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

File: 2200-B-2024-07

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 15, 2024

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 non-federal entities.

2. On October 22, 2024, pursuant to subsection 27(2) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*), the Minister issued a Cybersecurity Authorization for Activities on Non-Federal Infrastructures in relation to the governments of the Northwest Territories (GNWT), the Yukon (YG) and Nunavut (GNT) (Authorization). This is the second year the Minister issues a cybersecurity authorization that includes these three non-federal entities – which I approved in Decision 2200-B-2023-06 – and the third year a cybersecurity authorization is issued for GNWT (Decision 2200-B-2022-06).

3. On October 23, 2024, the Office of the Intelligence Commissioner received the Authorization 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 activities and classes of activities enumerated at paragraph 79 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 its mandate as the national signals intelligence agency (s 15(1), *CSE Act*), CSE carries out cyber protection activities to defend the 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*). 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.

7. To effectively engage in cyber protection activities on the federal and non-federal systems, CSE may have to contravene certain Canadian laws. In addition, CSE may incidentally acquire communications and information that interfere with the reasonable expectation of privacy of Canadians or persons in Canada. Prior to conducting these cybersecurity activities that may fall outside the boundaries of the law and infringe on Canadian privacy interests, the *CSE Act* requires CSE to obtain a ministerial authorization.

8. 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*).

9. The Chief of CSE must then present a written application to the Minister setting out the facts that would allow him to conclude that there are reasonable grounds to believe that the Authorization is necessary (s 33(2), *CSE Act*). The Minister must additionally conclude that the statutory conditions set out at subsections 34(1) and (3) of the *CSE Act* have been satisfied. The Minister sets out his conclusions in the authorization, which is provided to the Intelligence Commissioner for review. The Intelligence Commissioner approves the activities or classes of activities specified in the ministerial authorization if satisfied that the Minister's conclusions are reasonable.

10. The ministerial authorization is valid once approved by the Intelligence Commissioner (s 28, *CSE Act*). Only then can CSE carry out the authorized activities specified in the authorization – that is, the activities that may otherwise be unlawful and infringe on the privacy interests of Canadians or persons in Canada.

11. As specified in subsection 27(2) of the *CSE Act*, the Minister may authorize CSE to acquire any information originating from, directed to, stored on or being transmitted on or through the non-federal system for the purpose of helping to protect it, in circumstances described in paragraph 184(2)(e) of the *Criminal Code*, RSC 1985, c C-46, from mischief, unauthorized

use or disruption. Paragraph 184(2)(e) generally applies to persons who manage the quality of service of a computer system or its protection.

12. Despite any cybersecurity authorization, the *CSE Act* imposes limitations on CSE activities. CSE must not direct any of its activities at a Canadian or any person in Canada or infringe the *Canadian Charter of Rights and Freedoms* (*Charter*) (s 22(1), *CSE Act*). However, in conducting activities pursuant to an authorization, it is lawful for CSE to incidentally acquire information relating to a Canadian or a person in Canada (s 23(4), *CSE Act*). Incidentally means that the information acquired was not itself deliberately sought (s 23(5), *CSE Act*).

13. When CSE acquires personal information related to Canadians or persons in Canada, strict legislative and policy measures must be followed to use, analyse and retain this information. Indeed, CSE is required 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 (s 24, *CSE Act*).

14. 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 letter to the Intelligence Commissioner from the Minister;
    b) The Authorization;
    c) The Briefing Note from the Chief to the Minister;
    d) The Chief's Application, containing fifteen annexes including but not limited to:
        i. The letters of request from the three non-federal entities;
        ii. Two ministerial orders;
        iii. Retention and Disposition Table;
        iv. Key outcomes from the period of validity of the 2023–24 Authorization (Outcomes Report);
        v. The Mission Policy Suite for Cybersecurity (MPS) approved February 28, 2022; and
    e) Briefing Deck – Overview of the Activities.

III. STANDARD OF REVIEW

15. Pursuant to section 12 of the *IC Act*, the Intelligence Commissioner conducts a quasi-judicial review of the conclusions on the basis of which a ministerial authorization is made to determine whether they are reasonable.

16. The Intelligence Commissioner's jurisprudence establishes that the reasonableness standard, as applied to judicial reviews of administrative action, applies to my review.

17. 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 (*Mason v Canada (Citizenship and Immigration)*, 2023 SCC 21 at para 79). 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.

18. Relevant factual and legal constraints can include the governing statutory scheme, the impact of the decision, and principles of statutory interpretation. Indeed, to understand what is reasonable, it is necessary to take into consideration the context in which the decision under review was made as well as the context in which it is being reviewed. It is therefore necessary to understand the role of the Intelligence Commissioner, which is an integral part of the statutory scheme set out in the *IC* and *CSE Acts*.

19. A review of the *IC* and *CSE Acts*, as well as the legislative debates, shows that Parliament created the role of the Intelligence Commissioner as an independent mechanism to ensure that government action taken for the purpose of national security and intelligence was properly balanced with respect for the rule of law and the rights and freedoms of Canadians. To maintain that balance, I consider that Parliament created my role as a gatekeeper. While reviewing the Minister's conclusions, I am to carefully examine whether the important

privacy and other interests of Canadians and persons in Canada were appropriately considered and weighed as well as to ensure that the rule of law is fully respected.

20. When the Intelligence Commissioner is satisfied (*convaincu* in French) that the Minister's conclusions at issue are reasonable, he "must approve" the authorization (s 20(1)(a), *IC Act*). Conversely, where unreasonable, the Intelligence Commissioner "must not approve" the authorization (s 20(1)(b), *IC Act*).

IV. ANALYSIS

21. The Chief submitted a written Application for Cybersecurity Activities on Non-Federal Infrastructures (Application) to the Minister requesting authorization to carry out activities to help protect the systems of three non-federal entities of importance to the Government of Canada. The Application constitutes a request for a renewal of the ministerial authorization I approved in Decision 2200-B-2023-06. The Authorization does not set out any new activities as compared to last year's authorization.

22. Pursuant to past ministerial authorizations, sensors – software that aims to detect malicious cyber activity – have been deployed on the systems belonging to GNWT […], and on the systems belonging to YG […] and GNT […]. The sensors enable CSE to securely acquire information from the systems to identify malicious cyber activity. More specifically, the sensors consist of […] The Application describes why CSE seeks to continue to carry out theses cybersecurity activities on the systems belonging to the three territorial governments.

23. A description of the factual context leading to the past authorizations as well as additional details about the activities set out in the Authorization can be found in the classified annex to this decision (Annex A). I am including this information in an annex for two reasons. First, it will prevent the redaction of a significant portion of this decision, thereby rendering its public version easier to read. Second, it will ensure that the nature of the facts that were

before me, which would otherwise only be available in the record, are included in the decision.

24. Annexes XIII, XIV and XV of the record list the departments and agencies part of the territorial governments that use the non-federal entities' systems and would therefore be eligible to receive CSE's cybersecurity services pursuant to the Authorization.

25. Based on the facts presented in the Application submitted by the Chief on October 7, 2024, the Minister concluded that he had 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. In accordance with section 14 of the *IC Act*, I must review whether the Minister's conclusions on the basis of which the Authorization was issued are reasonable.

A. Subsection 34(1) of the *CSE Act* – Determining whether the activities are reasonable and proportionate

i. The meaning of reasonable and proportionate

26. To issue a cybersecurity authorization, the Minister must conclude that "there are reasonable grounds to believe that any activity (*activité en cause* in French) that would be authorized by it is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities" (s 34(1), *CSE Act*).

27. The Minister must arrive at his conclusion by applying his understanding of what the reasonable and the proportionate thresholds entail. Determining whether an activity is reasonable and proportionate is a contextual exercise and the Minister may consider a number of factors. The Intelligence Commissioner must determine whether the Minister's conclusions, which include his understanding of the thresholds, are "reasonable" by applying the reasonableness standard of review, explained previously.

ii. Reviewing the Minister's conclusions that the activities are reasonable

28. The Minister concluded at paragraph 49 of the Authorization that he had reasonable grounds to believe that the activities authorized in the Authorization are reasonable given the objective of helping to protect the systems of the non-federal entities, and potentially protect

federal systems and other systems of importance, from mischief, unauthorized use, or disruption.

29. To conduct its cyber security activities, the record indicates that CSE "must" acquire […] Given that the systems are located in Canada, at least some of this information will be related to Canadians or persons in Canada. However, I am satisfied that the cybersecurity activities set out in the Authorization are aimed at identifying and responding to cyber threats and not directed at Canadians or persons in Canada. They respect the legislative prohibition against deliberately seeking information relating to, and directing activities at, Canadians or persons in Canada (ss 22(1), 23(3), *CSE Act*).

30. Similar to last year's decision with respect to these non-federal entities, the Minister provides two main reasons to justify that continuing the cybersecurity activities is reasonable: 1) the activities for which the authorization is sought are effective; and 2) CSE's involvement in the cybersecurity response is required given the key role played by the non-federal entities in governing the Arctic, a strategic region for Canada.

31. First, the activities set out in the Authorization are effective and complement the non-federal entities' other cybersecurity activities. The Minister explains that the sophistication of cyber threats render them difficult to identify. CSE's cybersecurity solutions provide a separate and additional layer of defence to detect potential compromises, which could have devastating consequences such as loss of information or system functionality.

32. The record includes information on the effectiveness of the activities. For example, the Minister explains that over the course of the previous authorization, CSE used information collected by CSE's sensors deployed on the GNWT's systems to prepare and share with GNWT […] reports of malicious activities or vulnerabilities. In Decision 2200-B-2024-06, I stated that the mere existence of reports shared with the non-federal entity of a "vulnerability" does not necessarily constitute evidence supporting the reasonableness of CSE's continued presence on the non-federal system. The existence of a report does not speak to the impact of the vulnerability on the system. In the record before me, I am satisfied that the record provides sufficient details about the information contained in the report, which

in turn supports the Minister's conclusion that CSE's activities are effective. Although the record indicates that all three territories have experienced malicious cyber activity in the past, […].

33. The record also indicates that GNWT has implemented measures based on the advice and guidance provided by CSE. I note that last year's record set out four recommendations that GNWT was in the process of implementing. There is no update on whether these recommendations have been implemented. Further, the record indicates that GNWT is in the process of implementing one recommendation made by CSE, which is different than the four recommendations described last year. Where an authorization is sought for the same activities as a prior year, I would expect that the record would allow the Minister to understand the progress – if any – that has been accomplished.

34. Based on information in the record, I agree that CSE's activities have been and continue to be effective and strengthen each territorial government's cybersecurity posture.

35. The second ground for which CSE's activities are reasonable is that the non-federal entities in question deliver, with limited resources, critical public services to Canadians. As explained by the Minister, they hold sensitive personal information and play a central role in governing Canada's Arctic, which is of significant geopolitical interest to adversaries.

36. The Minister further supports his conclusion by relying on the service-provision role of the non-federal entities, and the geopolitical importance of the area where the non-federal entities are located. With the increased access to the Internet, Canada's Arctic Region is subject to more cyber threat activity and must be protected.

37. The Minister explains that the current state of the three non-federal entities' cybersecurity posture is not sufficient to identify and combat […]. Given the importance of the Arctic, CSE's support is required.

38. While the record does not explicitly state that CSE's cybersecurity solutions are intended to be permanent, there is no information suggesting that CSE's support will eventually no longer be necessary. This seems consistent with CSE's Annual Report 2023–24 which indicates that for securing the North, CSE intends to deploy its cybersecurity solutions "on an ongoing basis".

39. As I mentioned in Decision 2200-B-2024-06, the *CSE Act* does not explicitly limit the period of time CSE can assist a non-federal entity, subject to obtaining a ministerial authorization every year. In that Decision, I accepted the Minister's rationale that CSE's presence was still required because certain CSE recommendations central to ensuring a robust cybersecurity posture had not yet been implemented. In this Authorization, the rationale does not rest on outstanding CSE recommendations or the rebuilding and strengthening of the system following a cyber incident. Although the three non-federal entities have experienced malicious cyber activity in the past, the Minister does not rely on malicious cyber activity currently on the systems to justify his conclusions.

40. Rather, the Minister's conclusions largely rest on the strategic importance of the Arctic. Indeed, as an example, the record indicates that the continuing deployment of CSE cybersecurity solutions "will foster long term resilience to cyber threat actors and provide significant strategic benefit to Canada and its allies." In this sense, the Authorization is preventative or proactive rather than reactionary. I address a specific issue in relation to this in my remarks.

41. I accept the Minister's rationale that CSE's continued presence is necessary to ensure that the territorial governments' systems are properly protected from cyber threats. My conclusion takes into account the effectiveness of CSE's sensors, the current state of each territorial government's cybersecurity posture, as well as the information in the record about the importance of the Arctic to the Canadian national interest. As a result I find reasonable the Minister's conclusions that the activities set out in the Authorization are reasonable.

iii. Reviewing the Minister's conclusions that the activities are proportionate

42. The Minister concluded at paragraph 52 of the Authorization that he had reasonable grounds to believe the activities authorized are "proportionate given the manner in which they are conducted".

43. I am satisfied that the Minister's conclusions in this regard are reasonable. He recognizes that the proposed cybersecurity activities can lead to acquiring large volumes of information in order to identify cyber threats. Although there may be privacy interests in some of the information, the Minister explains that CSE is interested in any anomalous behaviour related to the information, rather than its content.

44. The Minister puts forward measures and controls to show that the activities are proportionate. The Minister sets out seven internal measures and controls applied by CSE:

a) no unassessed information is retained for longer than […] from the date upon which it is acquired;
b) CSE retains less than 1% of the total amount of data initially acquired through cybersecurity activities;
c) most of the analysis and mitigation is done through automated processes that limit employees' exposure to the unassessed information and all information is protected in accordance with CSE's operational policy;
d) every search performed on the acquired unassessed information is auditable to comply with the MPS;
e) access to information acquired under this Authorization is restricted to employees that have a need-to-know for the purpose of their work. Prior to accessing unassessed information, employees must pass an annual graded test, covering the legal and policy requirements that apply to handling this type of information;
f) all cybersecurity technologies are reviewed for legal and policy compliance; and,
g) the same conditions apply to information used by CSE for the purposes of identifying, isolating, preventing, or mitigating harm to federal systems and other systems of importance.

45. The Minister largely relies on the measures applied to information after it has been acquired to support his conclusion on proportionality. The Minister confirms that CSE's cybersecurity activities acquire a broad range of information in order to better protect federal and non-federal systems. This includes access to a large amount of information such as […] in which Canadians and persons in Canada may have a reasonable expectation of privacy.

46. I recognize that the Minister did not have the benefit of my comments made in Decision 2200-B-2024-06. As a result, I reiterate that the record does not indicate the total amount information that was acquired in the past. While 1% may seem minimal, CSE access to the non-federal system is extensive. The Minister and the Intelligence Commissioner would benefit from additional context in relation to the total volume of data collected to better ascertain the proportionality of the activities carried out by CSE and how they minimally impair the privacy of Canadians and persons in Canada.

47. The Outcomes Report indicates that during the previous authorization, CSE retained 384 "items" acquired from the non-federal entities' systems – which amounts to less than 1% of the total data acquired. I consider this precise accounting of retained information progress for purposes of ministerial accountability as well as for purposes of transparency. As noted in Decision 2200-B-2024-06, additional context to understand what constitutes an "item" would be helpful to the Minister and myself.

48. In addition, the Outcomes Report provides describes measures that GNWT has completed throughout the period of validity of the 2023–24 Authorization and the CSE recommendation being implemented. However, there is no information as to when the outstanding recommendations are expected to be completed. The length of time required by CSE to achieve this objective may be a factor to be considered when reviewing whether the activities are proportionate and I expect it will be addressed in future applications.

49. The Minister explains that access to information that contains a Canadian privacy interest 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. This limits access to information that may contain a Canadian privacy interest.

50. I can trace the Minister's rationale for relying on these measures. He concludes that the proposed activities justify any potential impairment of Canadian privacy interests. He also explains how the activities sought to achieve a reasonable balance between them. I am satisfied that the interests of Canadians and persons in Canada were considered and the balancing conducted is reasonable.

51. As for the Acts of Parliament that have the potential to be contravened, 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. Since CSE has obtained this consent, the possible contraventions of Canadian laws are remote. In the event an Act of Parliament is breached, the impact of the breach will be limited and if an Act of Parliament that is not listed in the Chief's application is contravened, the Chief will inform both the Minister and the Intelligence Commissioner.

52. 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.

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

53. 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))

54. Information is retained in accordance with requirements set out in CSE policies and governed by a retention schedule for the different types of information that may be acquired. The Minister explains that CSE's information management and record disposition requirements set out in CSE policies comply with the *Privacy Act*, RCS, 1985, c P-21 and the *Library and Archives of Canada Act*, SC 2004, c 11. As noted by the Chief, the non-federal entities in question may, at any time, request that CSE delete the information it has acquired from or through their systems.

55. CSE does not know in advance of collection what information will be helpful in identifying malicious activity. As a result, it acquires a large volume of information. CSE processes this information, mostly through automated means that limit CSE employee's exposure to the information contained in a file. The use of automated processes ensures that employees only interact with information required to develop detection and mitigation measures, or to determine retention and handling processes. This process may identify some of the information as "necessary" or "essential". All other information is considered to be unassessed information, even though it has gone through the automated processes.

56. The retention period for unassessed information is […], while information assessed as being "necessary" or "essential" to help protect the non-federal systems, or federal systems and designated systems of importance, can be retained "indefinitely or until the information is no longer useful for these purposes."

57. The Minister's rationale for the retention period for unassessed information is straightforward. He explains that there is often a period of time between when a compromise begins and when it is first identified. Once an indicator of compromise is identified, the effectiveness of CSE's activities depend on being able to examine unassessed information to identify any previously undetected compromises. CSE assesses that a […] retention

period for unassessed information is sufficient to allow it 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 defences that can also be used not only for the non-federal system, but also for other systems of importance and for federal systems.

58. After the […] period, unassessed information will automatically be deleted unless deemed "necessary" or "essential" to help protect the non-federal system, or federal systems and designated systems of importance. Further, unassessed information cannot be shared beyond CSE. In the Application, the Chief confirms that the three non-federal entities are aware and agree on the use of this information.

59. As explained in the record, the "necessary" criterion applies to information that does not relate to a Canadian or a person in Canada whereas the "essential" criterion applies to information that relates to a 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. By its nature, information deemed "necessary" does not contain any elements relating to Canadians or persons in Canada and is therefore less sensitive than information determined to be "essential". The purpose is to assist in developing detection and prevention analytics and further strengthen the cyber defence ecosystem.

60. Information about Canadians and persons in Canada is considered "essential" when without it, 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.

61. Information that is determined to be necessary or essential to identify, isolate, prevent, or mitigate harm to the non-federal system is retained in accordance with section 11.2 of the

MPS. CSE's internal compliance program circulates quarterly reminders to cybersecurity analysts to ensure that data retained in a corporate repository that has not been assessed as necessary or essential be deleted within […] of acquisition. Further, operational managers must revalidate on a quarterly basis whether the information remains essential. Information that is no longer essential must be deleted.

62. I am of the view that the Minister reasonably explains the rationale for retaining information for the length of time needed – […] for unassessed information and until no longer useful for information that is "necessary" or "essential". These retention periods allow CSE to effectively conduct cybersecurity activities.

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. CSE's cybersecurity activities are effective only with the acquisition of information. The Minister explains that threat actors deliberately […]. To effectively mitigate the sophisticated cyber threats described in this matter and to prevent potential cyber threats, CSE must acquire a vast range of information, which can then be assessed to identify malicious activity. The information includes […].

64. There is nothing in the record to suggest that CSE can achieve the same cybersecurity outcomes by using different cybersecurity activities that acquire less information, specifically information related to Canadians.

65. The Minister's conclusions provide 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. Further use, analysis, retention, or disclosure of information acquired under a cybersecurity authorization is subject to restrictions and conditions imposed by clients or disclosing entities.

66. For these reasons, I am satisfied that the Minister's conclusions are reasonable that he has reasonable grounds to believe that the acquisition of the information is necessary to identify, isolate, prevent or mitigate harm to the non-federal systems.

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))

67. 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.

68. The Minister sets out the CSE policy requirements to support his conclusion that all information relating to a Canadian or a person in Canada that is incidentally acquired will only be retained if it is assessed to be essential to identify, isolate, or prevent harm to the non-federal entities' systems.

69. With respect to the retention of Canadian-related information, all information acquired is handled in accordance with section 8 of the MPS. Specifically, section 8.2.2 indicates that the "essentiality test" is conducted by accredited and trained CSE employees either through manual or automated processes. Essentiality rationales must be recorded by employees. Proceeding this way limits access to the content of information that is highly sensitive to Canadians and exposure to the unassessed information. In my view, these measures contribute to compliance with the legislative obligation under section 24 of the *CSE Act* and supports the Minister's conclusions.

70. Access to unassessed information is strictly controlled and limited to those authorized to conduct or support cybersecurity activities (s 10.2, MPS). The list of personnel with approved access to unassessed information is tracked for accountability purposes.

71. Pursuant to section 24 of the MPS, measures are in place to protect the privacy of Canadians and persons in Canada when information related to them is disclosed. For example, personal

information may be suppressed so that reporting does not identify the identity of an individual. When information related to a Canadian is disclosed, the MPS sets out the required disclosure approval levels and requires that they be documented.

72. The Minister's conclusions and the record explain how information related to Canadians or persons in Canada can be disclosed, which 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 a computer system or network 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. To receive information disclosed by CSE that relates to Canadians or persons in Canada, the information must be necessary to help protect non-federal and federal systems.

73. In the letters of request to CSE, each non-federal entity asked that all personal or proprietary information that may be collected and retained be obfuscated before it is shared. Further, any information that is not relevant to CSE's mandate must be deleted in accordance with CSE's retention schedule. It is therefore my understanding that any disclosure of information acquired under the Authorization will first have to satisfy this direction.

74. The MPS sets out elaborate policies to control and safeguard information related to Canadians and persons in Canada 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.

75. In addition, there is reporting on the retention, use and disclosure of Canadian-related information in the section 52 End of Authorization Report provided to the Minister, a copy of which is provided to the Intelligence Commissioner. Reporting adds an additional layer of accountability. This reporting has improved since the initial cybersecurity authorization for

GNWT was approved in 2022 and now includes greater detail on the volume and nature of information that is retained.

76. Given the above, I am satisfied that the Minister's conclusion is reasonable that he has reasonable grounds to believe that information related to Canadians or persons in Canada will only be used, analysed or retained if essential to identify, isolate, prevent or mitigate harm to non-federal entity's system.

V. REMARKS

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

78. I note that section 52 End of Authorization Report in relation to the 2022 ministerial authorization raised a non-compliance incident that was not referred to in the record. The incident related to a request made by the Department of Justice for CSE to retain, for litigation purposes, information that was collected under the authorization and that should have been deleted within a specific time period. The same incident was described in Decision 2200-B-2024-06 where I found that while it did not affect the validity of the authorization under review, the Minister should have been provided with all relevant information. The same remark applies in the context of this Authorization.

A. Additional information to the Minister concerning legal use of information by non-federal entity

79. As I have mentioned in past decisions, the *CSE Act* does not explicitly require the Minister to consider whether the non-federal entity has the legal authority to collect, use and retain personal information of Canadians or persons in Canada for cybersecurity purposes. For this reason, in Decision 2200-B-2024-06, I made a remark that the Minister should be able to easily understand that the non-federal entity has the original jurisdiction to collect the information and that there is a legal foundation for its effective sharing with CSE for its use for cybersecurity purposes.

80. Non-federal entities should only allow CSE to carry out activities that they could legally carry out themselves. The obvious concern is the hypothetical situation where the Minister issues an authorization allowing CSE to conduct cybersecurity activities that collect information related to Canadians or persons in Canada on behalf of the non-federal entity where this entity does not itself have the legal authority to collect or use this information for cybersecurity purposes. In my view, providing the Minister with that assurance strengthens the ministerial authorization regime.

81. I recognize that CSE and the Minister did not yet have the benefit of Decision 2200-B-2024-06 when the Authorization was issued. In the current Authorization, the Minister explains that the non-federal entities are responsible for providing critical programs and services to residents, businesses, visitors as well as government departments, agencies and crown corporations. To exercise these responsibilities, they hold information of importance, including personal information of Canadians and persons in Canada. For the benefit of future cybersecurity authorizations, I recommend that the link between the entities' legal authority to collect the information and its use for cybersecurity purposes is more clearly outlined in the record for the Minister. This may include elements related to the consent of users of the systems belonging to the non-federal entities.

B. Reasonableness of activities in preventative contexts

82. As mentioned in my reasons, CSE's continued presence has a preventative, or proactive, objective. However, I wish to be clear that my conclusions do not entail that a designation as a non-federal entity of importance to the Government of Canada, in itself, is sufficient to support the Minister's conclusions that a cybersecurity authorization would be reasonable if deployed for a preventative objective.

83. I found reasonable the Minister's conclusions by relying on his rationale concerning the strategic importance of the Arctic to the Government of Canada as well as on evidence of malicious activity. This importance and the nature of the malicious activity was robustly explained and supported in the record.

84. A cybersecurity authorization pursuant to section 27(2) of the *CSE Act* is issued for the purpose of helping to protect a non-federal entity's system from mischief, unauthorized use or disruption. In contexts where cybersecurity activities are carried out for preventative or proactive purposes, I am of the view that the Minister nevertheless needs to establish a factual basis for CSE's assistance.

VI. CONCLUSIONS

85. 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 79 of the Authorization are reasonable.

86. I therefore approve the Minister's Cybersecurity Authorization for Activities on Non-Federal Infrastructures dated October 22, 2024, pursuant to paragraph 20(1)(a) of the *IC Act*.

87. 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.

88. 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 15, 2024

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner