~~TOP SECRET//SI//CANADIAN EYES ONLY~~

File: 2200-B-2024-05

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

REASONS OF DECISION RENDERED ON [...]

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

[...]

Canada

TABLE OF CONTENTS

I. OVERVIEW

1. On [...], I issued a decision approving a Cybersecurity Authorization for Activities on Non-Federal Infrastructures (Authorization), with reasons to follow. The Minister of National Defence (Minister) had issued the Authorization on [...]. Based on my review of the record, I was satisfied that the Minister's conclusions, made under subsections 34(1) and (3) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*) and on the basis of which the Authorization was issued, were reasonable.

2. Considering the context in which the Authorization had been issued, I was of the view that it was in the public interest to render my decision on an expedited basis and that my reasons should not delay the implementation of the cybersecurity solutions by CSE on the non-federal infrastructures. I therefore issued my decision, a copy of which is attached as Annex A. The following are my reasons.

II. CONTEXT

3. CSE is the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance (s 15(1), *CSE Act*). As part of its mandate, it 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.

4. To effectively engage in cyber protection activities, CSE may have to contravene certain Canadian laws. In addition, when conducting cybersecurity activities to protect electronic systems, CSE may incidentally acquire communications and information that interfere with the reasonable expectation of privacy of Canadians or a persons in Canada.

5. Prior to proceeding with activities that may have these effects, CSE is required to obtain a cybersecurity authorization issued by the Minister and approved by the Intelligence Commissioner. Pursuant to the *Intelligence Commissioner Act*, SC 2019, c 13, s 50 (*IC Act*),

the Intelligence Commissioner approves the activities or classes of activities specified in the ministerial authorization if satisfied that the Minister's conclusions are reasonable.

6. CSE may obtain a ministerial authorization that allows it to access electronic information and information infrastructures belonging 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.

7. The *CSE Act* sets out the process for CSE to obtain a cybersecurity authorization. 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*). 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*). Subsections 34(1) and (3) of the *CSE Act* set out the statutory conditions under which the Minister may issue a cybersecurity authorization. The ministerial authorization is valid once approved by the Intelligence Commissioner (s 28(1), *CSE Act*). Only then can CSE carry out the authorized activities specified in the authorization.

8. 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.

9. 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*).

10. 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*).

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

    a) The Authorization;
    b) Briefing Note from the Chief of CSE to the Minister;
    c) The Chief of CSE's Application, containing eleven annexes including but not limited to:
        i. The letters of request from […] non-federal entities;
        ii. Two ministerial orders;
        iii. Retention and Disposition Table;
        iv. The Mission Policy Suite for Cybersecurity (MPS) approved February 28, 2022; and
    d) Briefing Deck – Overview of the Activities.

III. STANDARD OF REVIEW

12. 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.

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

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 (*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.

15. 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*.

16. 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.

17. 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

18. In accordance with section 14 of the *IC Act*, I must review whether the Minister's conclusions – made under subsections 34(1) and (3) of the *CSE Act* and on the basis of which the Authorization was issued under subsection 27(2) of the CSE Act – are reasonable.

19. The Chief submitted to the Minister a written Application for a Cybersecurity Authorization (Application) authorizing CSE to carry out activities to help protect the systems of the non-federal entities in question.

20. The non-federal entities are of importance to the Government of Canada, as defined in the *Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada* issued on August 25, 2020.

21. The Application describes the nature and objectives of the cybersecurity solutions that will be deployed by CSE. They include: […] and […]. As statutorily required, each non-federal entity separately requested CSE's assistance in writing.

22. A description of the non-federal entities, the context in which they requested CSE's support as well, as the activities set out in the Authorization can be found in the classified annex to this decision (Annex B). I am including this information in a classified 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 on reasonable grounds that the Authorization is necessary and that the conditions of subsections 34(1) and (3) of the *CSE Act* were met.

24. The Minister also recognized that without the Authorization, the activities referred to in paragraph 72 may be contrary to other Acts of Parliament, or may interfere with the reasonable expectation of privacy of a Canadian or a person in Canada.

25. Consequently, the Minister issued a one-year Authorization.

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 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 42 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. As in past cybersecurity authorizations, 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*). 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. Therefore, to respect the prohibition, the cybersecurity activities must be aimed at cyber threats and not be directed at Canadians. I am satisfied that the cybersecurity activities set out in the Authorization respect this statutory requirement.

30. The Minister explains that the cybersecurity activities set out in the Authorization may lead to the collection and possible retention of information for 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 am of the view that the likelihood of CSE collecting such information is almost certain. Indeed, the record indicates that CSE "must" acquire […].

31. Nevertheless, the Minister justifies the reasonableness of the activities by relying on the current cybersecurity posture of the non-federal entities, the role they play in the lives of Canadians and persons in Canada, and on the fact that the activities for which the authorization is sought are effective.

32. Indeed, the record describes in great detail the compromises and potential compromises to the systems belonging to the non-federal entities – information that I have included in Annex B. The Minister explains that it is increasingly difficult to detect cyber-related compromises and that they can have serious effects on the non-federal entities, resulting in the loss of information or system functionality. Based on the information provided by the Chief, the Minister concludes that the current state of […] non-federal entities' cybersecurity posture is not sufficient to identify and counter the sophisticated methods and capabilities deployed by advanced and persistent threat actors.

33. According to the Minister, the systems of the non-federal entities must be secure in light of the important role they play in the lives of Canadians and persons in Canada. I find that the description of the role played by the non-federal entities supports the Minister's conclusions that the activities set out in the Authorization are reasonable.

34. To provide better cybersecurity, the Minister explains that CSE's knowledge and cyber solutions allow for the capacity to respond to threats unknown to commercial providers of cybersecurity. Cyber threats can be difficult to detect and compromises can rapidly result in

the loss of information or system functionality. Given the context in which the Authorization was issued, CSE's [...] also supports the Minister's conclusion that the activities are effective and reasonable.

35. CSE's activities help the non-federal entities identify [...] indicators of compromise, remove the presence of identified threat actors, strengthen cybersecurity posture to protect against future threats [...]. In addition, the activities would allow CSE to identify, isolate and better understand malicious cyber activity or other indicators of compromise in order to advise the non-federal entities on how to prevent or mitigate their systems. Indeed, the activities allow CSE to recommend mitigation actions or conduct mitigation actions, with the consent of the non-federal entities.

36. I am of the view that the Minister's conclusions reflect that he considered and was satisfied with the link between the current needs of the non-federal entities and the proposed cybersecurity activities. There is a clear reasoned connection between CSE's proposed cybersecurity activities and their objective, which is to help protect non-federal systems. The Minister relies on the important role played by the non-federal entities, which I find supports his conclusion. Considering the nature of the objective and the information in the record with respect to the nature of the activities, I find reasonable the Minister's conclusion that the activities are reasonable.

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

37. The Minister also concluded at paragraph 45 of the Authorization that he had reasonable grounds to believe the activities authorized are "proportionate given the manner in which they are conducted."

38. I am satisfied that the Minister's conclusions in this regard are reasonable with respect to the authorized activities described at paragraph 72 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 the content.

39. 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 Decision 2200-B-2024-02 (Cybersecurity Authorization to Help Protect Federal Infrastructures). In that decision, I commented that the Minister cannot satisfy one statutory requirement – that the activities are proportionate (s 34(1), *CSE Act*) – by relying on satisfying separate statutory requirements found in subsection 34(3) of the *CSE Act* (information will only be acquired if necessary; information will not be retained longer than necessary; information will only retained if necessary; Canadian-related information will only be retained if essential).

40. To address my comment, the Minister specifies that the internal measures and controls are divided into two categories – "statutory requirements on which CSE relies to determine its internal measures and controls", and additional measures and controls that go beyond what the statute requires. Based on the Minister's conclusions, it is unclear to me what the difference is between statutory requirements used by CSE to determine internal measures, and simply having the statutory requirements as internal measures.

41. Nevertheless, the Minister sets out the following six internal measures and controls applied by CSE:

    a) CSE retains less than 1% of the total amount of data initially acquired through cybersecurity solutions;
    b) 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;
    c) every search performed on the acquired unassessed information is auditable to comply with the MPS;
    d) 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;

e) all cybersecurity technologies are reviewed for legal and policy compliance; and,

f) 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.

42. The Minister largely relies on the measures applied to information after it has been acquired to support his conclusion on proportionality. I can trace the Minister's rationale for relying on these measures. He recognizes that CSE must first acquire a large amount of information such as [...], in which Canadians and persons in Canada may – according to him – have a reasonable expectation of privacy. The measures that support his conclusions relating to proportionality will be applied after the information is acquired. Further, access to the 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. Should information that may contain a Canadian privacy interest be acquired and retained, access to it and its use would be limited.

43. The Minister was cognizant of the privacy interests at issue – although his conclusions could provide more specificity about the likelihood and extent that these may be breached – and laid out the measures in place to protect them. 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.

44. With regard to the rule of law, the Minister explains that there is a remote possibility that offences beyond those listed in the Application may be committed, and other Acts of Parliament may be contravened, depending on the circumstances of the activity undertaken. The Minister and I will be notified should CSE contravene an Act of Parliament not listed in the Application. Since the non-federal entities have provided their consent for CSE to access their systems, I am of the view that the potential offences are limited in number and in impact

on Canadians and persons in Canada. Should an Act of Parliament be breached, the impact of the breach will be limited.

45. The Minister's conclusions reflect his understanding of the privacy interests at issue and the measures in place to protect them. Taking into account the privacy interests, he concluded that the activities were nevertheless 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

46. When the Minister finds that the activities are reasonable and proportionate pursuant to subsection 34(1) of the *CSE Act*, the Minister may issue an 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

c) the measures in place ensure that information acquired under the authorization identified as relating 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))

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

48. As it not possible for CSE to determine what information will be helpful in identifying malicious activity, it acquires a large volume of information. The Minister explains that CSE

processes this information, mostly through automated means. 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.

49. The retention period for unassessed information is […]. The Minister explains that 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. The […] 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 defences that can also be used not only for non-federal systems but also for federal systems.

50. After the […] period, unassessed information will be automatically deleted unless deemed "necessary" or "essential" to help protect […] or federal systems and designated systems of importance. Section 10.2 of the MPS states that access to unassessed information ([…]) must be strictly controlled and limited to those authorized to conduct or support cybersecurity activities. The list of personnel with approved access to unassessed information is tracked for accountability purposes. Unassessed information cannot be shared beyond CSE. Further, the Chief states in the Application that each non-federal entity in this instance is aware and agrees on the use of this information.

51. 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, […], for the purpose of helping to protect non-federal systems. By its nature, this information does not contain any information 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 strengthens the cyber defence ecosystem.

52. 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 systems. 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.

53. Information that is determined to be necessary or essential to identify, isolate, prevent, or mitigate harm to federal systems may be retained "indefinitely or until the information is no longer useful for these purposes." This information will be tracked in accordance with section 11.2 of the MPS and operational managers must review the information on a quarterly basis to revalidate whether it remains essential. Information that is no longer essential must be deleted.

54. I am of the view that retaining information for the length of time needed allows CSE to develop the required cyber defence tools to keep pace with the rapidly evolving tradecraft of malware threat actors. This allows for better protection of non-federal systems as well as federal systems.

55. Given the important restrictions on accessing unassessed information, the example provided, and the quarterly reviews to confirm that the retention of Canadian-related information remains "essential", I find the Minister's conclusion regarding the […] assessment period reasonable. I also agree with the Minister's conclusion that information that is "necessary" or "essential" to identify, isolate, prevent, or mitigate harm to non-federal systems may be retained until it is no longer useful.

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

56. CSE's cybersecurity solutions are effective only with the acquisition of information. Consequently, CSE is granted extensive access to the non-federal systems to monitor for malicious activity and to acquire a range of information including information that does not reveal the existence of a cyber threat. In so doing, it may – and almost certainly will given that the non-federal entities are located in Canada – also incidentally acquire information that interferes with the reasonable expectation of privacy of Canadians and persons in Canada.

57. The jurisprudence of the Intelligence Commissioner recognizes that the Minister is not a technical expert. However, it is reasonable for him when making conclusions to rely on the Chief's assessment that the acquisition of information is necessary to identify, isolate, prevent or mitigate harm to non-federal systems.

58. The Minister explains that threat actors deliberately disguise their malicious activity. As a result, it is not possible for CSE to predict [...]. Therefore, 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 [...].

59. There is nothing in the record to suggest that CSE can achieve the same cybersecurity outcomes by using different cybersecurity solutions 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 authorization and other aspects of its mandate. Before any information relating to Canadians or persons in Canada can be used, it must be assessed for essentiality to identify, isolate, prevent or mitigate harm to the non-federal systems and federal systems. Information that does not meet the essentiality test will be deleted. Further use, analysis, retention and disclosure of any information acquired under the Authorization are subject to restrictions and conditions set out in CSE's policies.

60. 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 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))

61. 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. At paragraph 62 of the Authorization, the Minister concludes that he has reasonable grounds to believe that the measures referred to in section 24 have been met.

62. 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 systems. 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 the 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.

63. 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.

64. 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 any reporting does not identify the

identity of an individual. The MPS also sets out the required disclosure approval levels accompanying different types of information. These approvals must be documented.

65. I note that in their 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.

66. 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. CSE employees must document rationales for retention, use and disclosure of information related to Canadians and persons in Canada. In my view, when followed, these measures provide an effective manner for CSE to respect the legislative requirement to sufficiently protect this information.

67. I am therefore 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 entities' systems.

V. REMARK

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

A. Consent of all persons whose information may be acquired

69. To deploy cybersecurity solutions on non-federal systems, the *CSE Act* requires that CSE obtain a written request – the consent – of the owner or operator of those systems. In contrast, in the case of cybersecurity activities on federal systems, the Minister must

conclude that there are reasonable grounds to believe that "the consent of all persons whose information may be acquired could not be reasonably obtained" (s 34(3)(b), *CSE Act*).

70. Conceptually, the information that may be acquired by CSE when providing services to a non-federal entity "belongs" to that non-federal entity. To issue a cybersecurity authorization, there is no requirement for the Minister to consider whether the non-federal entity has the legal authority to acquire or share the information that CSE may ultimately acquire through its cybersecurity solutions, which could include elements of consent. I am not suggesting that the non-federal entities here – or in general – do not have that legal authority. Rather, I highlight that carrying out cybersecurity activities raises complex issues relating to the collection and use of potentially personal information for cybersecurity purposes and obtaining consent for doing so. Given the increasing importance of cybersecurity for all Canadians, these should remain central issues for all entities responsible for protecting sensitive information.

VI. CONCLUSIONS

71. As set out in my decision of […] (Annex A), I approved the Cybersecurity Authorization for Activities on Non-Federal Infrastructures, which expires one year from the day of my approval.

72. As prescribed in section 21 of the *IC Act*, a copy of my decision and these reasons 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.

[…]

The Honourable Simon Noël, K.C.
Intelligence Commissioner