSE might discover that it needs to undertake a particular activity that would not be covered by the ministerial authorization for the activities issued by the Minister and approved by the IC.

Why is the IC's role important?

Review by the IC ensures that CSE has sufficient justification for carrying out activities that were not included in the original authorization.

How does CSE obtain it?

To amend a foreign intelligence or cybersecurity authorization there must be a significant change in any of the facts submitted as part of the original request for the authorization. When this happens, CSE must notify the Minister of the change as soon as feasible. If the Minister concludes that the change in the fact is significant, they must notify the IC of this conclusion.

To justify a request for an amendment, CSE must provide information to the Minister with the same level of detail that it used to justify the initial request for authorization. The Minister may amend an authorization when they have reasonable grounds to believe that, taking into account the significant change, the legislative conditions have been met.

Decision rendered in 2023

During this reporting period, no authorizations were submitted for review.

Authorizations Related to CSIS Activities ::

DATASET REGIME

Background

In a 2016 decision, the Federal Court of Canada concluded that CSIS had exceeded its legal authority by keeping information that was not related to a threat to the security of Canada or to the target of a CSIS warrant (*X (Re)*, 2016 FC 1105). In response, recognizing that a modern security and intelligence agency could not carry out its investigation functions without conducting data analytics on Canadian data that is not directly threat-related, Parliament amended the CSIS Act in 2019, creating what is referred to as the "dataset regime."

The CSIS Act defines a dataset as, "a collection of information stored as an electronic record and characterized by a common subject matter." A dataset may contain anything from a very little to a vast quantity of information.

Analysing information in the datasets it assembles can help CSIS make connections or identify patterns and trends that would not be apparent using traditional investigative techniques.

Under the dataset regime, CSIS activities related to datasets require ministerial authorizations, 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 the person designated by the Minister, to retain a foreign dataset (the Director of CSIS has been designated for this purpose)
- the Director's authorization to query a Canadian or foreign dataset in exigent circumstances

CLASSES OF CANADIAN DATASETS

(section 16 of IC Act)

What does it authorize?

A Canadian dataset contains personal information that predominantly relates to Canadians or persons in Canada, or Canadian companies. The information does not directly and immediately relate to activities that represent a threat to the security of Canada.

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 allows CSIS to collect Canadian datasets – therefore personal information that is not directly related to a threat – which falls into one of the approved classes.

Why is it required?

The ministerial authorization and oversight by the IC are required because Parliament wanted to ensure that any collection of Canadian-related information by CSIS that was not threat-related was reasonable.

To collect a Canadian dataset, CSIS must have reasonable grounds to believe that it falls within one of the classes that has been authorized by the Minister and approved by the IC. CSIS must also be satisfied that even if the information in the dataset is not immediately and directly related to a threat, it is still relevant to its duties and functions.

Once collected, CSIS has 90 days to evaluate the dataset and determine if it falls within an "approved class". If it does — and CSIS wants to keep the Canadian dataset and use the information it contains — it must obtain authorization from the Federal Court.

Datasets that do not belong to an approved class must be destroyed, although there can be exceptions. If a dataset does not belong to an approved class but CSIS considers it important to its operations, it may ask the Minister for the determination of a new class to which the dataset would belong. This new class would also require IC approval.

Why is the IC's role important?

The IC's review ensures that CSIS exercises its authority to collect non-threat-related information about Canadians and persons in Canada in a balanced manner, and that the Minister has given proper consideration of privacy interests. 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 who collect the information.

How does CSIS obtain it?

At least once every year, the Director of CSIS provides an application to the Minister describing the classes of Canadian datasets for which collection of personal information would be authorized. To issue an authorization, the Minister must conclude that using the information of any dataset in the class could lead to results that are relevant to the performance of CSIS duties and functions.

Decisions rendered in 2023

Central to the IC's decisions relating to the dataset regime is whether the Minister and the Director have set a reasonable balance between the notions of broadness and specificity when determining a class or authorizing the retention of a dataset. Authorizations must be defined broadly enough to allow CSIS to access information that, while not immediately and directly related to a threat to the security of Canada, is likely to assist in the conduct of its operations — but must also be specific enough to protect the privacy of Canadians. A reasonable balance increases accountability by ensuring that CSIS provides the Minister and the Director with the information they need to understand the scope and limits of the information they are authorizing CSIS to collect and retain.

In the first decision, the IC found that the Minister's conclusions in determining four classes of Canadian datasets not reasonable, and therefore did not approve them.

The IC's decision was based on the following two grounds:

i. The breadth of each of the four classes was excessive. The IC found that the classes were defined so broadly that it was difficult, if not impossible, to determine which datasets would be excluded from the classes. The IC's conclusion echoed comments made by the Federal Court in *Canadian Security Intelligence Service Act (CA) (Re)*, 2022 FC 645. In that matter, CSIS was seeking judicial authorization to retain two Canadian datasets that fell within what were the approved classes at that time. The Court commented that those classes were "exceptionally broad in scope [...] it is difficult to see how any collection of personal information might be excluded given the breadth of their scope." The IC agreed with this principle and commented that for the classes of datasets to be meaningful, they must be more precisely defined and include tangible examples of the types of information to be collected.

ii. The record provided to the IC lacked details on the measures that would be taken to protect the privacy rights of Canadians and meet the legislative requirements of the dataset regime. The IC stated that the general statements provided were not sufficient and that CSIS should identify specific measures that would be undertaken.

Prior to the IC's decision, classes of Canadian datasets approved the previous year were still valid. CSIS had collected a dataset under one of them. However, after the IC's decision not approving the four classes, it meant there were no longer approved classes of Canadian datasets in effect.

"[D]etermining classes of Canadian datasets is the initial step that can eventually lead to CSIS retaining information on Canadians and persons in Canada that is not threat-related. Its impact on privacy interests of Canadians and persons in Canada have the potential to be enormous and egregious. [The IC's oversight] will ensure that classes of Canadian datasets are not broader than what is prescribed and intended by the legislation."

—IC Decision, 2200-A-2023-03, paragraph 42

As a result, CSIS employees could no longer confirm that the dataset it had previously collected belonged to an approved class. This confirmation is necessary before CSIS can apply to the Federal Court for an authorization to retain the dataset and use the personal information it contains. This left CSIS with the choice to either destroy the dataset, or ask the Minister to determine a new class to which the dataset would belong. CSIS chose to make a request to the Minister, who responded by determining a single class to cover the dataset in question. This determination was then submitted to the IC for review and approval.

In the second decision, the IC was satisfied that the Minister addressed the concerns raised in the earlier decision, and the new single class of Canadian datasets was approved. CSIS addressed the initial concern that the class was too broad by including three criteria that provided sufficient specificity to the class. The IC noted that "[w]hen evaluating whether a class is unreasonably broad, what matters is the cumulative effect of the criteria." In his view, the criteria that defined the class of Canadian datasets led to "useful specificity."

The concern relating to the protection of privacy rights was addressed by clearly setting out and explaining CSIS policies as well as the procedural steps taken to protect the privacy rights of Canadians and persons in Canada. In this regard, the IC commended the collaboration between CSIS and the CSE in sharing their practices relating to protecting Canadian privacy interests. He noted the importance of agencies and departments in the national security and intelligence environment to avoid working in silos and to share processes, procedures and best practices.

RETENTION OF A FOREIGN DATASET

(section 17 of IC Act)

What does it authorize?

A foreign dataset is one that contains personal information predominantly related to non-Canadians who are outside of Canada or to non-Canadian companies.

With authorization from the Director of CSIS, CSIS may retain and use personal information about non-Canadians and persons 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?

After collecting a foreign dataset, CSIS cannot retain the dataset without a ministerial authorization issued by the Director. Approval of the authorization by the IC provides additional oversight, helping to ensure that the datasets retained by CSIS are in fact foreign datasets and do not contain information about Canadians or persons in Canada.

Why is the IC's role important?

The IC's review helps to ensure that CSIS has taken appropriate measures to delete any Canadian-related information, and is not retaining information that relates to the physical or mental health of an individual that a person would reasonably expect to remain private.

How does CSIS obtain it?

CSIS officials provide an application for retention of the foreign dataset to the Director. The application includes a description of the origin of the dataset, what it contains and how it was evaluated. To authorize the retention of the dataset, the Director must conclude that the dataset is indeed a foreign dataset; that its retention is likely to assist CSIS in the performance of its duties and functions; and that CSIS has destroyed any information relating to a Canadian or a person in Canada, as well as any information about the physical or mental health of an individual that a person would reasonably expect to remain private.

Decisions rendered in 2023

The IC approved three authorizations to retain a foreign dataset issued by the Director. In so doing, the IC was satisfied that the Minister's conclusions that the legislative requirements had been met were reasonable.

The IC also reviewed the reasonableness of the Minister's conclusions concerning how the datasets could be updated. While recognizing that the CSIS Act does not explicitly state that these conclusions are subject to the IC's review, the IC explained that the Act requires an authorization to retain a foreign dataset to specify the manner in which CSIS may update the dataset.

The IC also explained that his role is to review the conclusions that the Director is required to make when authorizing the retention of a dataset. The IC was therefore of the view that his responsibility extended to reviewing the conclusions concerning elements that must be specified in an authorization — such as the provisions for updating a dataset. The IC's conclusion in this regard was supported by the record in which CSIS recognized that the IC could find the Director's conclusions unreasonable based on the update provisions.

In his analysis of the update provisions, the IC referred to the Federal Court's decision in *Canadian Security Intelligence Service Act (CA) (Re)*, 2022 FC 645, in which the Court had raised a concern that the provisions for updating two Canadian datasets provided too much latitude to CSIS to modify them.

This general concern over CSIS having carte blanche to update a dataset also resonated with the IC. In the IC's view, the Director's conclusions related to updating a foreign dataset could be reasonable if the record reflects that the update will not change the nature of the authorized dataset. To determine this, a helpful question to consider is whether, when the Director authorized the retention of the foreign dataset, his understanding of the nature of the dataset could have included the proposed updates. In these instances, the IC was satisfied that the conclusions concerning the update provisions in the foreign datasets were reasonable because they would not change the nature of the datasets.

Notable remarks in the decisions

"Likely to Assist" Threshold

The "likely to assist" threshold does not require that the foreign dataset will eventually assist CSIS in the performance of its duties — only that it could potentially be of assistance. Over time, however, whether a specific dataset meets the "likely to assist" threshold may need to be revisited. In the IC's opinion, if a new request for an authorization to retain a foreign dataset beyond the initial retention period is submitted, the Director and the IC should be provided with at least an overview of its past usefulness. Even though the "likely to assist" threshold is forward looking, in reviewing a request to retain a foreign dataset, the IC believes that information about how it has been used in the past — when this information is available — may be a worthwhile factor to consider in evaluating whether it is "likely to assist."

Delay in authorizing the foreign dataset by the Director

In one of the requests for the retention of a foreign dataset, the Director acknowledged the significant delay between the request CSIS made and the issuance of the Director's authorization. The IC found that the documentation provided by the Director indicated that the length of time between the actual collection of the foreign dataset and the Director's authorization to retain it did not affect the value of the information. Nevertheless, the IC did not rule out the possibility that the passage of time could, in some circumstances, affect the reasonableness of the Director's conclusions — namely, how the information in the dataset would still be "likely to assist" CSIS.

The IC also indicated that any potential effects of the passage of time could be increased by the fact that there is no statutory time limit within which the Director must issue an authorization to retain a foreign dataset after receiving a request from CSIS to do so. The IC was not convinced that Parliament intended for there to be such a long delay between such a request and authorization.

QUERY OF A DATASET IN EXIGENT CIRCUMSTANCES

(section 18 of IC Act)

What does it authorize?

Querying a dataset means conducting a specific search of a dataset for information about a person or entity. The Director's authorization to query a dataset in exigent circumstances allows CSIS to conduct this type of search in situations where there is an urgent need for information and the approval for the retention of the dataset has not yet been sought.

Why is it required?

Normally, CSIS may query a dataset only after it has obtained approval to retain the dataset from the Federal Court (for a Canadian dataset) or the IC (for a foreign dataset). Requiring approval to retain a dataset ensures CSIS is exercising its authority to collect non-threat-related information in a reasonable way. However, the legislation recognizes that urgent situations may arise in which delaying a search for information in datasets could pose a risk.

The CSIS Act sets out two instances in which exigent circumstances exist:

- to preserve the life or safety of an individual
- to acquire intelligence of significant importance to national security, the value of which would be diminished or lost if CSIS had to comply with the retention authorization process

Why is the IC's role important?

The IC ensures that the Director's rationale for determining that exigent circumstances exist is sufficiently supported by the factual context.

How does CSIS obtain it?

CSIS submits an application to the Director of CSIS. To issue the ministerial authorization, the Director must conclude that the dataset in question is likely to assist CSIS in the performance of its duties and functions and that the query of the dataset is required in exigent circumstances.

The authorization issued by the Director must contain a description of the exigent circumstances and the dataset to be queried as well as the grounds on which the Director concludes that the query is likely to produce the intelligence required.

Prior to the query taking place, the IC must be satisfied that the conclusions of the Director are reasonable and approve the authorization "as soon as feasible" in a written decision. Should CSIS want to retain the queried Canadian or foreign dataset it must obtain the respective approval from the Federal Court or the IC.

Decision rendered in 2023

During this reporting period, no authorizations were submitted for review.

CLASSES OF ACTS OR OMISSIONS – JUSTIFICATION FRAMEWORK

(section 19 of IC Act)

What does it authorize?

A ministerial authorization respecting classes of acts or omissions allows CSIS employees or persons acting under their direction to carry out activities that would otherwise be against the law in Canada. The authorization from the Minister of Public Safety must specify the types or "classes" of acts and omissions that are to be allowed, and the classes must be approved by the IC. This is referred to as the "justification framework."

Why is it required?

CSIS investigates activities suspected of constituting threats to the security of Canada and reports on these to the Government of Canada. The CSIS Act recognizes that collecting information and intelligence on potential threats 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. Not being able to participate in the unlawful activity could put the people involved in the investigation at risk.

The justification framework provides immunity from prosecution to designated CSIS employees and persons working under their direction who commit otherwise unlawful acts that fall within one of the approved classes. The justification framework may also allow for information collected as a result of otherwise unlawful conduct to be considered to have been collected lawfully.

However, the justification framework does not mean designated CSIS employees and persons directed by them are above the law, nor does it allow them to infringe the safeguards guaranteed by the Charter. Anyone operating outside the limits of the approved framework could face criminal charges.

Limitations

(section 20.1 (18) of 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

Why is the IC's role important?

The IC's review ensures that the acts or omissions that would otherwise be unlawful are restricted to activities related to CSIS' duties. The IC's review holds the Minister accountable by ensuring the classes of otherwise unlawful acts or omissions that CSIS may commit or direct a person to commit are reasonable and proportional. The review also ensures that the classes of acts are well-defined and will be clearly understood by the CSIS employees who will ultimately have to decide whether a proposed unlawful act or omission falls within an approved class.

Only employees who have been "designated" by the Minister, on the recommendation of the Director, can commit or direct the commission of otherwise unlawful acts.

How does CSIS obtain it?

The Director of CSIS submits an application to the Minister of Public Safety that contains a description of the classes of offences, as well as a list of the main offences that would fall within each proposed class. The Minister must determine whether committing those acts or omissions is reasonable — taking into account CSIS' duties to collect information and intelligence and any threats to the security of Canada that may be the object of these activities.

"A proposed class, or the inclusion of specific acts or omissions in a proposed class, that may have an impact on an interest important to Canadians should be appropriately justified by the Minister's conclusions. As the decision maker, the Minister should be able to demonstrate with his conclusions that a class that includes an offence or offences that impact such an interest should be approved."

—IC Decision, 2200-A-2023-02, paragraph 64

Decisions rendered in 2023

In 2023, the IC reviewed two ministerial authorizations in relation to the justification framework. The IC focused on the need for the Minister's conclusions to provide a clear definition of the boundaries of each class. Indeed, the Minister's conclusions must reflect a good understanding of the broad purpose of the class; what types of acts or omissions fall within each class; and why they are necessary for CSIS to carry out its mandate. Clearly defined classes not only strengthen ministerial accountability, they allow CSIS employees and persons directed by them to have confidence in their understanding of the acts or omissions included in each class. They also guide CSIS in the lawful conduct of its investigative operations.

In the first decision, the IC approved seven of the eight classes determined by the Minister. The IC did not approve one of the classes for three reasons:

i. Some of the specific offences included in the class did not correspond to the definition of the class. The Minister did not justify why they should be included in the class.

ii. The IC found that it was unclear whether some offences included in the class could in fact be committed without violating the six specific limitations set out in the CSIS Act. The IC was of the view that if an act or omission will necessarily fail to respect the limitations, it cannot be included in the class.

iii. The IC found that certain offences in the class were offences that interfered with the course of justice. In making this finding, the IC emphasized that institutions of justice — not just courts of law, but all bodies and procedures whose goal is to ensure the respect of rules — are fundamental to the rule of law, which is of central importance to Canadians. When specific acts or omissions in a class may have an impact on fundamental Canadian institutions, the Minister must justify the impact with clear, specific and robust conclusions. The IC was of the view that the Minister had not sufficiently considered the impact of the class on these institutions.

The IC determined that the IC Act does not include the authority to carve out problematic types of acts or omissions from an otherwise reasonable class — the IC must either approve the entire class or not approve the entire class.

In response to the specific concerns raised in the IC's first decision described above, CSIS prepared a revised class that was determined by the Minister and submitted to the IC for review. In the second decision, the IC noted that the revised version of the class specifically excluded offences that could conflict with any of the "red line" limitations set out in the CSIS Act. CSIS also added new examples and provided additional details in the description of the class to ensure that it was clearly defined and narrowed. Satisfied that the concerns raised in the earlier decision had been addressed, the IC approved the class.

Notable remarks in the decisions

Broadly defined classes

The IC commented on the challenges in determining and giving effect to a class that is extremely broad, partly because some terms are not defined. As a result, a broad class may require more elaborate ministerial conclusions. The IC also reiterated that the description of the classes must make it clear that the acts or omissions listed are subject to the six limitations of the CSIS Act, and that nothing in the justification framework can justify the commission of an act that would infringe a right or freedom guaranteed by the Charter.

Validity period of a ministerial authorization

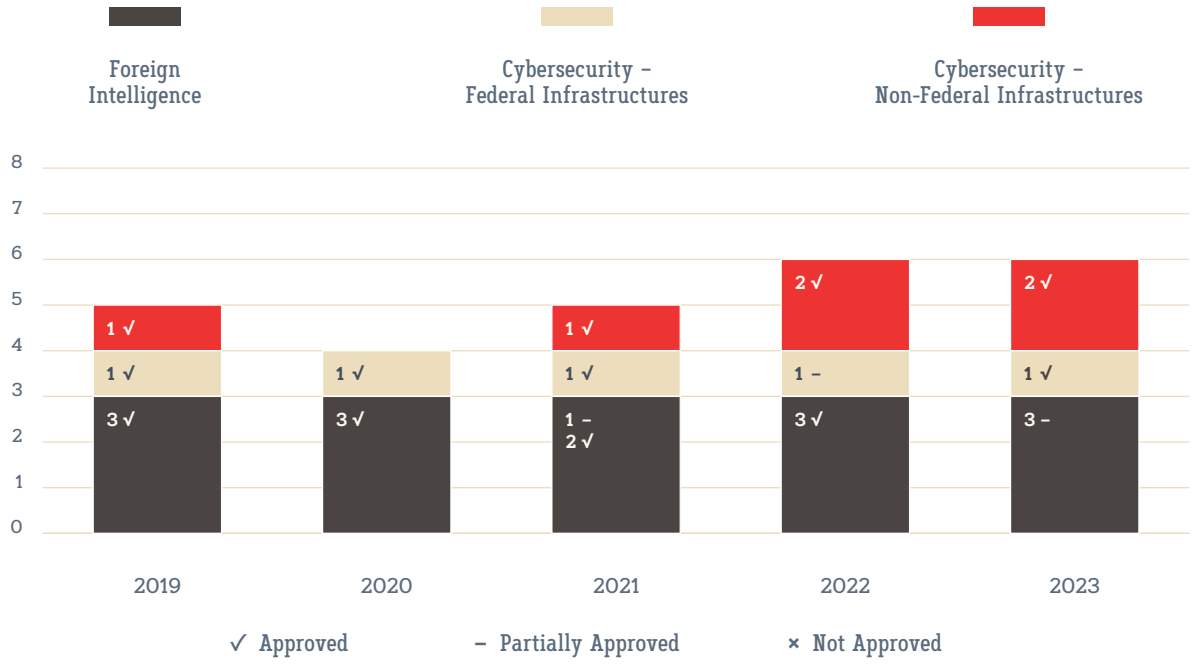
The IC took the opportunity to clarify an issue related to the validity period of a ministerial authorization. This is not specified in either the CSIS Act or the IC Act.

According to the Minister's interpretation, a class of acts or omissions would expire one year from the date of its determination — not one year from the date it was approved by the IC. The IC could not endorse this interpretation as it would effectively result in the determination of classes being valid for 11 months instead of one year. Further, this interpretation would mean that in previous years, there would have been a period during which there were no valid classes. This would also have been the case for classes of Canadian datasets under the dataset regime where the statutory language is the same.

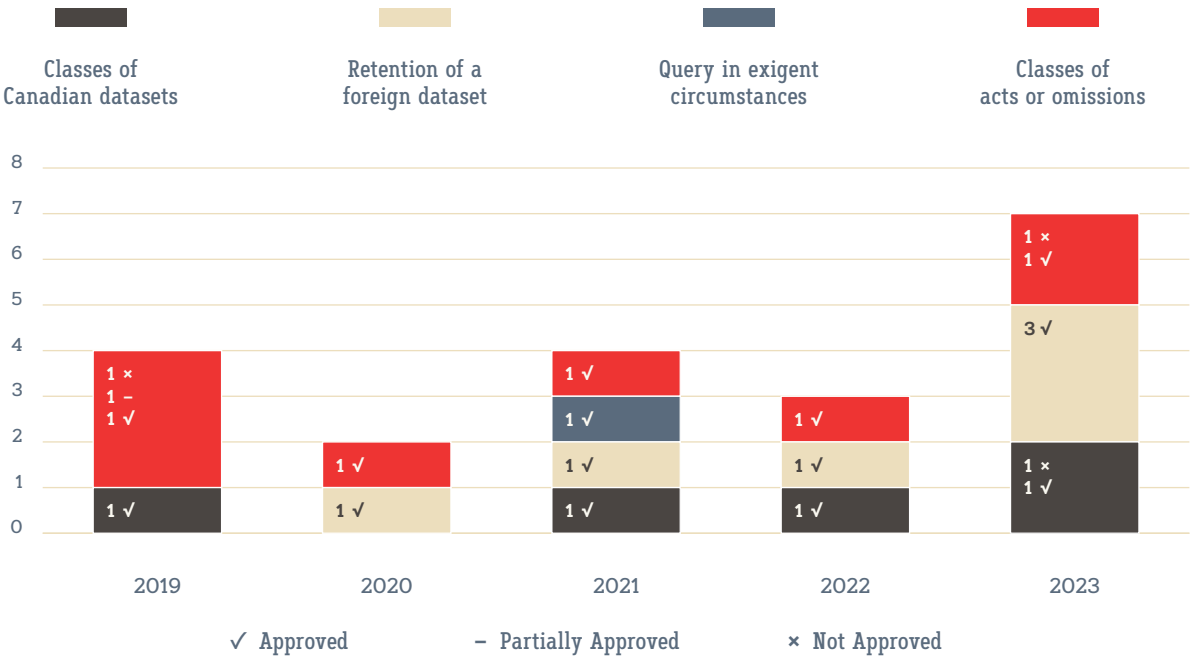
The IC pointed out that, in accordance with the CSIS Act, the Minister must determine classes "at least once every year". As this is the only reference to a validity period, the IC was of the view that the text and the context of the legislation lead to the interpretation that classes are to be valid for one year. Given that a determination is not valid until approved by the IC, this requires that the one-year validity period runs from the date the determination is approved by the IC.

5 Years – Results ::

Authorizations reviewed by the IC – CSE activities



Authorizations reviewed by the IC – CSIS activities



ORGANIZATION

IC

::

is appointed by Order in Council for a fixed term

::

must be a retired judge of a superior court

::

performs duties and functions on a part-time basis

::

is the Chief Executive Officer and Deputy Head of the ICO

ICO

::

supports the fulfillment of the IC's independent oversight mandate

::

Workforce
10

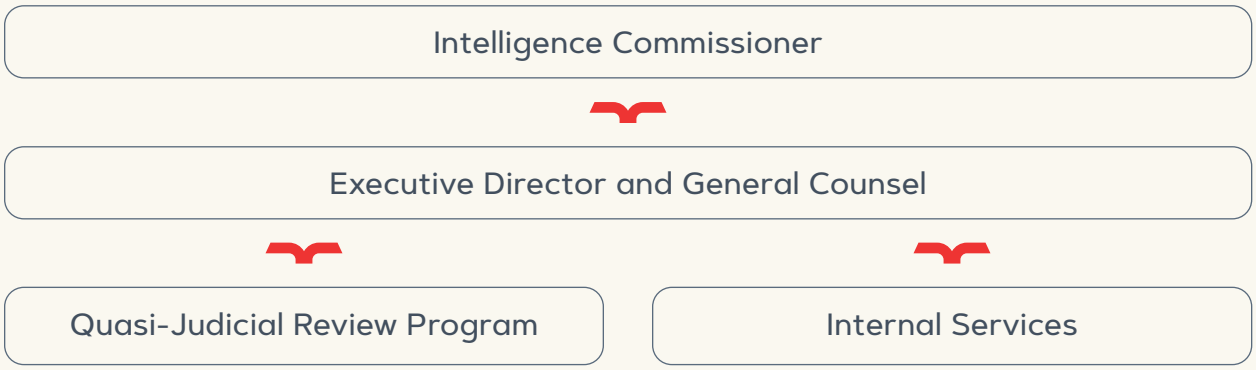
::

is a separate agency listed in Schedule V of the *Financial Administration Act*

::

$2,555,387
2023–24
Operating
Budget

Organizational Structure ::



The IC is supported by the Executive Director and General Counsel who is responsible for the management of the day-to-day operations of the ICO, 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 has an internal services program, which consists of the services that are provided for the ICO to meet its corporate obligations and deliver the quasi-judicial program. Services include: human resources, financial management, security, information technology, and information management.

Transparency ::

The IC communicates with the Canadian public through his decisions. The IC remains committed to making his decisions available and accessible to the public on the ICO website. To limit the amount of text that is redacted for reasons of national security in the public version of the decisions – and therefore improve the readability of the decision – this year, the IC started including a classified annex where a description of the activities and other classified information is included. The IC's analysis remains in the public version of the decision to ensure as much transparency as possible.

Collaboration ::

The IC is entitled to receive 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 2023, the IC received three reports from NSIRA.

On the international front, the ICO is a member of the Five Eyes Intelligence Oversight and Review Council (FIORC). FIORC was created in 2017 in the spirit of the existing Five Eyes partnership, the intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. The ICO participated in the 2023 FIORC annual meeting with the theme of the Lifecycle of National Security Accountability, held in Canada and hosted by NSIRA. FIORC members exchanged views on subjects of mutual interest and concern, and compared best practices in review and oversight methodology, accountability and transparency.

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 Commission of Inquiry Concerning 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.