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

File: CSE-2025-06

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*

JULY 2, 2025

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 three non-federal entities (Authorization).

2. The Authorization includes the activities approved by the Intelligence Commissioner over four previous years (Decisions CSE-2024-06, 2023-05, 2022-05, 2021-05) in relation to [Entity A]. It also authorizes new activities for [Entity A] as well as cybersecurity activities in relation to two additional non-federal entities: [Entities B and C]

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 and 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 87 of the Authorization are reasonable.

5. Consequently, pursuant to paragraph 20(1)(a) of the *IC Act*, I approve the Authorization.

II. CONTEXT

6. A detailed legislative context for CSE's cybersecurity activities is set out in past Intelligence Commissioner decisions. As part of its mandate, CSE carries out cyber protection activities to defend 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*).

7. The systems can belong to a federal institution – federal systems (s 27(1), *CSE Act*) – or to a non-federal entity designated as being of importance to the Government of Canada – non-federal systems (s 27(2), *CSE Act*) – such as entities operating in the health, energy, and

telecommunications sectors, as specified in the *Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada* issued on August 25, 2020. Where the authorization relates to a non-federal system, the owner or operator of that system must initiate the process by asking CSE, in a written request, to carry out cybersecurity activities to protect the system and its electronic information (s 33(3), *CSE Act*).

8. To understand vulnerabilities and compromises of non-federal systems, it is necessary for CSE to access and acquire information from those systems. In so doing, CSE may have to contravene certain federal laws. A ministerial authorization grants CSE the lawful authority to carry out cybersecurity activities that contravene a federal law or that lead to the incidental acquisition 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*).

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 Minister must, among other conditions, conclude that the proposed activities are necessary (s 33(2), *CSE Act*), reasonable and proportionate (s 34, *CSE Act*). The authorization is valid for up to one year following the Intelligence Commissioner's approval (s 36, *CSE Act*). It is only then that CSE may carry out the authorized activities.

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) Briefing Note from the Chief to the Minister;
    c) The Chief's Application, containing seventeen annexes including but not limited to:
        i. Letters of request from the non-federal entities;
        ii. Two ministerial orders;
        iii. Retention and Disposition Table;
        iv. List of recommendations from CSE to [Entity A]
        v. Outcomes Report for 2024-2025; and
        vi. Mission Policy Suite – Cybersecurity (MPS) approved February 14, 2025;
    d) Briefing Deck – Overview of the Activities; and
    e) Responses to Intelligence Commissioner's Remarks.

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, 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. On […], the Chief of CSE submitted an application to the Minister for the Authorization (Application). The Application sets out cybersecurity activities that CSE wishes to carry out and describes how CSE will analyse, process and retain the acquired information as well as the measures in place to protect the privacy of Canadians and of persons in Canada in cases where it incidentally acquires information about them.

17. The Application also sets out the cybersecurity solutions to be deployed on the non-federal systems – with the consent of the non-federal entities – which will allow CSE to securely acquire data and take mitigation actions, either manually or automatically. The solutions consist of: […]

18. A description of the non-federal entities, the cybersecurity activities and solutions 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.

19. The Minister concluded that there are reasonable grounds to believe that the Authorization is necessary and that the conditions of subsections 34(1) and (3) of the *CSE Act* were met. As a

result, the Minister issued the Authorization with a one-year validity period, subject to the Intelligence Commissioner's approval.

A. Updated Record

20. The cybersecurity activities that have been approved in the previous four years in relation to [Entity A] are again included in this year's Authorization, which additionally authorizes CSE to […]. The Authorization has expanded to also include cybersecurity activities allowing CSE to access the electronic and information infrastructures of two additional non-federal entities and proactively protect them from known and potential cyber threats.

21. In addition to the Authorization covering two new non-federal entities, the record includes a number of updates. Most notably, CSE has included an annex detailing its responses to certain remarks made in previous cybersecurity and foreign intelligence decisions. I note that CSE has taken seriously my remarks and its efforts to address them in a timely fashion strengthens the ministerial authorization regime. The Authorization addresses the following three issues raised in past remarks: (i) legal authority of the non-federal entities to collect and share information; (ii) consent of users of the non-federal systems; and (iii) sharing of reports based on malicious activities or vulnerabilities.

22. In Decision CSE-2024-05 related to a cybersecurity authorization, I remarked that although the Minister is not statutorily required to confirm that the non-federal entity has the legal authority to collect personal information of Canadians and persons in Canada from its network for cybersecurity purposes and subsequently share this information with CSE, being provided with that confirmation would be helpful to the Minister and myself. In the same vein, in last year's Decision CSE-2024-06 related to [Entity A], I stated that the Minister should be able to easily understand from the non-federal entity's letter of request to CSE that it has the jurisdiction to collect the information and that there exists a legal foundation for its effective sharing with CSE. Further, in Decision CSE-2024-07, I recommended that the link between the entity's legal authority to collect the information and its use for cybersecurity purposes should be more clearly outlined in the record for the Minister.

23. In the record related to Decision CSE-2025-01, the Chief indicated that CSE had received verbal confirmation that the non-federal entity had the legal authority to collect and use personal information for cybersecurity purposes but undertook to obtain confirmation in writing in future authorizations. I am pleased that the letters of request in this Authorization now confirm that each non-federal entity has the legal authority to acquire information for cybersecurity purposes and share it with CSE, in addition to providing CSE access to their systems, which contain personal information and private communications that may be incidentally acquired, used, analysed, retained or disclosed by CSE for cybersecurity purposes.

24. My concerns relating to the consent of persons whose information may be acquired have been raised in several cybersecurity decisions (i.e., CSE-2023-02; 2024-02; 2024-05; 2024-06; 2024-07; and CSE-2025-01). Although CSE obtains the consent of the owner or operator of non-federal systems on which it undertakes cybersecurity activities, contrary to cybersecurity authorizations on federal systems, there is no statutory requirement to consider the consent of the individuals whose information may be acquired (s 34(3)(b), *CSE Act*).

25. In Decision CSE-2024-06, I explained that information in which there is a reasonable expectation of privacy shared on a non-federal entity's system could eventually be retained by CSE for cybersecurity purposes. Consequently, issues relating to the consent of persons whose information may be acquired should remain central and be reflected in cybersecurity authorizations. In CSE 2024-07, I added that confirmation from the non-federal entities regarding their legal authority to collect and use the information for cybersecurity purposes may include elements related to the consent of users of the systems belonging to the non-federal entities. Further, in CSE-2025-01, I indicated that it would be useful for the confirmation to include an overview about the measures taken by the non-federal entity to provide notice to, and obtain consent from, the users of its systems that their information may be collected and used for cybersecurity purposes.

26. In this Authorization, CSE has undertaken to recommend to the non-federal entities to ensure that their login notices indicate to users that information contained or shared on the entities' devices and networks can be used for cybersecurity purposes. This includes personal information and private communications that may be incidentally acquired and could be used,

analysed, retained or disclosed. I expect CSE to inform the Minister and myself of developments related to this recommendation.

27. With respect to the content of the letters of request, I had also made a remark in Decision CSE-2025-01 that the Minister would benefit from a general outline of why the non-federal entity seeks CSE's support. Including additional detail in the letter of request has the benefit of more clearly articulating the objective to be accomplished by CSE and ensuring the consent of the requesting party is fully informed. I note that there are some additional details now provided in the letters of request.

28. With respect to sharing cyber defence reports with non-federal entities receiving cybersecurity services from CSE, I remarked in past decisions (CSE-2024-02 and CSE-2024-06) that CSE should indicate the link between vulnerabilities identified in its reporting to the entity and the impact of those vulnerabilities on the systems. I am satisfied that this year's Application provides additional context on the contents of CSE's reports including the impact the issues reported by CSE could have on the non-federal systems.

29. As set out in section 14 of the *IC Act*, I must review whether the Minister's conclusions made under subsections 34(1) and (3) of the *CSE Act*, on the basis of which the authorization was issued under subsection 27(2) of the *CSE Act*, are reasonable.

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

30. The Minister concluded that he had reasonable grounds to believe that the activities are reasonable given the objective of helping to protect the non-federal entities' electronic information and infrastructure, as well as to potentially protect federal systems and other systems of importance from mischief, unauthorized use, or disruption.

31. The Minister explains that the cybersecurity activities set out in the Authorization present a risk that CSE may acquire information in which Canadians or persons in Canada have a reasonable expectation of privacy. Given that the cybersecurity solutions acquire […]. I am of the view that CSE will almost certainly collect such information – which underscores the need for this

Authorization. I note, however, that I am satisfied that the cybersecurity activities set out in the Authorization respect the statutory requirement that CSE's activities are not directed at Canadians or persons in Canada.

32. To justify the reasonableness of the activities of the three non-federal entities, the Minister relies on three grounds: 1) the effectiveness of the activities for which the Authorization is sought; 2) the need for CSE's support given the important roles of the non-federal entities; and 3) the threat to the non-federal entities' systems posed by cyber threat actors.

33. First, the activities set out in the Authorization are effective and complement the other cybersecurity activities of the non-federal entities. The Minister explains that CSE's knowledge and cyber solutions allow for detection and response to threats unknown to commercial providers of cybersecurity solutions. The Minister also explains that the non-federal entities hold vast amounts of data and given their nature, are attractive targets to malicious actors. They also hold information […] providing opportunities for threat actors to exploit weaknesses and making cyber defence efforts more difficult.

34. Cybersecurity solutions allow CSE to identify and better understand malicious cyber activity or other indicators of compromise in order to advise the non-federal entities on how to protect their systems and to conduct mitigation actions. The information CSE collects can also help it protect federal systems and other systems of importance.

35. The second ground relied upon by the Minister is the critical role played by the non-federal entities. The Authorization renews cybersecurity activities to protect […] I note that […], which means that it is in the public interest that it be protected, but also that the information can be particularly attractive to ransomware actors. The Authorization also sets out new authorities for activities to identify and defend against highly sophisticated and persistent threats to […]

36. For its part, [Entity C] provides critical services to support […]. A cyber compromise could cause […]. I note that the current authorization with respect to [Entity A] only expires in October 2025 but agree with the Minister that expanding the scope of CSE's support to include [Entity C] is pressing given […]

37. The third reason supporting the Minister's conclusion is the existing cyber threat landscape. As indicated in Decision CSE-2025-01, the purpose of a cybersecurity authorization is to help protect the systems and information of the non-federal entity. Protecting the systems does not require responding to a cyber compromise. In contexts where cybersecurity activities are carried out for preventative or proactive purposes – where there is no known compromise or specific threat to the non-federal entity – the Minister nevertheless needs to establish a factual basis for CSE's assistance.

38. In the Authorization, the Minister does not state with certainty that the non-federal entities will be targeted by cyber threat actors. However, the record describes existing cyber threat actors in great detail, and provides information related to the likelihood of the non-federal entities' systems being the target of malicious cyber activities – information that I have included in Annex A. Underpinning the Minister's rationale is that the cyber threats to the non-federal entities exist as a direct correlation to the critical role they play. Indeed, ransomware incident data shows […].

39. CSE assesses that [Entity C] […].

40. I note that in last year's decision relating to [Entity A], I raised concerns relating to certain elements of the Minister's conclusions, in particular with respect to relying on the presence of ongoing threats and on the outstanding implementation of CSE recommendations to justify CSE's continued presence on the system. Specifically, I remarked that when renewing cybersecurity authorizations for extended periods of time, CSE should provide the rationale for its continued presence on the non-federal entity's systems and as a result, the Minister's conclusions may have to evolve to meet the reasonableness standard that I must apply.

41. The Authorization provides clarification of the rationale for CSE's continued presence on [Entity A]'s systems. It provides additional contextual information about the nature and type of threats currently faced by [Entity A] as well as future threats […]. Further, it is now clear which key recommendations remain to be implemented and the resulting impact on the entity's cybersecurity posture. I am satisfied that the additional information in the record addresses my previous concerns.

42. As explained by the Minister, […] [Entity A] cyber threat landscape and therefore requires deployment of CSE's […]. Although the steps taken by [Entity A] have improved its cybersecurity posture, malicious activity and vulnerabilities are still being detected. CSE's continued assistance is being sought to protect [Entity A]'s systems from current and ongoing threats. […] ensures a strong cybersecurity posture.

43. I find convincing the Minister's rationale that the nature of the non-federal entities makes them a likely target for cyber threat actors. There is a rational link between the cybersecurity activities and the effectiveness of protecting the non-federal entities' systems. I am also satisfied that the Minister has established a sufficient factual basis of the threat to the non-federal entities' systems. As a result, 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*)

44. The Minister also concluded that he had reasonable grounds to believe the authorized CSE cybersecurity activities are "proportionate given the manner in which they are conducted, and because they are rationally connected to the objective and will minimally impair the rights and freedoms of "third parties", as well as their ability to access or use equipment or infrastructure.

45. The Minister identifies the reasons for which the activities are necessary and useful, notably for acquiring information to help protect non-federal systems and to support other CSE activities. He recognizes that the authorized activities can lead to the acquisition of large volumes of information in order to identify cyber threats. However, the Minister notes that CSE retains only a very small percentage of the total amount of data initially acquired. I am satisfied that the Minister's conclusions in this regard are reasonable with respect to the authorized activities.

46. To show that the activities are proportionate, the Minister sets out the same internal measures and controls applied by CSE in past authorizations to ensure protection of the information it acquires. I can trace the Minister's rationale for relying on these measures and controls, and I am satisfied that they are reasonable. He explains how the activities seek to achieve a reasonable

balance between obtaining necessary information and privacy interests. CSE is interested in any anomalous behaviour related to the information, rather than its contents.

47. As for the Acts of Parliament that have the potential to be contravened, the Minister's balancing exercise is also evident. Indeed, the Authorization indicates they are limited in number because the activities would take place only on systems where CSE has received the express consent of the owner to operate. Also, the activities must fall within the scope of those outlined in the Chief's Application and are restricted to the acquisition of information for the protection of non-federal systems and federal systems. 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.

48. The Minister's conclusions reflect his understanding of the privacy interests at issue and the measures in place to protect them, as well as the potential impact on the rule of law. Taking these into account, he concluded that the activities were proportionate. I find that his conclusions are justified and intelligible. As a result, I am satisfied that the Minister's conclusions in relation to the proportionality of the activities are reasonable.

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

49. When the Minister finds that the activities are reasonable and proportionate pursuant to subsection 34(1) of the *CSE Act*, the Minister may issue a cybersecurity authorization to help protect non-federal systems if he concludes that there are reasonable grounds to believe that the three conditions set out at subsection 34(3) of the *CSE Act* are met, namely:

    a) any information acquired under the authorization will be retained for no longer than is reasonably necessary;
    b) any information acquired under the authorization is necessary to identify, isolate, prevent, or mitigate harm to non-federal systems; and
    c) 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))

50. Information is retained in accordance with requirements set out in CSE policies and is governed by a retention schedule. The Minister explains that the retention schedule 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.

51. CSE is unable to predetermine what information will be helpful in identifying malicious activity and therefore, acquires a large volume of information generated by or residing on the non-federal entities' systems. The Minister explains that CSE processes this information, mainly through automated means. This process may identify some of the information as "necessary" or "essential". All other information is considered to be unassessed, even though it has gone through the automated processes. The maximum retention period for unassessed information is 12 months.

52. There is often a period of time between when a compromise begins and when it is first identified. As explained by the Minister, the effectiveness of CSE's activities depend on being able to cross-reference and analyse multiple sources of already acquired information, including identified indicators of compromise. New vulnerabilities are discovered on an ongoing basis and a 12-month retention period allows CSE to reach back to the origins of an event or examine its evolution over time. Comparing a compromise against unassessed data or undetected threat activities helps CSE develop better mitigation actions and cyber responses that can also be used not only for the non-federal systems in this instance but other designated systems of importance, and federal systems.

53. Prior to the 12-month period, unassessed information will automatically be deleted unless deemed "necessary" or "essential" to help protect the non-federal systems, or federal systems and other designated systems of importance. The Chief states in the Application that the non-federal entities are aware and agree to this use of the information.

54. Access to unassessed information is strictly controlled and limited to those authorized to conduct or support cybersecurity activities (s 10.2, MPS). Every query performed against

acquired unassessed information is logged for audit and accountability purposes. Unassessed information cannot be shared beyond CSE.

55. The Minister also highlights that CSE's internal compliance program has an established process for responding to incidents. As long as the processes work as intended, this multi-layered approach allows CSE to maintain strong privacy protection measures.

56. As explained in the record, the "necessary" criterion applies to information that by its nature does not contain any elements relating to Canadian or a person in Canada. Information is considered "necessary" when it is required for the understanding of malicious cyber activity, including […], for the purpose of helping to protect non-federal systems. The purpose is to assist in developing detection and prevention analytics and further strengthen the cyber defence ecosystem.

57. In contrast, the "essential" criterion applies to information that relates to a Canadian or a person in Canada. Without this information, CSE would be unable to identify, isolate, prevent, or mitigate harm to the non-federal system. This may include […]. The information acquired may be highly sensitive to Canadians and most analysis is done through automated processes, which flags abnormal behaviour and limits employees' exposure to the content of the files.

58. Information that is determined to be necessary or essential to identify, isolate, prevent, or mitigate harm may be retained "indefinitely or until the information is no longer useful for these purposes." This information is tracked and operational managers "must review" retained recognized information related to Canadians or persons in Canada on a quarterly basis to revalidate whether it remains essential.

59. Given the multiple layers of internal controls and limits on access to unassessed information, 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 as well as 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.

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

60. CSE's cybersecurity activities are effective only with the acquisition of a vast range of information that is then assessed to identify malicious activities. CSE cannot predict which […] and is therefore required to acquire a substantial amount information. As the non-federal systems are located in Canada, CSE will incidentally acquire information that interferes with the reasonable expectation of privacy of Canadians and persons in Canada.

61. The Minister explains that while commercial cybersecurity platforms are currently used by the non-federal entities, they are "not sufficient to identify and counter persistent and increasingly complex cyber threats." As remarked in last year's decision in relation to CSE's cybersecurity activities (CSE-2024-06), it is unclear whether commercially available safeguards will ever be sufficient to fully protect non-federal entities' systems and federal systems. Without being alarmist, CSE's expertise has become more and more important in responding to growing sophisticated and complex cyber threats.

62. Finally, the Minister provides examples on 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. 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.

63. For these reasons, 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))

64. 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 its cybersecurity and information assurance aspects of its mandate. I note that these measures take on an even greater importance when the role of a non-federal entity is directly and intrinsically linked to sensitive information in which there is a reasonable expectation of privacy – which is the case of [Entity A and the type of information it collects].

65. With regard to the retention of information related to Canadians or persons in Canada (IRtC), the Minister reiterates that the information can only be retained if it is assessed to be essential – meaning that without the information, CSE would be unable to identify, isolate, or prevent harm to the non-federal entity's system. Essentiality rationales must be recorded by employees (s 8.2.2, MPS). In my view, these measures contribute to ensuring that CSE complies with its legislative obligation under section 24, and support the Minister's conclusions.

66. In order for CSE to disclose IRtC, the disclosure must be necessary to help protect non-federal systems, federal systems or other systems of importance. The Minister's conclusions and the record mirrors the statutory obligation found at section 44 of the *CSE Act*. The information is only disclosed to persons or classes of persons designated under the *Ministerial Order 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* issued on June 13, 2023, in accordance with section 45 of the *CSE Act*. These include owners or administrators of computer systems or networks used by the Government of Canada or a non-federal entity, as well as authorized persons or classes of persons within foreign entities with which CSE has established arrangements.

67. Prior to disclosing IRtC, CSE also has measures in place that must be followed (s 24, MPS). A method used by CSE is to suppress identifying information. When IRtC is disclosed, the MPS sets out the required disclosure approval levels, which must be documented.

68. I note that in the letters of request to CSE, each non-federal entity asked that all its proprietary information, and all personal information that may be collected and retained be obfuscated before it is shared beyond the entity and CSE.

69. The MPS sets out elaborate policies to control and safeguard IRtC that is acquired pursuant to a cybersecurity authorization. In my view, when followed, these measures provide an effective manner for CSE to respect the legislative requirement to sufficiently protect this information. Consequently, I am satisfied that the Minister's conclusion is reasonable.

V. REMARKS

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

A. Scope of the Authorization

71. In [Entity B]'s request letter, the [authorized representative of the entity] requests CSE "to assist in the protection of the electronic information and information infrastructure under the control and supervision" of his office. According to the record, the [description of the information infrastructure].

72. However, the record also identifies […] additional [entities] that are "within [Entity B]'s network". [Entity C] is one of the listed additional [entities], which also […]. The nature of some of these [entities] suggests that they can hold particularly sensitive information, […]. [Entity C] is the only entity of those listed for which a letter of request is included in the record, and for which […].

73. The Authorization indicates that CSE may determine when and for which [entity] CSE accepts requests to conduct cybersecurity and information assurance activities, provided [Entity B] is the owner of that infrastructure. CSE shall inform the Minister when it accepts such a request, and will subsequently inform the Intelligence Commissioner.

74. While the Authorization is clear that CSE may only conduct activities on infrastructure owned by [Entity B] given the fact the additional [entities] are listed as being "within [Entity B]'s network" I wish to make clear that no activities in relation to the infrastructure used by those [entities] that are not owned by [Entity B] are being authorized.

VI. CONCLUSIONS

75. 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 87 of the Authorization are reasonable.

76. 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*.

77. 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.

78. 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.

July 2, 2025

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner