2025

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

Photo credit : Richard Tardif

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

March 31, 2026

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 2025 calendar year, for your submission to Parliament.

Sincerely,

The Honourable Simon Noël, K.C.
Intelligence Commissioner

Canada

Table of Contents

INTELLIGENCE COMMISSIONER'S MESSAGE

Global developments in 2025 have reinforced the reality that Canada faces a complex national security and intelligence environment. While these challenges demand robust responses, they do not diminish Canadians' expectation that our national security and intelligence agencies operate within the rule of law. My 2025 Annual Report shows how my oversight continues to contribute to upholding this fundamental expectation.

In 2025, I issued 14 decisions, the most in a single year since the Intelligence Commissioner position was created in 2019. Even in my fourth year in the position, new issues continue to be raised through my oversight. This year, I considered the legal requirement for the renewal of dataset authorizations for the first time, assessed new activities the agencies sought approval for, and examined novel legal interpretations they raised. For the second year in a row, I issued a decision on an urgent basis with reasons to follow.

My decisions – which are made public – allow Canadians to understand why I find an authorization reasonable or not. Even though details about the activities themselves may be redacted for national security purposes, my decisions raise legal and operational issues that I believe Canadians should be aware of. Greater transparency strengthens public confidence in our national and security agencies and promotes the accountability necessary for lasting improvements.

I am pleased to report that CSIS and CSE have been responsive to the issues I raise in my decisions, whether by making necessary adjustments or providing additional information. My decisions effectively create a public record of how these concerns are being addressed. This process has led to concrete improvements in oversight. For example, decision makers and I now receive more detailed information of past authorizations, and the agencies have updated their internal policies in response to my remarks. In this year's decisions, I make a point of describing how CSE and CSIS have responded to past remarks, as well as identifying issues on which I am still awaiting additional information. Tracking this progress helps build public confidence by demonstrating that the oversight process leads to tangible improvements in the conduct of cybersecurity and intelligence activities.

One notable issue raised in my 2025 decisions concerns legal questions relating to activities that were not sufficiently described or justified in the authorizations. In these instances, I requested the agencies to provide additional information or to submit a new application to the Minister with further justification, in particular where a novel legal approach was involved. This Annual Report provides additional detail on these matters and my decisions will continue to address further developments.

The Intelligence Commissioner occupies a unique vantage point, with oversight over activities of both CSIS and CSE. I have used this position to identify areas where greater coordination or collaboration between the two agencies could yield improvements. In 2025, I identified legal issues common to both agencies and requested that they adopt a consistent approach to addressing them.

In an increasingly tumultuous world, the respect and value that Canadians have in democracy, the rule of law, and fundamental rights and freedoms are not prevalent everywhere. At a time when these values appear to be weakened in the global sphere, they must remain guiding principles for our security and intelligence agencies when engaging in national security activities.

My independent oversight helps assure Canadians that these agencies continue to be directed by these principles. It also helps define the boundaries within which CSE and CSIS can confidently operate and provides employees of the agencies with guidance on how to conduct their activities in compliance with the law and the *Canadian Charter of Rights and Freedoms*. Through my decisions, Canadians gain a clearer understanding of how these activities are conducted and overseen. And while the time we live in may call for new or updated powers for our agencies, such powers must continue to be accompanied by effective oversight and review.

My work is made possible through the dedication of the staff at the Office of the Intelligence Commissioner. I thank them for their expertise and professionalism in support of the successful delivery of my mandate.

I invite you to read this report to learn more about how the oversight process works to protect your rights and interests when I decide whether to approve the authorizations that come under my review.

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**
- **2025-26 Operating Budget is $2,635,580**

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:

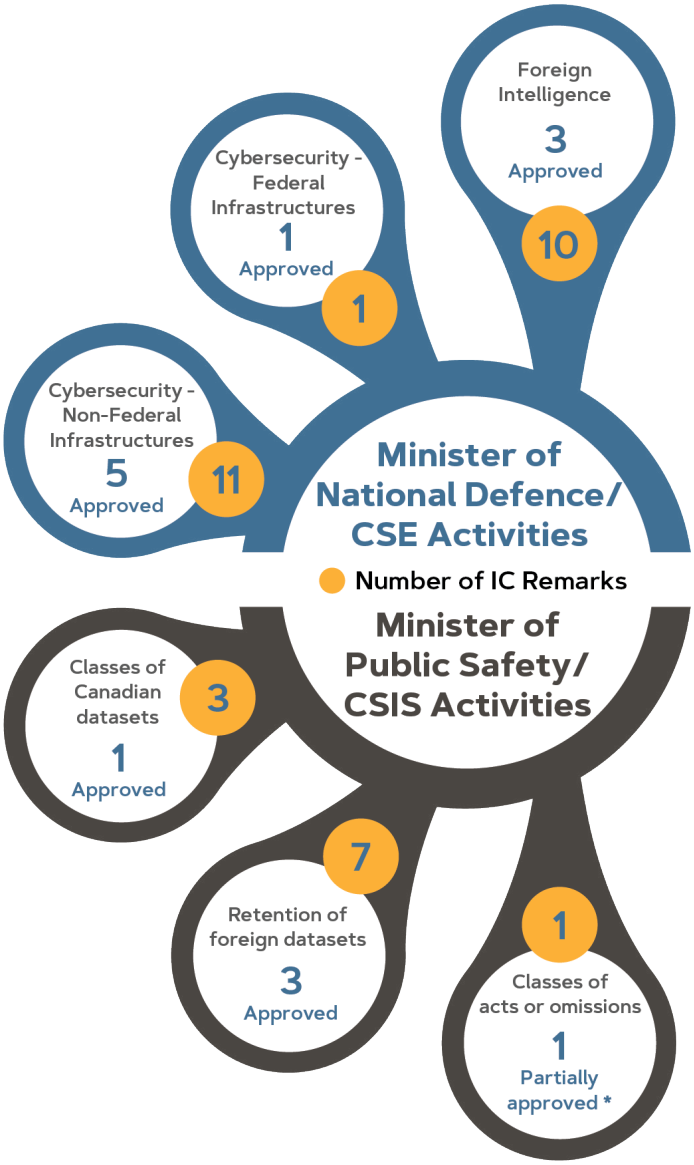
i. Classes of Canadian datasets;

ii. Retention of a foreign dataset; and

iii. 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.

Authorizations reviewed and IC decisions – 2025



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.

***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.

YEAR IN REVIEW

2025 Results at a glance

Authorizations

14 Received

13 Approved

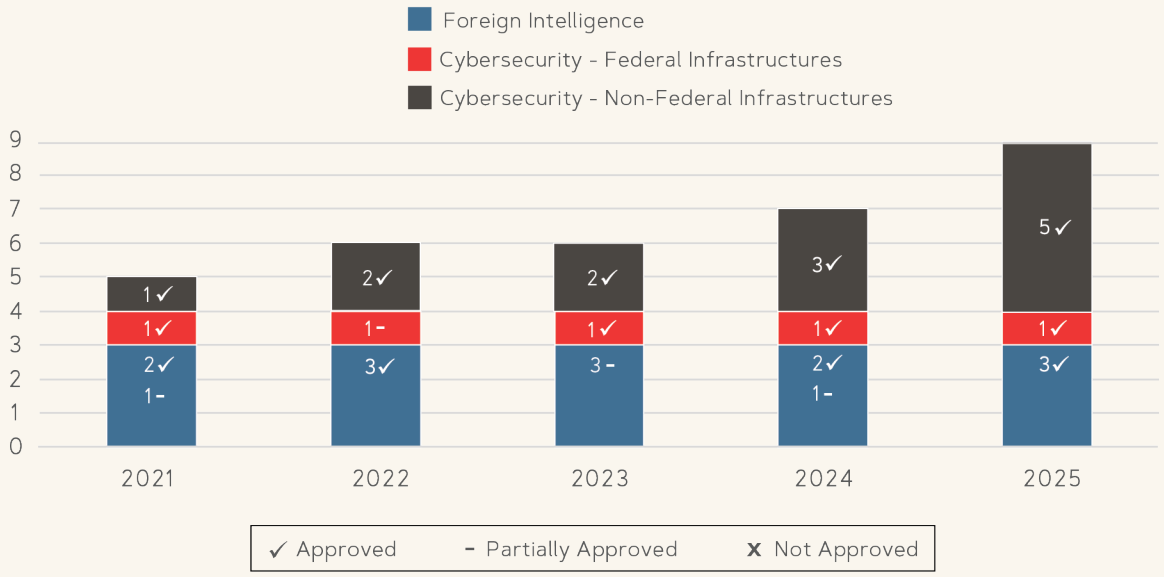
1 Partially approved

100% of decisions rendered in accordance with legislated timeframe

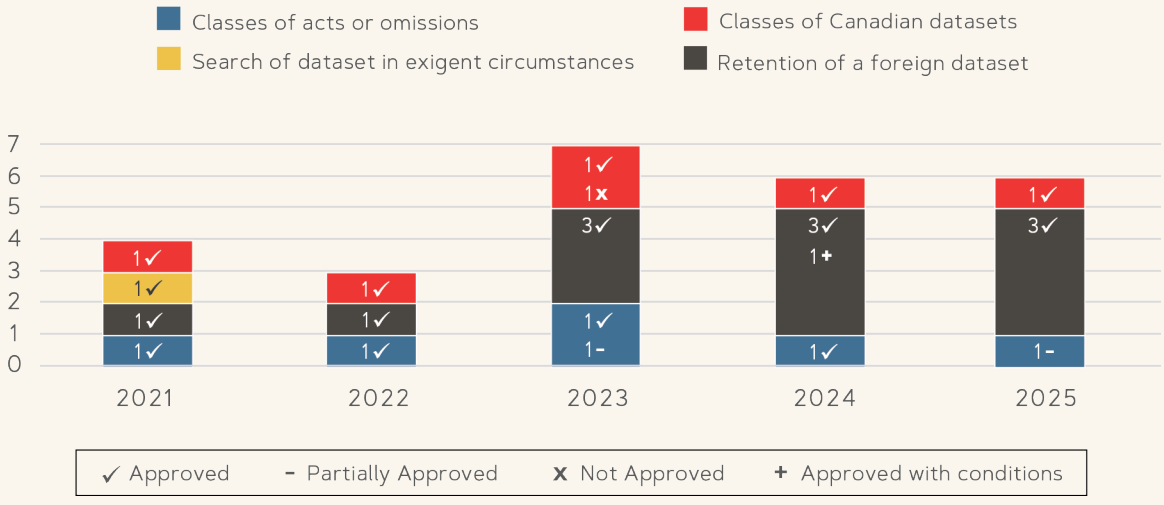
33 Remarks made by the IC

5 year overview

Authorizations reviewed by the IC CSE Activities



Authorizations reviewed by the IC CSIS activities



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.

Issuing a ministerial authorization is an important responsibility because it allows CSE and CSIS to undertake activities that contravene the laws of Canada, or potentially interfere with 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?

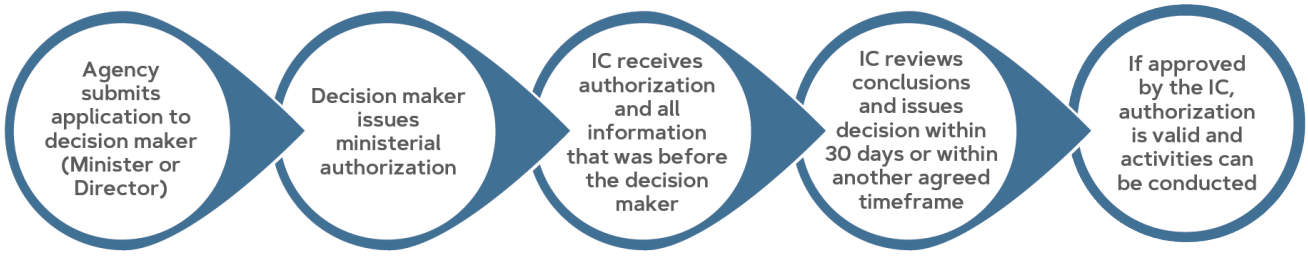
The Minister or Director provides conclusions – essentially reasons – supporting the activities set out in a ministerial authorization and explaining how the legislative requirements have been satisfied. The IC reviews these conclusions to determine whether they are reasonable. The IC applies the "reasonableness" standard of review as it is applied by Canadian courts: a reasonable decision is one that is justified, transparent and intelligible.

The IC's oversight ensures that the Minister or Director 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.

The IC may also receive information that is not directly related to a specific review to assist in the exercise of the IC's duties. The IC receives occasional 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 fulfil his role.



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. The IC must subsequently approve the authorization.

FOREIGN INTELLIGENCE AUTHORIZATION

(Section 13, IC Act)

What does it authorize?

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.

Why is the IC's role important?

The IC ensures that the foreign intelligence activities described in the authorization will not be directed at Canadians or persons in Canada, and that they are conducted in a way that is reasonable and proportional. The IC also verifies that the authorization includes measures that limit the impact on the privacy of Canadians and persons in Canada.

CYBERSECURITY AUTHORIZATION

(Section 14, IC Act)

What does it authorize?

CSE provides advice, guidance and services to help protect IT systems from hackers and other cyber threats. A cybersecurity authorization allows CSE to acquire information that may interfere with the reasonable expectation of privacy of Canadians or persons in Canada when conducting cybersecurity activities on IT systems. These systems can belong to the Government of Canada or to non-federal entities designated as being of importance to the Government – such as in the health, energy and telecommunications sectors.

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 or persons in Canada. The IC also ensures that CSE has appropriate measures in place to limit any impact on the privacy of Canadians and persons in Canada.

CSE and information related to Canadians

Although CSE cannot target Canadians or persons in Canada or infringe the *Canadian Charter of Rights and Freedoms* (Charter), it 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 this type of information 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.

Authorizations related to CSIS activities

DATASETS

The dataset regime set in out in the CSIS Act 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 assist CSIS in its duties. Analyzing personal information found in datasets can allow 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.

CLASSES OF CANADIAN DATASETS

(Section 16, IC Act)

A **Canadian dataset** predominantly relates to Canadians or persons in Canada. The IC must approve all classes of Canadian datasets.

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. To collect a Canadian dataset, CSIS must reasonably believe that it falls within an approved class. CSIS then evaluates any collected dataset to confirm whether it falls within a class approved by the IC. If it does, and CSIS seeks to retain the Canadian dataset, it must obtain authorization from the Federal Court.

Why is the IC's role important?

The IC ensures that the classes of Canadian datasets are relevant to CSIS' duties and are not too broad. 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. The IC must approve the retention of all foreign datasets.

What does it authorize?

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

Why is the IC's role important?

The IC's oversight confirms that the foreign datasets are related to CSIS' duties. The IC also ensures that CSIS has taken appropriate measures to remove any information that relates to a Canadian or a person in Canada and to also delete any private information that relates to the health of an individual.

CLASSES OF ACTS OR OMISSIONS – JUSTIFICATION FRAMEWORK

(Section 19, IC Act)

What does it authorize?

The justification framework allows designated CSIS employees, or persons acting under their direction such as human sources, to carry out activities that would otherwise be against the law in Canada. The IC must approve the classes of otherwise unlawful activities that CSIS can carry out.

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. 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. The ministerial authorization specifies the types or "classes" of acts or omissions that are allowed.

Why is the IC's role important?

The IC ensures that the classes are reasonable, well-defined and will be clearly understood by CSIS employees. The IC also confirms that the classes do not include prohibited activities and that there are appropriate safeguards for activities that may have an effect on interests important to Canadians – for example when they may have an impact on Canadian fundamental institutions such as academia, the free press, and democratic institutions.

Limitations

(Section 20.1(18), CSIS Act)

Certain activities 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

Simply repeating the statutory language that a class does not include acts or omissions that violate the statutory limitations or that infringe a Charter right or freedom is insufficient for defining a class. To render a justified decision, and to provide meaningful guidance to designated employees, it is necessary for the Minister's conclusions – and therefore the class definition – to actually apply these general limitations to the specific offences or types of offences being contemplated.

Decision CSIS-2025-01

ACTIVITIES OF THE INTELLIGENCE COMMISSIONER — 2025

Key findings in the IC's decisions

The IC's decisions are dynamic. They evolve to respond to new authorizations that may be based on updated information from the agencies, reflect changing circumstances, or adopt novel legal positions. While each decision applies to a specific authorization, it can also provide guidance that the agencies can draw on when planning future activities. Here are some key findings made by the IC in 2025.

PROPER SCOPE OF A CATEGORY

In **Decision CSE-2025-05**, the IC found that a foreign intelligence authorization did not – and legally could not – authorize an expanded set of supporting activities that the record suggested were included.

The scope of supporting activities has been a recurring issue in the IC's reviews of foreign intelligence authorizations since 2023. While the CSE Act provides that such authorizations may permit CSE to carry out "any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity," the Minister's conclusions must show a clear understanding of the specific supporting activities being authorized. This requires more than simply repeating the language found in the Act.

In this case, the record contained references suggesting that the supporting activities were not limited to supporting the activities set out in the current authorization. They could also be conducted to include supporting activities in other authorizations.

After careful examination of the wording of the authorization, of the CSE Act, and of relevant past decisions, the IC concluded that the ministerial conclusions were reasonable. Unlike some of the references in the record, the authorization itself properly confined supporting activities to those that would support only the activities described in the authorization. This decision reinforced previous conclusions that the scope of activities authorized by a minister must fall within the boundaries set by legislation.

DELINEATION OF A CLASS

In **Decision CSIS-2025-01**, the IC did not approve the Minister's authorization of a new class of acts or omissions – the only instance of non-approval in 2025. He did however approve the other eight classes in the authorization, which were the same as classes that had been approved in previous years.

The IC found that the Minister's conclusions did not explain how certain otherwise illegal acts that appeared to be included in the proposed new class would comply with the restrictions in the CSIS Act, which specify the types of acts that can never be justified. Equally important for the IC, the conclusions did not consider the potential impact of those acts on Canadian fundamental institutions such as academia, the free press, and democratic institutions.

The IC noted that it is not enough for the definition of a class to simply repeat the language from the legislation that acts that do not respect the statutory limitations are excluded. The Minister's conclusions must show that consideration was given to whether the acts described interact with the limitations in the CSIS Act, and how. The failure to address whether those restrictions were engaged created uncertainty as to whether certain acts were intended to be included in the class or excluded from it.

Role of the IC remarks in strengthening oversight

The remarks the IC includes in his decisions foster an ongoing dialogue with the agencies, helping to strengthen and improve the oversight process. By providing Canadians with insight into the types of concerns the IC has identified, and how the agencies work to address them, the remarks also contribute to a culture of accountability within the agencies.

The agencies have made timely and continuing efforts to address his remarks. These efforts have helped refine and strengthen the ministerial authorization regime. The examples below outline some of the key issues raised in the IC's remarks in his 2024 annual report, and how CSE and CSIS responded in 2025.

REPORTING OF COMPLIANCE INCIDENTS

The IC expects both agencies to promptly notify him and their respective ministers of any breach of the terms of an approved authorization. Timely notification is essential to addressing the IC's primary concern that agencies take immediate action to mitigate any impacts on privacy interests or the rule of law, and implement measures to reduce the risk of a reoccurrence. Through his decisions, the IC promotes transparency by describing how compliance issues are identified, addressed, and considered.

Recommending a policy on publicly disclosing compliance incidents

In his 2024 annual report, the IC described a compliance incident reported by CSE that involved the sharing of some information with international partners between 2020 and 2023 without first removing incidentally acquired information about Canadians. Throughout 2024, CSE kept the IC informed of its actions to mitigate the impacts of the incident.

In early 2025, CSE provided the IC with the results of its internal review, which identified a failure to follow internal policies as the cause of the non-compliance. The IC was satisfied with the thoroughness of CSE's response. The agency implemented robust internal measures to mitigate the impact of the breach, as well as new safeguards to reduce the risk of future gaps in compliance when sharing information with international partners.

After reviewing CSE's internal investigation report, the IC made a specific recommendation: that CSE develop an internal policy to govern its public disclosure of compliance incidents. Such a policy could guide CSE's approach to public disclosure – including when and how information would be disclosed – and reinforce the agency's commitment to transparency.

Providing information on past compliance incidents

In **Decision CSIS-2025-04**, for the first time since the dataset regime was established, CSIS applied for the renewal of an authorization to retain a foreign dataset. While applications for a renewal must meet the same legislative requirements as a new authorization, the IC pays particular attention to whether and how his remarks from previous decisions have been addressed.

In the original decision **(Decision CSIS-2024-05)**, the IC approved the authorization for one year rather than the five years requested, on the grounds that CSIS had not provided information related to a compliance incident involving the over-retention of Canadian-related information.

In his 2025 decision approving the renewal, the IC was satisfied with CSIS' responses to his original concerns over the missing information. At the same time, he reiterated his expectation that CSIS inform him without delay of confirmed compliance incidents as well as potential incidents that could impact future decisions.

This expectation was met in **Decision CSIS-2025-05**, where all documentation related to a potential compliance incident was included. The IC found that all remarks made by the former IC in 2020 had been addressed, while expanding

on one remark relating to the age of the information in the dataset. The IC asked CSIS to consider in future applications how the passage of time could affect whether the information continues to meet the "likely to assist" threshold required by the legislation.

Reporting of possible incidents of non-compliance

In last year's **Decision CSIS-2024-06**, the IC approved an authorization but raised concerns about a search of a dataset during the evaluation period that may have gone beyond what is permitted under the CSIS Act. Considering this a possible compliance incident, the IC requested CSIS to provide additional information to both him and the Director. In January 2025, the Director provided additional information to the IC to show that the search did not contravene the CSIS Act. Nevertheless, he advised that CSIS had referred the matter to its internal compliance procedures for an independent review.

SHARING OF RELEVANT INFORMATION

Ensuring that the ministers and the Director of CSIS have access to all relevant information when deciding whether to authorize activities is a matter of ongoing concern for the IC. Through his decisions, the IC has sought to improve the flow and completeness of relevant information and to encourage greater detail in reporting on the results of previous authorizations.

Access to Cabinet confidences

The IC Act currently does not entitle the IC to receive Cabinet confidences, even when this information may have been relied upon by a minister when issuing an authorization. In past decisions, the IC has noted that providing him with access to documents subject to Cabinet confidence – even in redacted form – should be considered in future applications. Without access to documents the minister has relied on to issue an authorization, the IC cannot fully assess whether the minister's conclusions are reasonable

Public inquiries into national security matters have demonstrated that Cabinet confidences can be effectively disclosed in a limited way without compromising their essential purpose. The IC already receives some documents related to Canada's intelligence priorities, and Public Safety Canada has recognized that additional documents relating to them could help better contextualize CSIS' duties and functions. The IC has welcomed the initiative, as expanding access would help strengthen the oversight process without intruding on core Cabinet confidences important to our system of government.

Greater substantive detail in reporting

The IC's approval of an authorization does not entail automatic approval of the same activities in the future. Each authorization is distinct: circumstances change, and new or updated information may also impact the substance of an application for renewal. The IC has made a number of remarks emphasizing the need for records to include more detailed reporting on the outcomes of past activities and on how the information collected is used. These remarks have led to notable improvements to the contents of the materials the agencies submit to their respective minister and the IC.

For example, following past remarks that applications to the Minister should reflect the operational reality, CSE now confirms to the Minister that information relating to Canadians "will" be incidentally acquired, where past applications indicated that such information "may" be acquired incidentally **(Decision CSE-2025-02)**. This shift from "may" to "will" reflects a more forthright acknowledgment of the operational reality and demonstrates how the IC's oversight encourages increased transparency and accountability.

In **Decision CSE-2025-03**, the IC noted that updated information included in the record offers a more comprehensive understanding of the types of information relating to Canadians and persons in Canada that is acquired incidentally through CSE data collection activities, and if or how it is shared beyond CSE.

The IC's decisions relating to CSIS also underscore his expectation that documentation align with the operational reality. For example, the IC has emphasized the need for additional

information to ensure the Minister has a complete picture of how the justification framework is applied, as well as how it has been applied in past years. In **Decision CSIS-2025-01**, CSIS addressed this concern by providing a copy of its relevant procedures and internal approval processes, allowing both the Minister and the IC to have greater confidence that CSIS conducts its activities according to the rule of law.

Transparency in potential use of personal information

Under the CSE Act, the agency has a mandate to provide cybersecurity protection to both federal and designated non-federal systems, such as entities operating in the health and energy sectors. The IC has consistently pressed CSE to explore effective ways to ensure users of these systems are given notice that their personal information could be collected and used for cybersecurity purposes.

In **Decision CSE-2025-03**, the IC noted that CSE has adopted his recommendation to properly notify users of federal systems that their personal information may be collected and used for cybersecurity purposes. CSE revised its own login notice to expressly mention this and recommended that other federal departments and agencies review their notices to provide a similar level of transparency.

While recognizing that CSE cannot compel non-federal entities to provide similarly explicit notices to their users, the IC noted that CSE now recommends that its non-federal clients update their login notices to clearly reflect how personal information can be collected and used for cybersecurity purposes **(Decision CSE-2025-07)**.

> Although it is not possible to exhaustively enumerate the factors to consider in assessing the sensitivity of information related to Canadians (IRtC), I wish to ensure that CSE employees are aware of the sensitivity of information that is related to Canadian fundamental institutions – such as our judicial processes (e.g., deliberative secrecy), democratic institutions (e.g., communication between constituents and their elected representatives), and free press (e.g., protection of journalistic sources). I would encourage CSE to consider explicitly referring to these elements in [their policies] as factors to consider when evaluating the sensitivity of IRtC.
>
> **Decision CSE-2025-08**

Legal issues

In carrying out his quasi-judicial assessment of whether the Minister's or the Director's conclusions are reasonable, the IC considers a range of legal questions. Drawing on his unique vantage point as the reviewer of activities of both CSE and CSIS, the IC used his dual responsibilities in 2025 to foster increased coordination and collaboration between the two agencies, where appropriate. Below are some notable legal issues considered in 2025 decisions.

Impacts on Canadian fundamental institutions

One reason the IC did not approve the proposed new class of acts or omissions in **Decision CSIS-2025-01** was that the Minister's conclusions failed to consider how some of the acts in the proposed class could affect Canadian fundamental institutions.

Canadian fundamental institutions include religious institutions, academia, trade unions, government and political institutions, and the media. The IC has previously emphasized that acts that could impact interests important to Canadians – including Canadian fundamental institutions – must be justified with clear, specific and robust ministerial conclusions. None were present in the record.

The IC considers possible impacts on Canadian fundamental institutions in all his decisions. For example, in **Decision CSE-2025-08**, he encouraged CSE to include these considerations when assessing the sensitivity of information relating to Canadians or persons in Canada incidentally acquired during cybersecurity activities. He further recommended that CSE revise its relevant policies to include explicit reference to the exceptional sensitivity of communications between constituents and their elected representatives, deliberative secrecy of courts and tribunals, and the protection of journalistic sources.

Interpretation of the scope of the prohibition against infringing a Charter right or freedom in the CSIS Act

The record in **Decision CSIS-2025-01** raised a novel interpretation of the important CSIS Act limitation that no act or omission that would infringe a right or freedom guaranteed by the Charter can be justified. Specifically, the record raised for the first time whether this provision could allow for the infringement of a Charter right or freedom, provided it could be justified under section 1 of the Charter, which permits rights to be limited by law if the limit is reasonable and justifiable in a free and democratic society.

The IC found that the Minister did not engage with this issue, and that the record contained insufficient information about it. He stated his expectation that CSIS would not change its existing interpretation, which provides that no Charter rights or freedoms may be infringed, even if that infringement could ultimately be justified.

The IC emphasized the significance of adopting a new legal approach relating to Charter rights, including the potential impact this would have on designated employees and the Canadian public at large. If CSIS wanted to change its legal approach, it would have to present a detailed record accompanied by ministerial conclusions which the IC would then assess.

Common approach to similar legal issues

In **Decision CSE-2025-05**, the IC observed that both the CSE Act and the CSIS Act include "justification" provisions that allow authorized person, in specified circumstances, to commit acts or omissions that would otherwise be contrary to Canadian laws. In this context, the IC noted that a Charter issue relating to a specific group of offences – previously identified in relation to CSIS in **Decision CSIS-2025-01** – would also seem to apply to CSE. The IC stated his expectation that the agencies adopt a common approach to the issue, informed by advice from the Department of Justice. A consistent approach is important to ensure legal certainty and to avoid conflicting interpretations across the two agencies.

Pre-emptively including offences in a class of acts or omissions

Decision CSIS-2025-01 raised another legal issue related to the justification framework: some of the acts the Minister included in the class were offences that were not in force. The Minister did not address this issue in his conclusions.

The IC concluded that the implicit interpretation – that it was within the Minister's jurisdiction to include these offences – was reasonable. The offences were clearly defined and it was reasonably foreseeable that they would become enforceable. Including them ensured that the purpose of the justification framework was fulfilled by avoiding any potential gaps that could delay approval once the offences came into force.

Authorizations during the caretaker period

The year 2025 marked the first time an application was made and an authorization issued while the caretaker convention was in effect during the federal election period. Under the convention, ministers are expected to exercise restraint and defer major policy decisions during the election period, unless certain exceptions – such as the decision being urgent and in the public interest – are met. While it is outside the IC's mandate to assess compliance with the convention, the IC recognized the important role his decisions play in informing the public and made note of the convention in his decisions when relevant.

In **Decision CSIS-2025-02**, CSIS provided a rationale for the Minister of Public Safety issuing the authorization during the caretaker period: determining the class is a routine decision, it is in the public interest, and it is reversible by any future minister. In contrast, CSE did not mention the convention in two applications made during the caretaker period **(Decisions CSE-2025-04 and CSE-2025-05)**.

To strengthen transparency and ministerial accountability, the IC called for future decision makers to ensure that considerations regarding the caretaker convention are fully addressed in their conclusions. This would allow the IC to communicate these considerations to the Canadian public through his decisions.

Ensuring that CSE targets are not Canadian

The CSE Act prohibits CSE from directing its activities at Canadians or persons in Canada. Ensuring compliance with this limit is an ongoing focus for the IC. In past decisions, the IC has raised concerns about the internal threshold CSE uses to determine whether a target is "foreign."

CSE's approach is to apply the threshold of whether there are reasonable grounds to believe the target is not Canadian. In 2025, both CSE and the Minister expanded on their rationale for using this approach, noting that a similar threshold is used by Canadian courts when considering criminal search warrants.

In **Decision CSE-2025-05**, the IC explained that the key issue is not how the threshold is described, but the actual steps taken by CSE to ensure the prohibition is respected. Based on the steps described in the record, the IC concluded that CSE treats the prohibition with the utmost seriousness. Past experience further shows that inadvertent targeting of Canadians or persons in Canada is extremely rare.

While satisfied that CSE's existing approach is reasonable, the IC expressed concern about whether CSE's justification for applying the reasonable grounds to believe standard appropriately reflects the object of that

prohibition against targeting Canadians and persons in Canada. The IC also observed that CSE's approach was developed under the *National Defence Act*. Given the change in wording of the relevant provisions when the CSE Act came into force, the IC noted that the approach should have been subject to a formal review at the time.

CSIS' use of foreign datasets

In 2025, the IC approved the renewal of the retention of two existing foreign datasets **(Decisions CSIS-2025-04 and CSIS-2025-05)**. In both cases, CSIS included information on its use of the datasets during the original authorization period, noting that some of its queries of the datasets generated results relating to Canadians or persons in Canada. As required by law, those results were deleted from the dataset, although CSIS reported that some of the underlying information was retained as part of ongoing investigations, as permitted by the CSIS Act.

The IC asked CSIS for additional details about the specific queries and the potential legal issue he identified, namely CSIS' authority to query a foreign dataset when it believes the query could produce results related to a Canadian. This issue arises in light of the agency's obligation to take reasonable measures to remove Canadian-related information from a dataset.

In making the request, the IC noted that the dataset regime is a tool to assist CSIS in carrying out its duties, and that it is his role to ensure it is used lawfully. He added that if current legislative provisions unduly hamper CSIS' ability to use foreign datasets, the Director should be made aware, in the event legislative amendments are necessary.

In **Decision CSIS-2025-05**, the IC also observed that the low number of queries during the initial five-year authorization period undermined the Director's conclusion that retaining the foreign dataset would likely assist CSIS in fulfilling its duties. While acknowledging the agency's explanation for the low query volume, the IC noted that meeting the threshold for retaining a dataset depends not only on its potential usefulness, but also on having the necessary resources and capacity to use it effectively.

Treatment of privileged information

Examining how CSIS and CSE treat privileged information is an ongoing priority for the IC. How the agencies handle privileged information acquired in the course of their activities has significant implications for the rule of law.

The IC has sought more information on the agencies' reliance on international affairs as a stand-alone exception to override solicitor-client privilege. In **Decision CSE-2025-02**, CSE relied on a Federal Court decision from October 2024 related to CSIS warrants as justification for continuing to include the international affairs exception (*Canadian Security Intelligence Service Act* (CA) (RE), 2024 FC 1689). Because that Federal Court decision was not made public until March 2025, the IC was able to assess its impact only in **Decision CSE-2025-03**. In doing so, he observed that the Court indicated that reliance on an international affairs exception must be addressed on a case-by-case basis and may be subject to additional judicial scrutiny. He emphasized that CSE should bring any relevant future court decisions to his attention.

While the Chief of CSE is already required to inform the Minister and the IC when incidentally acquired solicitor-client privileged information is used, analyzed, retained, or shared – and to date, this has never occurred – the IC encouraged CSE to align its processes more closely with those outlined by the Federal Court. Similarly, in **Decision CSIS-2025-02**, the IC encouraged CSIS to ensure its mandatory process for identifying and removing solicitor-client privileged information from Canadian datasets minimizes any infringements of that privilege.

Transparency and collaboration

Parliamentary committee – Bill C-8

In October 2025, the IC appeared before the House of Commons committee studying Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*.

Building on his 2024 testimony to the Senate on a previous version of the Bill (C-26), the IC expressed general support for the Bill but identified specific provisions that could allow access to information in which there is a reasonable expectation of privacy, without corresponding independent oversight. To address this gap, the IC proposed an annual ministerial authorization establishing a framework for how CSE uses, analyzes, retains, and discloses such information as a mechanism to strengthen oversight and public confidence by ensuring regular, structured accountability.

Online presence

In 2025, the Office of the Intelligence Commissioner (ICO) launched an official LinkedIn account to provide notice of new publications and support the IC's commitment to transparency.

Public and stakeholder engagement

ICO continues to benefit from its engagement with the public, federal partners, civil society, and academics. For example, in the past year, ICO staff hosted a presentation and discussion with colleagues from Canada's National Security and Intelligence Review Agency (NSIRA).

The IC is entitled to receive copies of classified reports prepared by NSIRA as well as the National Security and Intelligence Committee of Parliamentarians that relate to the IC's powers, duties, or functions. In 2025, the IC received parts of four classified reports from NSIRA. All of the IC's decisions are also shared with NSIRA.

The IC attended the 2025 Five Eyes Intelligence Oversight and Review Council (FIORC) meeting, co-leading two conference sessions. A new FIORC Charter was signed, describing the members' willingness to deepen knowledge sharing and to reinforce their shared commitment to transparent and accountable governance.

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.