~~**PROTECTED B**~~

File: 2200-B-2024-06

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*

OCTOBER 22, 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 a non-federal entity.

2. On […], 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 […] (Authorization). This is the fourth consecutive year the Minister issues a cybersecurity authorization in relation to this non-federal entity.

3. On […] 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 62 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 a 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 Authorization;
    b) Briefing Note from the Chief to the Minister;
    c) The Chief's Application, containing eight annexes including but not limited to:
        i. The letter of request from the non-federal entity;
        ii. Two ministerial orders;
        iii. Retention and Disposition Table;
        iv. List of recommendations from CSE to the non-federal entity;
        v. Key outcomes from the period of validity of the 2023–24 Authorization (Outcomes Report);
        vi. The Mission Policy Suite for Cybersecurity (MPS) approved February 28, 2022; and
    d) 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 a Cybersecurity Activities on Non-Federal Infrastructures (Application) to the Minister requesting authorization to carry out activities to help protect the system of the non-federal entity of importance to the Government of Canada. The Application describes the nature and objectives of the cybersecurity activities that will be conducted by CSE. In sum, […] acquired through the system and analysed by CSE to identify, isolate, prevent and mitigate harm to the entity's system.

22. A description of the non-federal entity as well as the activities set out in the Authorization can be found in the 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.

23. Based on the facts presented in the Application submitted by the Chief of CSE on […], 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*

24. 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*).

25. 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*

26. The Minister concluded at paragraph 33 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 system of the non-federal entity, and potentially protect federal systems and other systems of importance, from mischief, unauthorized use, or disruption.

27. The activities set out in the Authorization would permit CSE to access a system that is located in Canada. The Minister explains that these cybersecurity activities may lead to the collection and possible retention of information in which Canadians or persons in Canada have a reasonable expectation of privacy. Given the context of the Authorization and the description of information that CSE must acquire to effectively carry out its activities, I know that CSE collects such information. Indeed, the record indicates that CSE "must" acquire […].

28. Nevertheless, in issuing a cybersecurity authorization, the Minister implicitly recognizes that any information related to Canadians or persons in Canada acquired through the activities is

not deliberately sought, but rather incidentally acquired – and therefore does not contravene the legislative prohibition against deliberately seeking information relating to, and directing activities at, Canadians or persons in Canada (s 22(1), *CSE Act*). Indeed, subsection 23(3) of the *CSE Act* clarifies that despite the prohibition on directing activities at Canadians or persons in Canada, CSE may carry out cybersecurity activities to protect systems and mitigate any harm – which includes systems located in Canada. I am satisfied that the cybersecurity activities set out in the Authorization are not directed at Canadians or persons in Canada.

29. Similar to last year's decision with respect to this non-federal entity (Decision 2200-B-2023-05), the Minister provides two main reasons to justify that continuing the cybersecurity activities is reasonable. First, the activities set out in the Authorization are effective and complement the non-federal entity's other cybersecurity activities. The Minister explains that the activities allow CSE to identify and better understand malicious cyber activity or other indicators of compromise in order to advise the non-federal entity on how to protect its system and to conduct mitigation actions. The information collected can also help protect federal systems and other systems of importance.

30. Secondly, [...], CSE's cybersecurity activities are necessary to continue to repair and rebuild the information infrastructure and to protect it against other cyber threats. The Minister explains that although the non-federal entity has made substantial progress with the implementation of CSE's recommendations to improve its cybersecurity posture, there is continued presence of malicious activity on the system and some of the key recommendations remain to be completed.

31. To underscore the ongoing threat to the non-federal entity's system, the Minister makes reference to three reports shared with the non-federal entity in the last year – [...]. He also provides detail on a specific threat actor that has targeted entities operating in the same sector of importance to the Government of Canada as the non-federal entity.

32. In summary, according to the Minister, the sensitivity and importance of the information held by the non-federal entity, the previous compromise it experienced and the continued evidence of malicious activity and vulnerabilities specified in the three reports shared with the entity during the period covered by the previous authorization, are grounds to find that the activities authorized in the Authorization are reasonable.

33. I have no difficulty finding reasonable the Minister's conclusion that the cybersecurity activities set out in the Authorization are effective. I also accept that the information in the record supports the conclusion that the non-federal entity cybersecurity posture still requires CSE's support. Indeed, in the first two authorizations with respect to this non-federal entity, the reasonableness of the Minister's conclusions were supported by the cyberattacks – which were detailed in the record – and the entity's inability to counter typical or expected cyber threats. CSE's cybersecurity activities were required to detect the threats and mitigate them. In last year's authorization, the Minister confirmed that […], the non-federal entity's cybersecurity posture at that time was still insufficiently developed to counter cyber threats. Relying on the information in the record, this underlying rationale for which the Minister's conclusions in past authorizations were reasonable – an insufficiently robust cybersecurity posture – continues to apply in this Authorization.

34. Nevertheless, I have concerns regarding certain elements of the Minister's conclusions, in particular with respect to relying on the presence of ongoing threats and on outstanding CSE recommendations to justify CSE's continued presence on the system.

35. With respect to the ongoing threats, the Minister relies on the three reports shared with the non-federal entity as evidence there is continued malicious activity and vulnerabilities. There is very little information in the record about this malicious activity and these vulnerabilities and some of the information is unclear. The Minister and the Chief simply state that two reports concerned "vulnerabilities". The impact of these vulnerabilities on the system is not discussed. The Minister and the Chief state that a third report involved […] but the Outcomes Report states that the third report was […]. […] It is unclear whether these refer to the same vulnerability.

36. The existence of reports shared with the non-federal entity of a "vulnerability" do 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. The record does not explain whether the "vulnerability" is serious or is the result of an inconsequential oversight. Similarly, the record does not explain why […] threatens the system. To rely on the impact of the vulnerability, as does the Minister, the record must reflect the nature of that impact. If the Minister's conclusions rely on the continued presence of vulnerabilities, the Chief's application should robustly reflect the link between the vulnerabilities included in the reports and the impact for the system.

37. As I have stated in past decisions, the Minister justifiably relies on CSE's technical expertise to support his conclusions. Nevertheless, when relying on this expertise, the Minister's conclusions should demonstrate an understanding of the implications of CSE's technical findings.

38. My concern regarding the reliance on the outstanding recommendations also relates to a lack of clarity in the record. In last year's authorization, the Minister justified the reasonableness of his conclusions partly on the existence of […] outstanding recommendations anticipated to be completed in 2024.

39. Based on the Minister's conclusions in last year's authorization, it was my understanding that following the completion of the […] outstanding recommendations – which he anticipated would be implemented in 2024 – CSE's support would no longer be required. Indeed, as I wrote in last year's decision: "This should then allow the non-federal entity to counter typical or expected cyber threats." (para 42)

40. Yet, as explained by the Minister and the Chief in this Authorization, […] key recommendations still remain to be completed. Further, […] current outstanding key recommendations are different than last year's […] outstanding recommendations (as seen in Annex A). As the Minister relies on the recommendations to conclude that CSE's activities are reasonable, the record should clearly and consistently indicate which key

recommendations remain to be implemented, as well as the implications of outstanding recommendations on the entity's cybersecurity posture.

41. On this point, in last year's decision, I noted that the record could have provided additional details on the relationship between the [...] outstanding recommendations and the state of the non-federal entity's system. This was addressed in the record before me. The Minister explains why, without the final recommendations in place, the non-federal entity's system remains vulnerable. I find this conclusion by the Minister reasonable.

42. Ultimately, despite my concerns, the Minister's conclusion that the system remains vulnerable, along with the fact that CSE's cybersecurity activities are effective, support the conclusions that the proposed activities are reasonable. The Minister's conclusions are reasonable because CSE's cybersecurity activities are necessary while the entity's cybersecurity posture is still being developed. There is a rational link between the cybersecurity activities and the protection of the non-federal entity's system.

43. In my remarks at the end of the decision, I return to some implications of renewing a cybersecurity authorization for an extended period of time.

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

44. The Minister concluded at paragraph 35 of the Authorization that he had reasonable grounds to believe the activities authorized are "proportionate given the manner in which they are conducted".

45. I am satisfied that the Minister's conclusions in this regard are reasonable with respect to the authorized activities described at paragraph 62 of the Authorization. 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.

46. The Minister puts forward measures and controls to show that the activities are proportionate. I note that the measures mirror those included in the authorization that was the subject of my

recent Decision 2200-B-2024-05 with respect to a non-federal entity. 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.

47. 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. The information retained is less than 1% of the total amount of data initially acquired. I note 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.

48. The Outcomes Report indicates that during the previous authorization, CSE retained 40 "items" acquired from the non-federal entity's system – which is less than 1% of the total data acquired. This is the first authorization in which there is a precise accounting of retained information. I appreciate and commend CSE for giving effect to past remarks by providing the Minister and myself with additional information on the real world impacts of the authorizations. I consider this progress for purposes of ministerial accountability as well as for purposes of transparency. I would however note that additional context to understand what constitutes an "item" would be helpful to the Minister and myself.

49. In the Authorization, the Minister explains some of the progress that has been achieved implementing CSE's recommendations and elements that remain outstanding. The length of time taken is largely attributable to the procurement process. I find this to be a reasonable explanation. However, the record does not provide a timeline as to when the outstanding recommendations may be completed or when CSE's cybersecurity activities will no longer be required. 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 further address this issue in my remarks.

50. 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. While the Minister was cognizant of the privacy interests at issue, I reiterate my comment made in Decision 2200-B-2024-05 concerning a non-federal entity that his conclusions could provide more specificity about the likelihood that these may be breached – and laid out the measures in place to protect them.

51. 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.

52. 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 a system 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. I return to the issue of consent at paragraph 72 of this decision. 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.

53. 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

54. 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))*

55. Information is retained in accordance with requirements set out in CSE policies and governed by a retention schedule. 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.

56. The Minister explains that CSE's cybersecurity activities are [...]. As it not possible for CSE to predetermine what information will be helpful in identifying malicious activity, it acquires a large volume of unassessed information [...].

57. In addition, CSE processes the unassessed 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.

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

59. As explained by the Minister, there is often a period of time between when a compromise begins and when it is first identified. Therefore, the effectiveness of CSE's activities depend on being able to cross-reference and analyse multiple sources of information already acquired, including identified indicators of compromise. A [...] retention period for unassessed information allows CSE to reach back to the origins of an event or examine its evolution over time. New vulnerabilities are discovered on an ongoing basis. 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.

60. 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. 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. Unassessed information cannot be shared beyond CSE. In the Application, the

Chief confirms that the non-federal entity in question is aware and agrees on the use of this information.

61. As indicated 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, this information 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.

62. 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.

63. 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.

64. 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. I am also satisfied that the important restrictions placed on CSE employees on accessing unassessed information, the quarterly reminders they

receive to check corporate repositories and those provided to operational managers to confirm that the retention of Canadian-related information remains "essential" support the reasonableness of the Minister's conclusions.

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

65. 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 [...].

66. 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. 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.

67. 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 system.

*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))*

68. 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.

69. The Minister reiterates that information relating to a Canadian or a person in Canada can only be retained if it is assessed to be essential, defined by CSE as meaning that without the information, CSE would be unable to identify, isolate, or prevent harm to the non-federal entity's system. As indicated in section 8.2.2 of the MPS, 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. As outlined in section 24 of the MPS, privacy 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. These approvals must be documented.

71. 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.

72. In its letter of request to CSE, the 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. I reiterate a remark made in Decision 2200-B-2024-05 with respect to a non-federal entity that the issues relating to the collection and use of personal information and to consent of persons whose information may be acquired should remain central and be reflected in cybersecurity authorizations. Indeed, information in which there is a reasonable expectation of privacy shared on a non-federal entity's system may end up being retained by CSE, a Government of Canada agency for cybersecurity purposes. 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.

73. 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.

74. Canadian private communications, […] that are incidentally acquired, are accounted for in the End of Authorization Report provided to the Minister, a copy of which is provided to the Intelligence Commissioner (s 52, *CSE Act*). The latest report shows that no private communications were acquired, retained or shared.

75. 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.

76. I note that in a remark in last year's decision with respect to this non-federal entity, I indicated that I expected CSE to provide the Minister and myself with greater understanding of the nature, frequency and volume of the retention of information where Canadian privacy interests are involved. As previously mentioned, this has been addressed in the Outcomes Report – with the caveat of providing additional context on what constitutes an "item" and

the total amount of data retained. Based on the nature of the type of Canadian-related information retained described in the Outcomes Report, it can be readily understood how its retention is essential. When the essentiality of retaining the Canadian-related information may not be evident, I remain of the view that the record should explain why retention of that the type of information is essential – especially when, as is the case here, some information is retained as being essential but is not included in reports to the non-federal entity.

## V. REMARKS

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

### A. Renewing cybersecurity authorizations for extended periods of time

78. The Minister indicates that cyber-related compromises are becoming increasingly difficult to detect, especially without CSE cybersecurity activities. Indeed, he writes that "[t]he commercially available safeguards put in place by [the non-federal entity] are not sufficient to identify and counter persistent and increasingly complex cyber threats." This raises the question of whether commercially available safeguards will ever be sufficient on their own. While last year's authorization recognized that there would be an eventual cessation of CSE's cybersecurity activities on the non-federal entity's system – at the time expected in 2024 – this year's record does not indicate when the outstanding recommendations might be completed, or suggest that once the recommendations are fully implemented, CSE's presence will no longer be required.

79. The *CSE Act* does not limit the period of time CSE can assist a non-federal entity. However, the rationale for CSE's continued presence reflected in the Minister's conclusions may have to change over time. I mention this because in the event that the cybersecurity authorization for this non-federal entity is renewed once the recommendations have been implemented – or there is no longer a reasonable explanation to account for the time it is taking to implement outstanding recommendations – the Minister's conclusions may have to evolve to meet the reasonableness standard that I must apply.

80. Cybersecurity authorizations are intrusive on privacy interests given the necessary collection of information in which Canadians have a reasonable expectation of privacy – even though the collection is ancillary to safeguarding the system. I consider the degree of intrusion even higher in the case of cybersecurity authorizations in support of non-federal entities because CSE – a Government of Canada agency – is collecting information it would otherwise not have access to. And of course, the intrusion is exacerbated the longer it lasts. It is therefore important that the rationale for continuing this ancillary collection over an extended period of time is sufficiently considered and justified in the Minister's conclusions.

**B. Compliance Incident**

81. In the 2022–23 End of Authorization Report summarizing the outcomes of the activities carried out under the 2022 ministerial authorization, a compliance incident is described. The Minister was informed that following a request by the Department of Justice (DOJ), CSE retained information for litigation purposes collected pursuant to the authorization that would otherwise have been deleted within a specific time period. CSE's internal compliance team, in collaboration with DOJ, conducted a study examining the retention of the information for litigation purposes. CSE is currently reviewing options to ensure compliance in handling this type of information. I am of the view that such exceptions with respect to handling information collected pursuant to an authorization should eventually be reflected in the conditions set out in authorization.

82. While the non-compliance does not raise the validity of any authorization I have previously approved, the compliance incident is not referenced in this record. I am of the view that the Minister, as the decision maker, should have had the information in the record before him to determine whether it was relevant to his conclusions. The End of Authorization Report is an important information tool for the Minister and myself to see how activities have been carried out. Indeed, the report is not only meant to satisfy a legal requirement. It provides details on the activities undertaken under the Authorization which could be relevant in issuing future authorizations. For these reasons, I am of the view that relevant information from the report should, when appropriate – for example when there has been a compliance issue and what has been done to rectify it – be included in the record before the Minister.

## VI. CONCLUSIONS

83. 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 62 of the Authorization are reasonable.

84. 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*.

85. 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.

86. 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.

87. In last year's decision, I wrote that I was of the view it would be beneficial to make public CSE's role in supporting and rebuilding the non-federal entity's cybersecurity posture – if the passage of time allowed for it. I reiterate the same view with respect to this Authorization.

October 22, 2024

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner