File: CSE-2025-08

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*

NOVEMBER 5, 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 – the governments of the Northwest Territories (GNWT), the Yukon (YG), and Nunavut (GNT) (Authorization).

2. The Authorization renews existing cybersecurity activities previously approved by the Intelligence Commissioner in relation to the three entities and adds new activities in relation to the GNWT. This is the third consecutive year in which a cybersecurity authorization covering all three territorial governments has been issued (see previously Decisions CSE-2024-07, CSE-2023-06), and the fourth consecutive year a cybersecurity authorization covering the GNWT has been issued (Decision CSE-2022-06).

3. On October 9, 2025, pursuant to subsection 27(2) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*), the Minister issued the Authorization. It was received by the Office of the Intelligence Commissioner the next day 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 90 of the Authorization are reasonable.

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

II. CONTEXT

6. 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*).

7. 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.

8. 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.

9. 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 three territorial governments. 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*).

10. 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*).

11. 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*).

12. 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 September 26, 2025, containing seventeen annexes including but not limited to:
        i. Letters of request from the three territorial governments;
        ii. Two ministerial orders;
        iii. Outcomes Report for 2024-2025;
        iv. Two Strategic Cyber Threat Assessments;
        v. Mission Policy Suite – Cybersecurity (MPS) approved August 2025;
        vi. Record of Changes MPS Cybersecurity August 2025 Update; and
        vii. Lists of agencies within the territorial governments' networks;
    c) Responses to Intelligence Commissioner's Remarks;
    d) The Chief's Briefing Note to the Minister; and
    e) Briefing Deck – Overview of the Activities.

III. STANDARD OF REVIEW

13. 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.

14. 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.

15. 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.

16. 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

17. The Chief's Application constitutes a request for the renewal of the authorized cybersecurity activities I approved last year (Decision CSE-2024-07), with the added deployment of [...] to the GNWT's network. A description of 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

18. In my decisions, I make remarks that raise legal or factual issues of concern, with the aim of improving the content of future records or otherwise highlighting issues for CSE's consideration. Before considering CSE's specific responses to some of my latest remarks, I wish

to acknowledge CSE's overall responsiveness to the issues raised. This process has resulted in tangible improvements to the ministerial authorization process.

19. As regards specific responses to my more recent remarks, I am satisfied that CSE now provides sufficient contextualization of incidental acquisition of information relating to a Canadian or a person in Canada (IRtC). The Minister acknowledges that through its activities, CSE "will" acquire information that interferes with the reasonable expectation of privacy of Canadians or persons in Canada or contravene any other Act of Parliament. I am also satisfied with the detailed information found in the Outcomes Report about the types of information retained by CSE, the sharing of reports with the non-federal entities, the potential impact of identified vulnerabilities, and whether any reporting containing IRtC was shared with international partners (it is indicated none was).

i. Letters of request

20. In last year's decision (CSE-2024-07), I remarked that the record before the Minister should confirm the non-federal entities' legal authority to collect and share the information that is ultimately collected by CSE through its cybersecurity activities. The territorial governments now expressly confirm their authority in the letters of request.

21. Following that decision, I made additional remarks in other cybersecurity decisions intended to further improve the contents of letters of request. In Decision CSE-2025-01, I explained that it would be beneficial for each request letter to provide a general outline of the reason(s) for which the non-federal entity is requesting CSE's support, while acknowledging that certain factors, such as classification levels, may limit the level of detail included in the letters. In Decision CSE-2025-07, I noted that letters of request could be modified to better reflect whether they constitute the first request an entity has made for CSE's assistance, or whether they seek the renewal of ongoing assistance already being provided under an existing authorization. I note that YG's letter indicates that the request is a "renewal" of the agreement with CSE, but GNT's letter does not (nor does GNWT's letter, but it predates my remark).

ii. User notices and consent

22. Another remark that has been discussed in previous cybersecurity decisions relates to the consent of persons whose information may be acquired by CSE when it conducts activities on the non-federal entities' systems. As indicated in Decision CSE-2025-06, CSE has undertaken to recommend to the non-federal entities 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, analyzed, retained or disclosed.

23. In this record, CSE explains that it has reached out to the three non-federal entities and requested that they provide an overview of the measures taken to provide login notices to its users. Further, CSE has now incorporated this question into its procedures for new non-federal clients and is in the process of requesting this information from other existing non-federal clients. I recognize that CSE cannot mandate the non-federal entities to take specific measures, and that notification and consent requirements may vary by jurisdiction. Nevertheless, CSE commits to continue to provide recommended language for use in login notices by its non-federal clients. I appreciate CSE's continued commitment to addressing my remark.

iii. Potential of sharing of information relating to Canadians with systems of importance outside of Canada

24. In my recent Decision CSE-2025-07, I made a remark on the need for the Minister to have a complete understanding of how IRtC incidentally collected and retained by CSE could potentially be shared for cybersecurity purposes with designated persons or classes of persons, including owners or operators of systems of importance designated by ministerial order pursuant to section 21 of the *CSE Act*. In sum, I described how 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* (Section 45 Ministerial Order), allows for the sharing of IRtC with the owners or operators of systems of importance. I observed that the record did not reflect the designations of the electronic information and

information infrastructures of the Governments of Ukraine and Latvia as systems of importance, nor the resulting possibility that IRtC could therefore be shared with these governments.

25. CSE has indicated that any sharing of IRtC with Ukraine or Latvia would be included in the Outcomes Report, along with any other international partners IRtC was shared with. CSE also confirms that Annex 2 of the SOI Order does not currently contain any designations.

26. The main point of my remark stands. The current ministerial order allows sharing of IRtC with the owners or operators of any system of importance. The record includes the August 2020 SOI Order. In the absence of any reference that any other ministerial order designating a system of importance exists, the record risks giving the Minister and I an incomplete picture that it is the only directive designating systems of importance. The way in which IRtC is treated and can potentially be shared – in particular outside of Canada – is relevant to both our respective assessments and should be properly reflected in the record.

iv. Updated MPS Cybersecurity

27. The record includes a recently amended version of the MPS Cybersecurity dated August 8, 2025, as well as a Record of Changes outlining new and amended provisions of the MPS. Some amendments were made to align with the *Mission Policy Suite for Foreign Intelligence* while others address remarks that I have made in previous decisions. Overall, I note that the MPS provides additional wording and more examples to clarify the acceptable parameters for certain activities, the prohibition against directing activities at Canadians or persons in Canada, and to reflect the new 2025 National Cyber Security Strategy. Some changes are also made for clarification in the section pertaining to the disclosure of IRtC where there are reasonable grounds to believe the information is relevant to an imminent danger of death or serious bodily harm. The MPS now indicates that any such instances must be specifically reported to National Security and Intelligence Review Agency (as opposed to “appropriate review bodies”); I expect they would also be included in outcomes and end of authorizations reports.

28. Additional amendments to the MPS are linked to the retention schedules for IRtC and non-IRtC acquired under an authorization and requirements associated with acquired solicitor-client communications.

29. I note that the changes made to provisions on solicitor-client privilege mirror those described in a foreign intelligence decision (CSE-2025-04, paras 58 to 60) emphasizing the importance of limiting access to potentially privileged communications. In my decision, I had suggested that CSE consider delineating its process with more definitive terms and am of the view that the restriction that "upon recognition, personnel will strictly restrict access to the communication on a need-to-know basis" included in the MPS is a positive step in this direction.

v. Compliance incident

30. As set out in last year's decision at paragraph 78, the 2022-2023 end of authorization report for activities in relation to the GNWT described a compliance incident concerning the over-retention of certain information due to a litigation hold. The most recent end of authorization report covering November 30, 2023 – November 14, 2024 provides an update of the incident and steps taken to address it.

31. The present record does not provide an update on these steps. I trust that the forthcoming end of authorization report will address if and when the relevant litigation hold has lifted, and confirm whether the over-retained information was deleted. I remain of the view expressed in Decision CSE-2024-06 that exceptions to the usual handling information under an authorization, such as those caused by litigation holds, should be set out in the authorization.

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

32. The Minister concludes that there are reasonable grounds to believe that the authorized activities are reasonable on the basis that cyber attacks are increasingly more sophisticated and difficult to detect. The conclusions explain that CSE must acquire large amounts of information in order to detect and analyze cyber compromises, and that it is not possible to know in advance which information will be particularly relevant or necessary. Finally, the Minister concludes that acquisition of information is necessary to enable real-time mitigation actions, so as to prevent cyber compromises.

33. The Minister additionally relies on the previous compromise experienced by one of the territorial governments and the continued evidence of vulnerabilities and malicious activity experienced by each of the territorial governments. Lastly, he relies on the sensitivity and importance of the territorial governments' information infrastructures as well as the information contained within them.

34. Reasonableness and proportionality must be assessed "having regard to the nature of the objective to be achieved" (s 34(1), *CSE Act*).

35. The purpose of an authorization relating to a non-federal system like the one before me, must be to help protect its information infrastructure from mischief, unauthorized use or disruption. Conversely, the purpose of an authorization relating to a federal system must be to help protect the infrastructure of the federal system.

36. The Minister's conclusions on reasonableness and proportionality articulate the objective in different ways. The Minister's first description of the objective refers to helping to protect "federal systems and systems of importance" (emphasis added). Paragraph 57 of the Minister's conclusions also refers to information acquired from deployed sensors being used "to identify, isolate, prevent, or mitigate harm to federal systems and subsequently those designated as systems of importance." The Minister then ends by setting out the objective as "helping to protect each of the territorial governments' electronic information and information infrastructures."

37. Based on a holistic and contextual reading of the record (*Vavilov,* para 97), I remain satisfied that the objective to be achieved has not changed from previous authorizations. Paragraph 15 of the Application helpfully distinguishes between the "primary objective" of protecting the territorial governments' infrastructures and several "sub-objectives", including using acquired information to help protect federal systems and other non-federal systems of importance. Similarly, paragraph 59 of the Authorization refers to protecting the territorial governments' infrastructures […] protecting federal systems and other non-federal systems of importance. In my view, these two references most accurately represent the overarching objective gathered

from reading the full record, which is first and foremost to protect the systems of the territorial governments.

38. In light of the above, future authorizations should ensure the objective is described consistently throughout the authorization and application, and properly reflects the type of authorization being pursued. As per the *CSE Act,* the primary objective of an authorization pertaining to a non-federal entity must be to protect that entity's systems.

39. I have previously noted that a specific rationale should be articulated for the need for the continuation of activities that have already been previously authorized multiple times (Decision CSE-2024-06 at para 78; Decision CSE-2024-07 at para 84). Here, the Minister's detailed reasons as to why the Authorization is necessary also double as such a rationale. The Minister bases his conclusion on the strategic importance of the Arctic to Canada, the current cybersecurity posture of each territorial government, as well as the cyber threats the territories have faced, and are expected to continue to face.

40. I note that the record does not include any updates on the status of outstanding recommendations from CSE that the GNWT was in the process of implementing. I understand this may reflect the overall shift in the rationale for CSE's involvement, which is moving away from responding to a specific incident towards maintaining a more proactive presence due to the strategic importance of the territories. Nonetheless, I had noted the same absence in last year's decision (para 33) and expected that it would be addressed in this year's record. While the Minister's description of the reasons the Authorization is necessary in this case allows me to be satisfied that his conclusion is reasonable, I re-emphasize my expectation that the record should allow the Minister to understand the progress that has been accomplished, including in relation to specific recommendations CSE had previously put forward.

41. The Minister explains 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 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.

42. 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*)

43. The Minister also concludes that he had reasonable grounds to believe the authorized 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 third parties' ability to access or use equipment or infrastructure.

44. To reach that conclusion, the Minister relies, like last year, on seven internal measures and controls applied by CSE after 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 this type of information and use it on a need-to-know basis for their work. The Minister was cognizant of the privacy interests at issue and laid out the measures in place to protect them.

45. In last year's decision pertaining to the same three entities, I noted that the record did not indicate the total amount of information (i.e. "items") acquired over the course of a previous authorization. An estimated total figure of "records" acquired is now provided, with the switch of metric from "items" to "records" explained. The provided figures confirm that CSE acquired a voluminous number of records, but retained only a small portion, representing well under 1% of the total.

46. 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.

47. As the Briefing Deck to the Minister indicates, the planned deployment of another type of cybersecurity solution ([...]) to GNWT represents the [...]. The deployment is at the specific

request of the GNWT, with the Application emphasizing the past sophisticated compromise of the GNWT's network.

48. In many parts of the record, references to deploying the existing solutions have simply been updated to also include reference to the to be deployed solution. I take this to implicitly suggest that the new solution's operation in this new context is not expected to fundamentally differ from the already deployed solutions, or to fundamentally change the Minister's assessment of the proportionality of the activities.

49. Nevertheless, the Minister's conclusions could have been strengthened by explicitly setting out such an assessment. As is noted in new wording in the updated MPS, risk assessments can "help to determine if the potential risks associated with an activity are reasonable and proportionate" when considering the objective of the activity. I note that a footnote identified as forming part of the amendments to the MPS (which does not appear to have actually been included in the updated MPS), indicates that changes that might necessitate a risk assessment include deploying an activity or service to a new category of client such as a non-federal entity. This appears to be the situation here.

50. As I have previously noted, deployments to non-federal systems are arguably the activity that is most incidentally intrusive to Canadians and persons in Canada (Decision CSE-2024-06 at para 80). I highlight that in this particular case, the deployment could encompass not only the core departments of the territorial government, but also independent agencies and bodies that are "within its network" and that have unique and heightened privacy concerns ([...]). It is not clear to me from the record whether a risk assessment taking this context into consideration was undertaken.

51. Ultimately, based on the deployment being requested by the territorial government and the fact that nothing in the record suggests the new deployment would fundamentally alter the proportionality of the activities, I am satisfied 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

52. When the Minister concludes that there are reasonable grounds to believe 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 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))

53. The Minister finds it is necessary to retain unassessed information for up to 12 months because it is not possible for CSE to determine in advance what information will be helpful for identifying and preventing malicious cyber activity. As explained by the Minister, this is necessary to allow for retroactive analysis. Indeed, 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. 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.

54. It is a condition of the Authorization that all acquired information is handled in accordance with relevant CSE operational policy. Information is retained in accordance with the MPS, which contains a retention schedule for the different types of information that may be acquired.

55. The Minister explains that retention periods account for the *Privacy Act* 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.

56. 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.

57. 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. I note that the update to the MPS has not corrected an apparent discrepancy I have previously identified as regards the wording of this requirement; whereas the Authorization provides that operational managers "must review" the retained IRtC, the MPS provides that they are "reminded to review" it (Decisions CSE-2025-07 at para 45 and CSE-2025-01 at paras 78-82).

58. In considering how "necessary" and "essential" are defined, it is helpful to again consider the delineation in the *CSE Act* between cybersecurity authorizations for federal systems and those pertaining to non-federal systems. For cybersecurity authorizations relating to non-federal entities, the Minister must conclude that any information acquired by CSE under the authorization will be necessary, or, in the case of IRtC essential, to identify, isolate, prevent or mitigate harm to <u>systems of importance</u> (s 34(3)(c)(ii) & 34(3)(d)(ii)) (emphasis added).

59. I note that the term "essential" is not defined consistently across the record. Paragraph 71 of the Authorization, which defines the term for the purpose of the Authorization, mirrors the statutory wording exactly. However, paragraph 66 of the Authorization states that information is retained

if it is essential or necessary to help protect "federal systems and systems of importance" (emphasis added). Paragraph 123 of the Application includes a definition referring only to systems of importance but expanding the scope of "essential" to include information assessed as providing insight into […], for the purpose of helping to protect systems of importance. The MPS also includes this same broader definition but extends it to protecting federal systems or systems of importance (MPS Annex E).

60. I view the increased number of references to information being essential to protect both federal systems and non-federal systems of importance to be a reflection of CSE's experience that – in practice – information that is essential to protecting non-federal systems will also be essential to protecting federal systems, and vice versa. Indeed, viewed in light of this experience, the distinction made in the *CSE Act* on this point begins to seem artificial.

61. That does not, however, change the fact that the conditions are specifically set out as they are in the *CSE Act*. In order to be retained, IRtC acquired under an authorization issued under subsection 27(2) must be essential to identifying, isolating, preventing or mitigating harm to non-federal systems of importance (s 34(3)(d)(ii)) (emphasis added). Similarly to my assessment of the objective of the Authorization, I am satisfied the Minister's conclusions respect this condition, but highlight that care should be taken to be consistent in the articulation of "essential" and "necessary", in a way that reflects the statutory condition.

62. 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.

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

63. The Minister's conclusions rearticulate that CSE's cybersecurity activities are only effective if CSE is able to acquire a wide range of information. The Application notes that the commercial measures in place at the non-federal entities are insufficient to detect and counter the sophisticated methods and capabilities deployed by advanced and persistent threat actors. CSE's foreign intelligence activities give it unique visibility into these actors' capabilities, intentions and activities.

64. 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 of importance.

65. Given all of 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))

66. 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. I emphasize, as I have previously, that 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 (Decision CSE-2024-06).

67. 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 further provides that information must be handled in accordance with section 8 of the MPS, which provides that essentiality rationales – determined either through manual or

automated processes – must be recorded (s 8.2.2, MPS). In my view, this measure contributes to ensuring that CSE complies with its legislative obligation under section 24 and supports the Minister's conclusions.

68. In addition, the Minister sets out additional terms, conditions and restrictions to protect the privacy of Canadians and persons in Canada. Namely, CSE will implement reasonable measures to limit access to information and will to the extent possible conduct analysis through automated processes that limit employees' exposure to unassessed information. CSE will also establish and maintain procedures to verify and ensure that it is conducting its activities in accordance with the Authorization.

69. In order for CSE to disclose IRtC, the disclosure must be necessary to help protect the territorial governments' systems, 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*. The information is only disclosed to persons or classes of persons designated under the Section 45 Ministerial Order. 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.

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

71. I note that in the letters of request to CSE, each non-federal entity asks that all personal information, information that identifies the non-federal entity, or proprietary information of the non-federal entity be obfuscated before it is shared beyond CSE and the non-federal entity. The Minister's Authorization itself provides that the disclosure of information acquired remains subject to such client conditions. In Decision CSE-2025-01, I highlighted that various references in the record made it unclear how exactly such requests for obfuscation interact with CSE policies in the MPS and how they are therefore operationalized. I expect upcoming records to provide clarification on this point.

72. The MPS sets out detailed 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 conclusions are reasonable.

V. REMARKS

73. I would like to make the following three remarks which do not alter my findings regarding the reasonableness of the Minister's conclusions.

A. Clarification of Outcomes Report

74. The Outcomes Report includes statistics on the number of users being monitored by one of the cybersecurity solutions deployed to the territorial governments' networks. I note that the number of monitored users varies significantly from the most recent End of Authorization report; the user numbers have […] across all three territories. No explanation is provided.

75. As previously remarked in decision (CSE-2024-02 at para 87), where the information presented in an outcomes or end of authorization report varies significantly from one report to another, an explanation must be provided. Consequently, I expect the next End of Authorization report to provide an explanation for the variation in the user numbers.

B. Scope of the Authorization

76. As has become standard, the Application includes annexes listing the departments and agencies "within" each territorial government's network that are eligible for CSE's cybersecurity and information assurance activities. My comparison of the lists of agencies that are described as being "within" one of the territorial government's networks (GN) shows that [some agencies] that were included in last year's annex have been removed without explanation. I acknowledge that CSE does not control which agencies use the information infrastructures belonging to the respective territorial governments. However, given that the list informs the potential scope of the authorization and information that could be acquired, and that the nature of an agency can

determine if it holds information that raises particular privacy considerations, whether an agency is added or removed from the eligibility list could be relevant to the Minister and myself. CSE should therefore make efforts to ensure the list is accurate and summarize any modifications to the list in the record.

C. Assessing sensitive IRtC

77. As stated in the record, the MPS is treated as an evergreen document that is periodically updated to reflect evolving legal and policy developments. I am convinced that the most recent updates improve the guidance available to CSE employees implementing the activities set out in authorizations. The amendments to the MPS coupled with the variety of agencies who use the territorial governments' electronic infrastructures brings me to make the following remark.

78. In past decisions, I have highlighted the fact that cybersecurity activities can lead to the collection of information that is highly sensitive – for example health-related information. The MPS explains that CSE uses a contextual approach to determine the level of sensitivity of IRtC, and that stronger privacy protection measures are in place for more sensitive IRtC. This framework also applies to the disclosure of information.

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

VI. CONCLUSIONS

80. 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 90 of the Authorization are reasonable.

81. I therefore approve the Minister's Cybersecurity Authorization for Activities on Non-Federal Infrastructures dated October 9, 2025, pursuant to paragraph 20(1)(a) of the *IC Act*.

82. 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.

83. 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.

November 5, 2025

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner