

File: CSE-2025-04



Office of
the Intelligence
Commissioner

Bureau du
commissaire
au renseignement

P.O. Box / C.P. 1474, Station / Succursale B
Ottawa, Ontario K1P 5P6
613-992-3044 • Fax 613-992-4096

INTELLIGENCE COMMISSIONER
DECISION AND REASONS

IN RELATION TO A FOREIGN INTELLIGENCE AUTHORIZATION
FOR [...]]
PURSUANT TO SUBSECTION 26(1) OF THE
COMMUNICATIONS SECURITY ESTABLISHMENT ACT AND
SECTION 13 OF THE *INTELLIGENCE COMMISSIONER ACT*

MAY 29, 2025

TABLE OF CONTENTS

I.	OVERVIEW	1
II.	CONTEXT	1
III.	STANDARD OF REVIEW	3
IV.	ANALYSIS	4
	A. Updated record.....	5
	B. Are the Minister' s conclusions reasonable (s 34(1), <i>CSE Act</i>)	8
	C. Are the Minister' s conclusions proportionate (s 34(1), <i>CSE Act</i>).....	9
	D. Subsection 34(2) of the <i>CSE Act</i> - Conditions for issuing an authorization	9
	i. <i>Any information acquired under the authorization could not reasonably be acquired by other means and will be retained for no longer than is reasonably necessary (s 34(2)(a))</i>	10
	ii. <i>Any unselected information acquired under the authorization could not reasonably be acquired by other means (s 34(2)(b))</i>	11
	iii. <i>Measures to protect privacy will ensure that information acquired under the authorization identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to international affairs, defence or security (s 34(2)(c))</i>	11
V.	REMARKS	12
	A. Caretaker convention	12
	B. Solicitor-client privilege	13
	C. Retention of metadata	16
	D. [...].....	18
VI.	CONCLUSIONS	188
ANNEX A		

I. OVERVIEW

1. This is a decision reviewing the conclusions of the Minister of National Defence (Minister) in relation to a Foreign Intelligence Authorization for [REDACTED] (Authorization) made pursuant to the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*). The Authorization is a renewal of authorized activities approved by the Intelligence Commissioner in Decision CSE-2024-03 on July 9, 2024, and no new operational authorities are being sought.
2. On April 29, 2025, pursuant to subsection 26(1) of the *CSE Act*, the Minister issued the Authorization and submitted it to the Office of the Intelligence Commissioner (ICO) for my review and approval. Pursuant to the *Intelligence Commissioner Act*, SC 2019, c 13, s 50 (*IC Act*), the Intelligence Commissioner must provide a written decision either 30 days after the day on which the authorization is received, or within any other period agreed to with the Minister (s 20(3)). The Authorization is valid for a period of one year following the Intelligence Commissioner's approval (s 28(1), *CSE Act*).
3. Based on my review and for the reasons that follow, I am satisfied that the Minister's conclusions in relation to activities and classes of activities enumerated at paragraphs 63 and 64 of the Authorization are reasonable.
4. Consequently, pursuant to paragraph 20(1)(a) of the *IC Act*, I approve the Authorization.

II. CONTEXT

5. A detailed legislative context of CSE's collection of foreign intelligence is set out in past Intelligence Commissioner decisions. In summary, CSE may acquire, covertly or otherwise, information from or through the global information infrastructure (GII) – essentially the Internet, computer and telecommunications networks, and associated devices – that provides intelligence about foreign targets located outside of Canada (s 16, *CSE Act*). The information is acquired based on the Government of Canada's (GC) foreign intelligence priorities and for technical or operational reasons that support the foreign intelligence aspect of CSE's mandate.

6. Foreign intelligence constitutes information about the capabilities, intentions or activities of foreign targets in relation to international affairs, defence or security, including cybersecurity (s 2, *CSE Act*). As defined by CSE, a target is a “specific foreign entity whose activities are of interest to the GC (or who has access to information of foreign intelligence interest), such as a foreign individual, state, organization, or terrorist group, located outside Canada, whose activities are believed to be of foreign intelligence interest.”
7. To effectively engage in foreign intelligence activities, CSE may have to contravene certain Canadian laws. It may also incidentally acquire communications and information that infringe on the privacy interests of Canadians (Canadian citizens, permanent residents or corporations formed under Canadian or provincial law) and persons in Canada. To engage in these foreign intelligence activities, CSE must first obtain an authorization issued by the Minister and approved by the Intelligence Commissioner (s 26, *CSE Act*).
8. The authorization sets out the Minister’s conclusions – effectively the reasons – supporting the activities or classes of activities that CSE may carry out. The Minister must, among other conditions, conclude that the proposed activities are necessary (s 33(2), *CSE Act*), reasonable and proportionate, and that measures are in place to protect the privacy of Canadians or persons in Canada (s 34, *CSE Act*). To approve the authorization, the Intelligence Commissioner must be satisfied that the Minister’s conclusions are reasonable (s 13, *IC Act*). It is only then that CSE may carry out the authorized activities. The Minister and the Intelligence Commissioner receive a report on the outcomes of the activities carried out under the authorization within 90 days of the end of its validity period (s 52, *CSE Act*).
9. Even with an authorization, CSE is prohibited from directing its activities at Canadians or persons in Canada and infringing the *Canadian Charter of Rights and Freedoms (Charter)* (s 22(1), *CSE Act*). However, CSE may incidentally acquire information relating to Canadians or persons in Canada (s 23(4), *CSE Act*). Incidentally means that the information was not deliberately sought and the information acquisition activity was not directed at Canadians or persons in Canada (s 23(5), *CSE Act*). To use, analyse, retain or disclose this information, CSE is statutorily required to have measures in place to protect the privacy of Canadians and of persons in Canada (s 24, *CSE Act*).

10. In accordance with section 23 of the *IC Act*, the Minister confirmed in his cover letter that he provided me with all the information that was before him when issuing the Authorization.

The record is therefore composed of:

- a) The Authorization dated April 29, 2025;
- b) Briefing Note from the Chief of CSE (Chief) to the Minister dated April 4, 2025;
- c) The Chief of CSE's Application dated April 4, 2025, including eight annexes:
 - i) Ministerial Directive – Government of Canada Intelligence Priorities for 2023-2025;
 - ii) National SIGINT Priorities List, February 2025;
 - iii) Outcomes Report for 2024;
 - iv) SIGINT Operations Risk Acceptance Form (SORAF);
 - v) Mission Policy Suite – Foreign Intelligence approved on August 17, 2023 (MPS FI);
 - vi) [...] – *Bykovets* and Foreign Intelligence Activities;
 - vii) Ministerial Order – Designations for the purpose of section 43, *CSE Act*; and
 - viii) Summary of CSE's Measures to Protect the Privacy of Canadians;
- d) Briefing Deck – Overview of the Activities; and
- e) Responses to the Intelligence Commissioner's Remarks.

III. STANDARD OF REVIEW

11. The *IC Act* requires the Intelligence Commissioner to review whether the Minister's conclusions are reasonable. I will therefore apply the reasonableness standard, as applied in judicial reviews of administrative action.

12. As indicated by the Supreme Court of Canada, when conducting a reasonableness review, a reviewing court is to start its analysis by examining the reasons of the administrative decision maker. In *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, at paragraph 99, the Court succinctly describes what constitutes a reasonable decision:

A reviewing court must develop an understanding of the decision maker's reasoning process in order to determine whether the decision as a whole is reasonable. To make this determination, the reviewing court asks whether the decision bears the hallmarks of reasonableness – justification, transparency and intelligibility – and whether it is justified in relation to the relevant factual and legal constraints that bear on the decision.

13. Relevant factual and legal constraints can include the governing statutory scheme and the impact of the decision. The governing statutory scheme set out in the *IC* and *CSE Acts* highlights the role of the Intelligence Commissioner as an independent mechanism to ensure that government action taken for the purpose of national security and intelligence is properly balanced with the respect of the rule of law and the rights and interest of Canadians.
14. When the Intelligence Commissioner is satisfied (*convaincu* in French) that the Minister's conclusions at issue are reasonable, he "must approve" the authorization (s 20(1)(a), *IC Act*). Conversely, where unreasonable, the Intelligence Commissioner "must not approve" the authorization (s 20(1)(b), *IC Act*). In both cases the Intelligence Commissioner must set out his reasons for doing so.

IV. ANALYSIS

15. On April 4, 2025, the Chief submitted a written Application for a Foreign Intelligence Authorization for [...] (Application) to the Minister. The Application sets out the foreign intelligence activities that could be conducted by CSE to covertly collect information on or through the GII. It also describes how the Chief proposes that CSE will analyse, process and retain the information and the measures in place to protect the privacy of Canadians and of persons in Canada, in cases where it incidentally acquires information about them.
16. These activities could contravene Canadian laws or interfere with the reasonable expectation of privacy of Canadians or persons in Canada and their description can be found in the classified annex to this decision (Annex A). The annex renders the eventual public version of this decision easier to read and ensures that the decision contains the nature of the facts that were before me, which otherwise would only be available in the record.

17. Based on the facts presented in the Application submitted by the Chief, the Minister concluded on reasonable grounds that the Authorization is necessary and that the conditions of subsections 34(1) and (2) were met. Consequently, the Minister issued a one-year authorization for CSE to carry out the activities set out at paragraphs 63 and 64 of the Authorization.
18. The activities are the same as those approved in last year's authorization. They are again divided in three classes and involve similar approaches to accessing information as well as similar legal, policy, reputational, partnership, and operational risks. The activities may also result in similar contraventions of Acts of Parliament and interferences with privacy interests.

A. Updated record

19. Past approvals of the activities do not entail that they will automatically be approved again. Every ministerial authorization is distinct and is reviewed on its own record.
20. I am satisfied the record contains new information that addresses remarks I made in last's year decision as well as other previous decisions in relation to foreign intelligence authorizations. CSE has also provided updated operational information to ensure the Minister is presented with current information to evaluate the effects of the activities. I also note that the 2023 MPS FI is currently being revised and I expect it to include amendments in relation to CSE's measures to protect the privacy of Canadians. I am looking forward to this new version, as the MPS is a critical tool for guiding the conduct of CSE employees, as well as an important element in the Minister and the Intelligence Commissioner's analysis to understand how proposed activities will be conducted.
21. In last year's decision with respect to these activities, I remarked that the record would benefit from tangible examples of how privacy interests are taken into account during the internal risk assessment process leading to the approval of an activity. The new example found in the Application is helpful in showing how operational plans and risk assessments identify potential privacy risks to Canadians and persons in Canada and the associated mitigation measures. I reiterate that examples like these are helpful to the Minister as well as to me to better understand the concrete effects of activities.

22. In the same manner, section 17.2 of the MPS FI states that to meet the requirements of the *CSE Act*, analysts must, upon recognition, assess the essentiality of incidentally acquired communications with recognized information relating to Canadians or persons in Canada (IRtC) with respect to international affairs, defence or security and apply corresponding privacy annotations. The recognition of IRtC is typically conducted through human inspection (“eyes on”), but may also be done using automated means, where feasible. I remain of the view that to strengthen the oversight roles played by the Minister and myself, the record should provide tangible examples – similar to the one provided for operational plans and risk assessments – to show how an analyst assesses whether IRtC is essential to international affairs, defence or security, and the resulting rationale they prepare. Substantially documenting such important decisions is imperative to ensure that the established policies and procedures are strictly followed. The Minister and I need such information to fulfil our respective roles.
23. In Decision CSE-2023-04, I made a remark to the effect that to carry out the proposed foreign intelligence activities, CSE applies the standard of “reasonable grounds to believe” that a target is not a Canadian or a person in Canada, and noted that a higher legal threshold may be more appropriate given the legislative prohibition against CSE targeting Canadians or persons in Canada. In Decision CSE-2024-04, I noted that the Minister’s conclusions should address the issue. This issue is addressed in the Application and the Minister’s conclusions. I also note that [...] on the topic was provided with the authorization in CSE-2025-05, which was received by ICO on the same day as this Authorization. In sum, the Minister essentially supports the threshold by analogy: the reasonable grounds to believe threshold is the common standard in the *Criminal Code* and most federal enactments authorizing search warrants, where privacy and *Charter* rights are engaged. It is therefore sensible, according to the Minister, that the same threshold may be relied upon where the actions of the state risks the inadvertent – as opposed to deliberate in the context of search warrants – intrusion of these rights.
24. I expand more at length in Decision CSE-2025-05, but when conducting the reasonableness review as required, I find the Minister’s rationale supporting the standard reasonable. In my view, determining an appropriate threshold is a useful illustration of the importance for the

Minister and myself to understand the concrete results of past authorizations. The inadvertent targeting of Canadians is extremely rare, which supports the reasonableness of the Minister's conclusions related to the use of the "reasonable grounds to believe" threshold. Frequent inadvertent targeting of Canadians could raise questions about whether the threshold was appropriate, or whether the threshold was being properly applied. Indeed, in practice, the legal threshold may be less important than the effectiveness of the actual process used by CSE to ensure that it does not target Canadians.

25. In my most recent foreign intelligence decision (CSE-2025-02) I made a remark in relation to the conditional language used by the Minister and the Chief when describing the incidental acquisition of IRtC, which can occur despite the target being foreign. I was of the view that the language used could be better contextualized to reflect CSE's operational reality, which is that the activities in that authorization would almost certainly result in the incidental acquisition of IRtC. This remark is also partially addressed in this matter. In the Application, the Chief makes it clear that "[g]iven that incidental acquisition does occur, CSE ensures that it has measures in place to protect the privacy of Canadians and persons in Canada". Further, while CSE activities are not directed at Canadians or persons in Canada, these activities "will result in the incidental acquisition of information that is later identified as relating to a Canadian or person in Canada." However, I note that the Minister's conclusions have not been updated to reflect these changes, despite the summary of changes in Briefing Deck to the Minister indicating they have been.
26. As set out in section 13 of the *IC Act*, I must review whether the Minister's conclusions on the basis of which the authorization was issued under subsection 26(1) of the *CSE Act*, are reasonable.
27. In addition to finding that a foreign intelligence authorization is necessary, the Minister must conclude that "there are reasonable grounds to believe that any activity (*activité en cause* in French) that would be authorized by it is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities" (s 34(1), *CSE Act*). The Minister must arrive at his conclusions by applying his understanding of what those

thresholds entail. Determining whether an activity is reasonable and proportionate is a contextual exercise and the Minister may consider a number of factors.

28. Given that the Authorization constitutes a renewal, and the Minister's conclusions – subject to the updates noted above – have not substantially changed, my reasons highlight what I consider are the central elements of the Minister's analysis.

B. Are the Minister's conclusions reasonable (s 34(1), *CSE Act*)

29. The Minister concluded that he had reasonable grounds to believe that the activities are reasonable “given the objective of acquiring information from the GII for the purpose of providing foreign intelligence”.
30. In support of his conclusion, the Minister explains that the activities – described in Annex A – enable CSE to acquire information of foreign intelligence interest that would otherwise be inaccessible to it. Indeed, the Chief indicates in her Briefing Note that these activities are [...]. The activities carried out under the previous authorization enabled the production of a wide-range of reports to fulfil the GC's intelligence priorities.
31. Relying once again on the Chief's explanation that “these activities represent a fair, sound, logical, and well-founded means to achieve the objective of acquiring information from the GII”, the Minister also concluded that he had reasonable grounds to believe that the activities are necessary and reasonable for foreign intelligence collection.
32. I find the Minister's conclusions reasonable. He understood the nature of the activities and explained how they are necessary. There is a rational connection between the activities and the objective of collecting foreign intelligence from or through the GII for the purpose of providing intelligence to the GC based on its intelligence priorities. Indeed, the Outcomes Report shows how effective the same activities have been in the past. The classes of activities are also sufficiently specific for CSE employees to understand the activities that they may lawfully carry out.

C. Are the Minister's conclusions proportionate (s 34(1), *CSE Act*)

33. The Minister also concluded that he had reasonable grounds to believe the activities authorized are proportionate given the nature of the activities and the manner in which they are conducted. Indeed the activities “are subject to measures and controls that limit CSE’s acquisition of information to that which is relevant to the fulfillment of its foreign intelligence mandate.”
34. The measures and controls in place include the MPS FI, the internal compliance program, the measures specified in the Authorization and CSE policies, and the need for CSE to obtain an operational plan and risk assessment for all activities, regardless of duration. As the activities are directed at specific foreign targets, both the total volume of information collected, as well as the possibility of collecting information that is Canadian-related, is lower than if the targets were broader.
35. I am satisfied that the Minister conducted a balancing exercise taking into account the objective and nature of the activities. He was aware of the privacy interests at issue and laid out the measures in place to protect them, showing that the proposed activities justify any potential impairment of Canadian privacy interests.
36. The balancing was also applied by the Minister to the rule of law when he considered the effects of CSE’s activities and the potential of contravening Acts of Parliament described in the record. For these reasons, I am satisfied that the activities are proportionate.

D. Subsection 34(2) of the *CSE Act* – Conditions for issuing an authorization

37. In addition to finding the activities reasonable and proportionate, the Minister may issue an authorization for foreign intelligence activities only if he also concludes that there are reasonable grounds to believe that the conditions set out at subsection 34(2) of the *CSE Act* are met, namely:
- a) any information acquired under the authorization could not reasonably be acquired by other means and will be retained for no longer than is reasonably necessary;

- b) any unselected information acquired under the authorization could not reasonably be acquired by other means, in the case of an authorization that authorizes the acquisition of unselected information; and
- c) the measures referred to in section 24 will ensure that information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed, or retained only if the information is essential to international affairs, defence or security.

i. Any information acquired under the authorization could not reasonably be acquired by other means and will be retained for no longer than is reasonably necessary (s 34(2)(a))

38. I am satisfied that any information acquired under the Authorization could not reasonably be acquired by other means. Indeed, in his conclusions, the Minister provides a description of the information that is acquired through the activities, which require a high level of technical capabilities and expertise. It is clear that due to the [...] the proposed activities would allow CSE to acquire information that most likely would not otherwise be accessible by other means.

39. I am also satisfied that any information acquired under the Authorization will be retained for no longer than is reasonably necessary. In his conclusions, the Minister establishes a connection between the types of information and their retention period and explains why the different retention periods are reasonably necessary for operational reasons. Namely, the information is retained pursuant to the retention schedule found in the MPS FI, which incorporates minimum retention periods set out in the *Privacy Act*, RCS, 1985, c P-21, and the *Library and Archives of Canada Act*, SC 2004, c 11. For operational reasons, information may be deleted earlier than the maximum retention period. However, in some cases there are technical and operational reasons for the retention of certain types of information for a longer period, even indefinitely. Finally, information assessed for the purposes of foreign intelligence is subject to limited access by CSE employees authorized to operate under that aspect of the mandate.

40. For these reasons, I find that the Minister's conclusions in relation to the acquisition and retention of any information acquired and retained under the Authorization are reasonable.

ii. *Any unselected information acquired under the authorization could not reasonably be acquired by other means (s 34(2)(b))*

41. Pursuant to the *CSE Act* unselected information is information that is acquired, for technical or operational reasons, without the use of terms or criteria to identify information of foreign intelligence interest (section 2). Unselected information could include information that interferes with the reasonable expectation of privacy of Canadians or persons in Canada, which would only be retained if determined to be essential, as set out in the next section.

42. As explained by the Minister, the value of some of the activities depends on the ability for CSE to acquire unselected information, which CSE could not collect without conducting the activities set out in the Authorization. Once acquired, CSE may apply selection criteria in order to select any information that may be of foreign intelligence interest.

43. For these reasons, I am satisfied that the Minister has reasonable grounds to believe that unselected information could not reasonably be acquired by other means with respect to activities set out in the Authorization.

iii. *Measures to protect privacy will ensure that information acquired under the authorization identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to international affairs, defence or security (s 34(2)(c))*

44. Section 24 of the *CSE Act* requires CSE to have measures in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of information related to them acquired in the course of activities further to the foreign intelligence aspect of its mandate.

45. The Minister concludes that he has reasonable grounds to believe that the measures referred to in section 24 have been met. Indeed, one of the measures set out at section 17 of the MPS FI stipulates that information relating to a Canadian or a person in Canada can only be used, analysed or retained if it is assessed as essential to international affairs, defence or security interests, including cybersecurity. As I have found in past decisions, I am satisfied that CSE's definition of "essential" is reasonable. In last year's decision, I remarked that given the importance of the essentiality criterion in relation to the use of

information related to Canadians or persons in Canada, in addition to the Chief, the Minister should also articulate his rationale respecting the definition of “essential”. I note that the Minister’s conclusions now include the definition of essential, but did not add a rationale addressing how the definition is reasonable.

46. Further, the Minister’s conclusions indicate that on a quarterly basis, operational managers “must review” the retained information and revalidate whether it is still essential. Information that is no longer essential must be deleted.
47. Other measures referred to by the Minister include CSE’s compliance program, which is described as being responsible for conducting monitoring activities that help to verify that operations comply with the MPS FI as well as the conditions of the authorization under which they are carried out. Also, information that is deemed essential is stored in repositories controlled and limited to employees who are properly accredited and trained to conduct foreign intelligence activities.
48. Given the multiple layers of internal controls to protect the privacy interests of Canadians and limit access to unassessed information, I am satisfied that the Minister’s conclusions are reasonable and that IRtC will only be retained, analysed and used if it is essential to international affairs, defence or security, including cybersecurity.

V. REMARKS

49. I would like to make three additional remarks to assist in the drafting and consideration of future of ministerial authorizations, which do not alter my findings regarding the reasonableness of the Minister’s conclusions.

A. Caretaker convention

50. According to the ICO’s records, the present file is the first in which CSE has made an Application to the Minister during the caretaker period. According to the Privy Council Office’s *Guidelines on the conduct of Ministers, Ministers of State, exempt staff and public servants during an election* (PCO Guidelines), the caretaker period begins upon the dissolution of Parliament and ends either when a new government is sworn-in or when an

election result returning an incumbent government is clear. The caretaker period was therefore most recently in effect from March 23 to April 29, 2025.

51. Pursuant to the PCO Guidelines, during the caretaker period Ministers must restrict themselves to matters that are routine, or non-controversial, or urgent and in the public interest, or reversible by a new government without undue cost or disruption, or agreed to by opposition parties (in those cases where consultation is appropriate).
52. Although no reference to the caretaker period or convention appears in the Application or the Authorization, the Minister – given his role and responsibilities – was certainly aware of the applicability of the caretaker convention. The Chief’s Application, made during the caretaker period (on April 4), requested the Minister’s decision at his “earliest convenience” in order to evenly distribute ministerial authorizations over the year. The Minister ultimately issued the Authorization on April 29, the day that the caretaker period ended.
53. As I noted in Decision CSIS-2025-02, as a quasi-judicial decision maker, my role is not to consider whether the caretaker convention has been respected or not; as a convention, it is not enforced judicially. Nevertheless, given that the decisions of the Intelligence Commissioner are an important source of information through which the public can become aware of ministerial authorizations, I am of the view that it is important to raise the issue in this decision.
54. To strengthen transparency and ministerial accountability, I would encourage applications made during caretaker periods in the future to provide responsible Ministers with considerations regarding the applicability of the caretaker convention. This would assist the Minister in making the determination of whether issuing the authorization falls within the types of decisions that can be made during the caretaker period, in particular where new or novel authorities are sought. Further, the ministerial conclusions could be reflected in publicly released decisions of the Intelligence Commissioner.

B. Solicitor-client privilege

55. CSE has made considerable efforts to address concerns I have raised in past remarks relating to solicitor-client privilege. These remarks have raised three main elements. The first is the question of whether jurisprudence allows for the piercing of solicitor-client privilege for reasons of international affairs (as a distinct ground separate from national security). The second is whether the Minister is the appropriate person to render decisions on whether CSE can use, analyse, retain or disclose solicitor-client communications it has acquired. The third element is that any resulting process should ensure that access to the potentially privileged information is as restricted as possible.
56. In Decision CSE-2025-02, I noted that CSE had indicated that it will continue to include an international affairs exception on the basis that the recent Federal Court decision, *Canadian Security Intelligence Service Act (CA) (Re)* 2024 FC 1689, leaves the door open to such an exception for CSIS. The Federal Court decision had not been included in that record and as its public version was not yet available, I could not comment on its impact. CSE provided my office with a redacted copy following my decision and it has since been publicly released, with the same redactions. Following my review of the Federal Court's decision, I wish to highlight that the Court holds that the question of the exception is one to be addressed by judges on a case-by-case basis and that "judges may be more rigorous in probing the justification where CSIS relies on the information as necessary to assist in the conduct of foreign affairs as opposed to the investigation of a threat to the security of Canada" (at para 100). I therefore underscore the importance of CSE's stated commitment to "continue to monitor future relevant decisions from the Court"; any such decisions should be brought to my attention and also assessed by CSE for any impact on its inclusion of an international affairs exception.
57. The Federal Court's decision also prompts me to expand on the second and third elements of my remarks relating to solicitor-client privilege. While in Decision CSE-2024-01 I expressed satisfaction that CSE's explanation of its process for handling incidentally intercepted solicitor-client communications minimized the number of individuals who may have access to these communications, the Court's decision offers a reminder for CSE to ensure that its process restricts this access as much as possible.

58. The Court, reiterating many of the same principles from *Re Unnamed person*, 2020 FC 1190, emphasizes the importance of limiting access to potentially privileged communications. The Court finds that a maximum of two CSIS employees should have access to the content of the communications when determining whether an application should be made to the Court to seek authorization to retain and use the information. The Court also notes that although counsel for the Attorney General of Canada may make submissions to the Court with respect to privilege, they should not have access to the contents of the communication (at paras 24 and 139).
59. As described in the Authorization, “upon recognition”, CSE restricts access on a “need-to-know basis”. CSE’s process also envisions Department of Justice counsel being consulted to determine whether the communication is in fact subject to solicitor-client privilege, which without further clarification suggests counsel could have access to the contents of the communications.
60. I reiterate that inadvertently collecting privileged communication is extremely rare and note no instance the Minister approving a request to retain any such communication has been reported to me, as would be required. Although CSE’s process minimizes access to potentially privileged communications, given the rare occurrence, CSE may want to consider delineating its process with more definitive terms. In any event, CSE should account for the need to minimize the intrusion as part of its overall consideration of the process used to evaluate whether a communication is privileged, as well as the process to determine whether CSE can use, analyse, disclosure or retain the communication.
61. Noting that the Federal Court’s decision indicated that further clarification may be needed with respect to how CSIS assesses whether a communication is privileged, I would encourage cooperation between CSE and CSIS to ensure that CSE’s procedure reflects the final conditions approved by the Federal Court. While the two agencies’ legislative schemes are different, I am of the view that the underlying principles relating to privileged communications are equally applicable to CSE and that there is a valuable opportunity for it to benefit from the specific guidance the Federal Court has given CSIS.

C. Retention of metadata

62. From my first decision pertaining to a foreign intelligence authorization (CSE-2023-01) onwards, I have sought further information regarding the retention period for metadata. My original remark on this topic had two main components. The first requested additional details regarding the rationale for the specific retention period for metadata. The second sought clarification of how metadata is reviewed and assessed, particularly in situations where initial query results are deleted but the underlying metadata is not, and is instead returned to the metadata repository. In last year's decision (CSE-2024-03), I added that in relation to this second component, addressing *R v Bykovets*, 2024 SCC 6 [*Bykovets*], would be important, given that the Court recognized an elevated privacy interest in an IP address, which CSE classifies as metadata.
63. The record before me contains [...] which addresses the operational implications of *Bykovets* on CSE's retention of metadata, as well as elements of both of my remarks. [...] includes additional helpful background on the broad categories of metadata records that CSE acquires. It also contains some new information regarding steps CSE takes to reduce the likelihood of acquiring information related to Canadians; for example, [...]. Indeed, future applications and authorizations would benefit from incorporating some of this information.
64. [...] concludes that while applicable to CSE's acquisition, retention and use of metadata, the impact of *Bykovets* on them is "negligible." This is largely owing to the overall scheme of the *CSE Act* which requires that the activities must be authorized by the Minister, and approved by the Intelligence Commissioner. More relevant to my remarks, [...] explains that CSE has long recognized that its metadata acquisition program has the potential to interfere with the reasonable expectation of privacy of Canadians and persons in Canada. However, CSE applies privacy protection measures to every type of metadata independently of the nature of the privacy interest that may be engaged, and these safeguards ensure that CSE's activities are reasonable and proportionate. As a result, for CSE, a judicial decision finding a higher privacy interest in a type of metadata – to the extent that the context was applicable to CSE's operations – does not affect its internal processes that are already sufficient to account for these interests.

65. With respect to retention of metadata, [...] explains more clearly that the [...] retention period represents the time period that CSE reasonably believes the metadata remains operationally useful as a source of foreign intelligence. A higher privacy interest, given CSE's existing protection measures, does not affect CSE's assessment of what constitutes a reasonable retention period for metadata.
66. As for the second component of my remark in relation to the assessment of Canadian-related metadata, [...] clarifies the process to determine whether metadata contains IRtC. This is also now reflected in the Minister's conclusions. In essence, retained metadata is queried for a variety of purposes and queries return a number of results. What is now clear is that a CSE analyst will only assess whether metadata contains IRtC – and whether that IRtC is essential – if the metadata record resulting from the query is considered to be operationally useful. I understand this to mean that only if CSE wishes to actually use the metadata will an assessment with respect to IRtC be made. If a query result is determined to be operationally useful and contains IRtC, an essentiality assessment is made. If the information is assessed as not essential to international affairs, defence, or security interests, including cybersecurity, the metadata is deleted.
67. The much improved explanation is appreciated and highlights the importance of clarity, especially in relation to technical aspects of an authorization. Indeed, I note that past records explained that where the results of a query were “not deemed as essential”, the underlying metadata was not deleted, “as there remains a possibility that this information could be deemed at a later date to be essential to satisfy other foreign intelligence purposes.” This rationale for retaining metadata containing IRtC has been eliminated from the record. Rather, the clarified rationale explaining why metadata records containing IRtC are not deleted is because they have effectively not been assessed.
68. While I do not take the change in language to mean that CSE's practice has changed, applications to the Minister should seek to describe CSE's activities in a way that is unambiguous. Indeed, Intelligence Commissioner decisions have found that where the conclusions do not exhibit a clear understanding of the activities, they may not be reasonable.

69. As a whole, I find [...] helpful and underscore the importance of records accompanying a ministerial authorization reflecting the impact of changes in relevant case law or legislation. In my view, CSE's exercise of responding to my remarks with respect to metadata has brought increased clarity to the ministerial conclusions on a number of issues.

D. [...]

70. [This and the following paragraph highlight a discrepancy found in the record in relation to the described scope of an activity. The Intelligence Commissioner suggests that future records should, for the benefit of the Minister, be updated to better describe the scope of the activity.]

71. [...]

VI. CONCLUSIONS

72. Based on my review of the record, I am satisfied that the Minister's conclusions made under subsections 34(1) and (2) of the *CSE Act* in relation to activities and classes of activities enumerated at paragraphs 63 and 64 of the Authorization are reasonable.

73. I therefore approve the Authorization pursuant to paragraph 20(1)(a) of the *IC Act*.

74. As indicated by the Minister, and pursuant to subsection 36(1) of the *CSE Act*, this Authorization expires one year from the day of my approval.

75. As prescribed in section 21 of the *IC Act*, a copy of this decision will be provided to the National Security and Intelligence Review Agency for the purpose of assisting the Agency in fulfilling its mandate under paragraphs 8(1)(a) to (c) of the *National Security and Intelligence Review Agency Act*, SC 2019, c 13, s 2.

May 29, 2025

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner