~~TOP SECRET//SI//LIMITED/CEO~~

File: CSE-2025-09

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 CYBERSECURITY AUTHORIZATION FOR ACTIVITIES ON NON-FEDERAL INFRASTRUCTURES PURSUANT TO SUBSECTION 27(2) OF THE *COMMUNICATIONS SECURITY ESTABLISHMENT ACT* AND SECTION 14 OF THE *INTELLIGENCE COMMISSIONER ACT*

[...]

Canada

TABLE OF CONTENTS

I. OVERVIEW

1. This is a decision reviewing the Minister of National Defence's (Minister) conclusions authorizing the Communications Security Establishment (CSE) to help protect electronic information and infrastructures (i.e., computer systems, devices and networks) belonging to a non-federal entity – [...] (Authorization).

2. The Authorization sets out activities identical to those I approved in relation to the same non-federal entity on [...] (Decision CSE-2025-01).

3. On [...], pursuant to subsection 27(2) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*), the Minister issued the Authorization. On [...], it was received by the Office of the Intelligence Commissioner for my review and approval under the *Intelligence Commissioner Act*, SC 2019, c 13, s 50 (*IC Act*).

4. For the reasons that follow, I am satisfied that the Minister's conclusions made under subsections 34(1) and (3) of the *CSE Act* in relation to the activities and classes of activities enumerated at paragraph 81 of the Authorization are reasonable. Consequently, pursuant to paragraph 20(1)(a) of the IC Act, I approve the Authorization.

II. CONTEXT

5. As part of the cybersecurity aspect of its mandate, CSE carries out cyber protection activities to help protect certain electronic systems, devices, networks and the information they contain from criminal and state-sponsored cyber threats. CSE also provides advice and guidance to strengthen the cybersecurity posture of these systems (s 17, *CSE Act*).

6. Pursuant to the *CSE Act*, CSE is required to obtain a ministerial authorization for any activities under the cybersecurity aspect of its mandate that would contravene any federal laws or involve the acquisition by CSE of information that interferes with the reasonable expectation of privacy of Canadians (Canadian citizens, permanent residents, or corporations formed under Canadian or provincial law), and persons in Canada (ss 22(4), 27, *CSE Act*). In order to effectively carry out cybersecurity activities, CSE acquires such information.

7. The *CSE Act* establishes two distinct types of ministerial authorizations for cybersecurity activities: those issued in relation to federal systems (s 27(1)), and those issued in relation to non-federal systems that have been designated as important to the Government of Canada – non-federal systems (s 27(2)) – for example those related to the health, energy and telecommunications sectors.

8. Authorizations relating to non-federal systems must meet two requirements. First, the systems must have been designated in a ministerial order as being of importance to the Government of Canada (s 21, *CSE Act*). The *Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada* (SOI Order) issued on August 25, 2020, sets out broad classes of designated systems, one of which encompasses the non-federal entity. Second, the authorization process must be initiated by the owner or operator of the non-federal system making a written request to CSE to carry out the activities that would be authorized (s 33(3), *CSE Act*). The record includes the written request from the non-federal entity for CSE's support in conducting cybersecurity activities.

9. The authorization sets out the Minister's conclusions – effectively the reasons – supporting the activities or classes of activities that CSE may carry out. The authorization is valid for up to one year if approved by the Intelligence Commissioner (s 36, *CSE Act*).

10. Despite an authorization, the *CSE Act* imposes limits on CSE's cybersecurity activities. CSE is prohibited from directing its cybersecurity activities at Canadians or persons in Canada and from 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 acquired was not itself deliberately sought (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*).

11. In accordance with section 23 of the *IC Act*, the Minister confirmed in his cover letter that he provided me with all information that was before him when issuing the Authorization. The record is therefore composed of:

    a) The Authorization;
    b) The Chief of CSE's Application to the Minister (Application) dated [redacted], containing the following annexes:
        i. The letter of request from the non-federal entity;
        ii. Four ministerial orders;
        iii. Outcomes Report for 2025;
        iv. Six Cyber Centre overview/threat assessments;
        v. Mission Policy Suite – Cybersecurity (MPS) approved November 2025; and
        vi. Record of Changes to the MPS;
    c) Responses to Intelligence Commissioner's Remarks;
    d) The Chief's Briefing Note to the Minister (Briefing Note); and
    e) Briefing Deck – Overview of the Activities.

III. STANDARD OF REVIEW

12. 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.

13. 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 [*Vavilov*], 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.

14. 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 interests of Canadians.

15. 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 not satisfied the conclusions are reasonable, 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

16. The Minister issued the Authorization with a one-year validity period, subject to my approval. A description of the non-federal entity as well as the cybersecurity activities set out in the Authorization can be found in the classified annex to this decision (Annex A). The annex renders the eventual public version of the 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.

A. Updated record

17. The record includes responses to the remarks I made in Decision CSE-2025-01 in relation to the same non-federal entity, as well as those found in subsequent decisions relating to other cybersecurity authorizations. I am pleased with the prompt and thorough responses provided by CSE to address the issues raised in my remarks and I am of the view that the ongoing oversight process established is working effectively.

i. Letters of request

18. The first of these remarks raised a theme I returned to in several cybersecurity decisions rendered in 2025, namely the content of the letter of request from the system owner. Key aspects of my remarks have been addressed by including express confirmation of the non-

federal entity's legal authority to acquire information and to share it with CSE for cybersecurity purposes. The letter also reflects that it constitutes a renewal of existing cybersecurity activities by requesting their continuation.

19. Additionally, further to my remark that it would be useful for the application to give an overview of measures the non-federal entity is taking to provide notice to, and obtain consent from, the users of its system, the record indicates that the non-federal entity has provided CSE with an overview of its acceptable use policy and that it makes employees aware that the non-federal entity conducts cybersecurity monitoring. As indicated in Decision CSE-2025-08 (para 23), CSE commits to continue to provide recommended language for use in login notices by its non-federal clients.

20. Another remark linked to the letters of request made in last year's decision is the language used in relation to the obfuscation of personal and proprietary information prior to disclosure. I was of the view that there was a lack of clarity with respect to whether the non-federal entity has a clear understanding of CSE's privacy protection measures set out in the MPS. The current letter of request clarifies when the obfuscation of information is required: when sharing cybersecurity reports outside of CSE to recipients other than the system or information owner, CSE only shares threat information, such as […] of observed suspicious activity. Information such as details about the victim's name, the department or entity name, is obfuscated.

ii. MPS update – November 2025

21. The updated MPS included in the record rectifies an inconsistency between provisions in authorizations providing that operational managers "must review" recognized retained information relating to a Canadian (IRtC) on a quarterly basis and previous MPS versions stating that they are simply "reminded to review". Another important addition to the MPS that does not apply to this Authorization, but to other authorizations related to non-federal entities I have approved, is that CSE will notify the Minister and subsequently myself when it accepts a new request from a non-federal entity to expand cybersecurity activities to additional sub-entities that use its information infrastructures, provided those sub-entities were listed in the original authorization.

22. One main outstanding point relates to my encouraging CSE to consider elaborating its approach to determining the level of sensitivity of IRtC to explicitly refer to the sensitivity of information that is related to Canadian fundamental institutions. I appreciate that CSE is conducting further analysis and consultation regarding this point made in my most recent decision (CSE-2025-08).

iii. Additional updates

23. In Decision CSE-2025-08, my reasons underscored that the *CSE Act* sets out different specific requirements for cybersecurity authorizations for federal systems and for non-federal systems. More specifically, the primary objective of an authorization should not combine the protection of both types of systems, and evaluating whether information is "necessary" and "essential" should reflect the type of authorization that the Minister has issued. The current Application and Authorization properly reflect this delineation.

24. The record also provides an update related to the interception of solicitor-client communications. I note that the new wording contained in the condition governing the retention of solicitor-client communications has narrowed its scope. Only solicitor-client communications found essential to identifying, isolating, preventing or mitigating harm to the non-federal entity's electronic information and information infrastructure listed in the Authorization may be retained by the Chief and referred to the Minister for decision. Contrary to past authorizations, reference is no longer made to all other federal systems and systems of importance. I welcome this additional restriction which addresses concerns I have raised in past remarks relating to solicitor-client privilege. I note for clarity that no instance of the Chief deciding to retain solicitor-client communications has been reported to me to date. I also note that I am still awaiting the result of CSE's work in relation to whether it is appropriate for the Minister to be the decider of whether privileged communications should be retained.

25. My remark regarding the inclusion of ministerial orders designating systems of importance has been addressed by including two additional orders from 2022 respectively designating the electronic information or information infrastructures of the Government of Ukraine and the Government of Latvia as systems of importance. Importantly, this gives the Minister a complete

picture of how IRtC could potentially be shared. For clarity, I note that it is indicated no IRtC was shared with either government during the course of the existing authorization.

26. Finally, in addition to being updated to address specific remarks or issues I have raised, it remains essential that the record always present the Minister and I with the most accurate information. The following are examples where an update would have been required:

    a) The Application indicates that the non-federal entity has procured a commercial cybersecurity product to conduct vulnerability scanning, but the Briefing Note continues to state the non-federal entity lacks the capability. The Briefing Note also still refers to upcoming events […] that have already occurred.

    b) The Application refers to […] from the first quarter of 2024 and a predicted trend for the end of 2024. An update could have been provided to reflect the latest available data and/or reflect whether the predicted trend was realized.

    c) The Outcomes Report contains less information than is usually included. Namely, no information is provided on the date(s) that CSE's cybersecurity solutions were deployed. Since the initial authorization was issued and approved on an expedited basis given the circumstances, I suggest inclusion of this information in the end of authorization report prepared pursuant to section 52 of the *CSE Act* to reflect the status of the deployment from the beginning of the authorization until the end.

    d) The wording used to describe the scope of information acquired though a particular cybersecurity solution – […] – has been modified from the initial authorization. Whereas the original stated that the solution accesses […] (i.e., the non-federal entity), the current Application indicates that "the only […] that will be accessed by CSE are those containing predefined security and usage telemetry made accessible by the client" (emphasis added). This seems to have narrowed the […] accessed by CSE, yet the remaining description of the cybersecurity solution remains the same and indicates that CSE will acquire […]. I would therefore appreciate future applications to add clarification as to the scope of information accessed through the

[…] cybersecurity solution. It would also be useful for the Minister and myself if the record indicated whether the non-federal entity has chosen to deploy a certain approved capability […]. I note that this capability has the potential to expand the scope of the ty types of information that CSE would collect.

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

27. The Minister once again issued the Authorization on a proactive basis; there is no known compromise or specific threat to the non-federal entity. Nevertheless, the Minister establishes a factual basis for CSE's support. Indeed, the record describes existing cyber threat actors in great detail, and provides information related to the likelihood of the non-federal entity's systems being the target of malicious cyber activities – information that I have included in Annex A. The Minister relies on compromises experienced by other entities and the continued evidence of vulnerabilities and malicious activity experienced by those entities. […].

28. The Minister also relies on the sensitivity and importance of the non-federal entity's information infrastructures as well as the substantial information contained within them, which [list of information held by the non-federal entity] The conclusions explain that CSE must acquire large amounts of information in order to detect and analyze cyber compromises. The Minister also concludes that the acquisition of information is necessary to enable real-time mitigation actions, so as to prevent cyber compromises.

29. In sum, the Minister bases his conclusions on the strategic importance of the non-federal entity, its cybersecurity posture, as well as the cyber threats faced by entities similar to the non-federal entity that are expected to continue. Moreover, he is aware that the cybersecurity activities set out in the Authorization will lead to the acquisition of information in which Canadians or persons in Canada have a reasonable expectation of privacy. I am satisfied that the activities described will respect the statutory requirement that CSE's activities are not directed at Canadians or persons in Canada.

30. Based on the above, I find reasonable the Minister's conclusions that the activities set out in the Authorization are reasonable.

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

31. The Minister also concludes that he had reasonable grounds to believe the authorized activities are proportionate. He considers the manner in which they are conducted, the fact that they are rationally connected to the objective and that they will minimally impair the rights and freedoms of third parties, as well as third parties' ability to access or use equipment or infrastructure.

32. Like last year, the Minister reaches that conclusion by relying on seven internal measures and controls applied by CSE after the information is acquired. I can trace the Minister's rationale for relying on these measures. Access to acquired information is restricted to designated CSE employees who are trained to handle the information and use it on a need-to-know basis for their work. As explained in the record, while analysts have access to the range of information acquired, their interest is in the anomalous behaviour and not the contents of any files, emails, or chat messages themselves. The Minister was cognizant of the privacy interests at issue and laid out the measures in place to protect them.

33. As for the Acts of Parliament that have the potential to be contravened, I am satisfied that the Minister reasonably concludes that they will be proportionate because the activities must be within the scope of those outlined in the Application. As an additional safeguard, if there is a contravention of an Act of Parliament not listed in the Application, the Chief will inform both the Minister and the Intelligence Commissioner.

34. I find that the Minister's conclusions in relation to the proportionality of the activities are justified and intelligible and am satisfied that they are reasonable.

D. Subsection 34(3) of the *CSE Act* – Conditions for issuing an authorization

35. After establishing that the activities are reasonable and proportionate, the Minister may issue the authorization if he concludes that there are also reasonable grounds to believe that the three conditions set out at subsection 34(3) of the *CSE Act* are met, namely that:

    i. any information acquired under the authorization will be retained for no longer than is reasonably necessary;

    ii. any information acquired under the authorization is necessary to identify, isolate, prevent, or mitigate harm to non-federal systems; and

iii. the measures in place ensure that information acquired under the authorization identified as relating to Canadians and persons in Canada will be used, analysed or retained only if essential to identify, isolate, prevent or mitigate harm to non-federal systems.

i. Any information acquired under the authorization will be retained for no longer than is reasonably necessary (s 34(3)(a))

36. As it is not possible to determine in advance what information is needed to help identify and prevent malicious cyber activity, the Minister finds it reasonable for CSE to retain unassessed information for up to 12 months. The effectiveness of CSE's activities depends on being able to cross-reference and analyse multiple sources of already acquired information, including identified indicators of compromise.

37. It is a condition of the Authorization that all acquired information is handled in accordance with relevant CSE operational policies. Information is retained in accordance with the MPS, which contains a retention schedule for the different types of information that may be acquired. Further, the retention periods account for the *Privacy Act*, RSC, 1985, c P-21, minimum retention requirement of two years for any personal information used for an administrative purpose (*Privacy Regulations*, SOR/83-508, s 4), and CSE's information management and record disposition authority issued under the *Library and Archives of Canada Act*, SC 2004, c 11.

38. Prior to the end of the 12-month period, all unassessed information will automatically be deleted unless it is deemed "necessary" or "essential" to help protect non-federal systems. Information assessed as being "necessary" or "essential" can be retained until it is "no longer of use to CSE's cybersecurity and information assurance mandate". The "necessary" criterion applies to information that by its nature does not contain any elements relating to Canadian or a person in Canada. The "essential" criterion applies to information that is identified as relating to a Canadian or a person in Canada.

39. Information retained because it is essential must be reviewed by an operational manager on a quarterly basis to revalidate whether it is still essential; information that is no longer essential must be deleted.

40. I find the Minister's conclusion regarding the 12-month assessment period reasonable. Indeed, retaining information for the length of time needed allows CSE to effectively conduct cybersecurity activities and develop the required cyber responses to keep pace with the rapidly evolving tradecraft of malware threat actors. This allows for better protection of non-federal systems, and in turn federal systems. I also agree with the Minister's conclusion that information that is "necessary" or "essential" to identify, isolate, prevent, or mitigate harm to non-federal systems may be retained until it is no longer useful, provided it is still "necessary" or "essential" for that purpose following the required quarterly reviews.

ii. Any information acquired under the authorization is necessary to identify, isolate, prevent, or mitigate harm to non-federal systems (s 34(3)(c))

41. The Minister's conclusions rearticulate that CSE's cybersecurity activities are only effective if CSE is able to acquire a wide range of information and identify patterns that indicate anomalous activities. The Application notes that the commercial measures used by the non-federal entity are insufficient to detect and counter the sophisticated methods and capabilities deployed by advanced and persistent threat actors.

42. The Minister provides examples of how the information acquired under this Authorization may also be used by CSE to support activities under other cybersecurity authorizations and other aspects of its mandate, including authorized activities in relation to other non-federal systems. Nevertheless, before any information relating to Canadians or persons in Canada can be used, it must have been assessed to be essential for cybersecurity purposes. Further use, analysis, retention and disclosure of any information acquired under the Authorization is subject to restrictions and conditions set out in the MPS, including conditions imposed by CSE's clients or disclosing entities.

43. Given the above, I am satisfied that the Minister's conclusions are reasonable.

iii. Measures to protect privacy will ensure that information acquired under the authorization identified as relating to Canadians or persons in Canada will be used, analysed or retained only if it is essential to identify, isolate, prevent or mitigate harm to non-federal systems (s 34(3)(d))

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 under the cybersecurity and information assurance aspect of its mandate. As indicated in the Intelligence Commissioner's jurisprudence, such measures take on an even greater importance where the role (or network reach) of a non-federal entity is directly and intrinsically linked to sensitive information in which there is a reasonable expectation of privacy.

45. With regard to the retention of IRtC, the Minister reiterates that the information can only be used or retained if it is essential to identify, isolate, or prevent harm to non-federal systems. The Minister sets out additional terms, conditions and restrictions to protect the privacy of Canadians and persons in Canada. Notably, the need for this information to be handled in accordance with section 8 of the MPS, which provides that essentiality rationales must be recorded (s 8.2.2, MPS).

46. Other reasonable measures put in place by CSE consist of limiting access to information and conducting analysis through automated processes – to the extent possible – that limit employees' exposure to unassessed information. Persons accessing information acquired under this Authorization must not only operationally support CSE and its requirements but must have an understanding of the legal and policy requirements for the activities relative to their responsibilities. CSE also carries out regular compliance assessments to help identity and address privacy incidents that may occur during the course of operational activities.

47. In order for CSE to disclose IRtC, the disclosure must be necessary to help protect the non-federal systems as well as federal systems or other systems of importance. The Minister's conclusions and the record mirror the statutory condition found at section 44 of the *CSE Act*. As indicated in last year's decision, the information is only disclosed to persons or classes of persons designated under the section 45 Ministerial Order issued on June 13, 2023 *(Designating Recipients of Information Relating to a Canadian or Person in Canada Acquired, Used, or*

Analyzed Under the Cybersecurity and Information Assurance Aspect of the CSE Mandate). These include owners or administrators of computer systems or networks used by the Government of Canada or a non-federal entity and authorized persons or classes of persons within foreign entities with which CSE has established arrangements.

48. Prior to disclosing IRtC, CSE also has measures in place that must be followed (s 24, MPS) including the obfuscation of identifying information. The MPS sets out the required disclosure approval levels for IRtC, which approvals must be documented.

49. The MPS sets out detailed policies to control and safeguard IRtC that is acquired pursuant to a cybersecurity authorization. In my view, these measures contribute to ensuring that CSE complies with its legislative obligation under section 24, and support the Minister's conclusions. Consequently, I am satisfied that the Minister's conclusions are reasonable.

V. REMARKS

50. I would like to make the following remark which does not alter my findings regarding the reasonableness of the Minister's conclusions.

A. Providing for exceptions to retention periods in authorizations

51. In Decisions CSE-2024-06 and CSE-2025-08, I raised a compliance incident linked to litigation holds. Namely, following a request by the Department of Justice, CSE retained information for litigation purposes collected pursuant to the authorization in question that would otherwise have been deleted within a specific time period. I had expressed that potential exceptions to the usual handling of raw client data retained under an authorization, such as those caused by litigation holds, should be set out in the authorization.

52. With the benefit of the additional information provided in this Authorization, I remain of the view that it is advisable that the terms, conditions or restrictions of future authorizations address potential exceptions to the retention periods to be applied, including specifically those caused by litigation holds. It is especially applicable here as it is foreseen that at least one litigation hold will continue to be in place during the current Authorization. A benefit of the condition would be that in the ordinary course, any such resulting over-retention would not necessarily need to be approached as a compliance incident by CSE.

53. I wish to however emphasize that exceptions to the ordinary operation of established retention schedules set out in the MPS should be just that – exceptional, and as limited in number and scope as possible. As explained by CSE, the over-retention concerns raw client data that was handled within [certain peripheral systems]. While I am not privy to the details of either litigation holds, it is not evident how raw-client data collected pursuant to ministerial authorizations would normally be relevant to either litigation, or more generally to litigation against the Government of Canada.

VI. CONCLUSIONS

54. Based on my review of the record submitted, I am satisfied that the Minister's conclusions made under subsection 34(1) and (3) of the *CSE Act* in relation to activities enumerated at paragraph 81 of the Authorization are reasonable.

55. I therefore approve the Minister's Cybersecurity Authorization for Activities on Non-Federal Infrastructures dated […], pursuant to paragraph 20(1)(a) of the *IC Act*.

56. 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.

57. 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.

[…]

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner