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

File: CSE-2025-01

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 FOR 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) for a non-federal entity – [...] – pursuant to the *Intelligence Commissioner Act*, SC 2019, c 13, s 50 (*IC Act*). A copy of this decision is attached as Annex A.

2. The Authorization was issued on [...], by the Minister of National Defence (Minister) pursuant to subsection 27(2) of the *Communications Security Establishment Act*, SC 2019, c13, s 76 (*CSE Act*). Given the context of the Authorization, I agreed with the Minister's request that I review the Authorization on an expedited basis. In my view, the three-day delay between the Minister's signature and the receipt of the Authorization by my office did not diminish the urgent nature of the Authorization. Based on my review of the record, I was satisfied that 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 were reasonable. To avoid any delay in allowing the Communications Security Establishment (CSE) to provide cybersecurity support to the non-federal entity, on the same day that I received the Authorization and related materials for review, I issued my decision with full reasons to follow. Below 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 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 have to incidentally acquire communications and information that interfere with the reasonable expectation of privacy of Canadians or persons in Canada.

5. Prior to proceeding with activities that may have these effects, CSE is required to obtain an authorization issued by the Minister and approved by the Intelligence Commissioner. To approve the activities or classes of activities specified in the authorization, the Intelligence Commissioner must be satisfied that the Minister's conclusions – essentially the reasons for issuing the authorization – are reasonable (s 14, *IC Act*).

6. A ministerial authorization allows CSE to access electronic information and information infrastructures belonging either 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. 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 from mischief, unauthorized use or disruption.

7. When the authorization relates to a non-federal system, the owner or operator of that system must ask 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 them to conclude that there are reasonable grounds to believe that the authorization is necessary (s 33(2), *CSE Act*).

8. Subsections 34(1) and (3) of the *CSE Act* set out the additional statutory conditions under which the Minister may issue a cybersecurity authorization. The 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.

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* (s 22(1), *CSE Act*). When conducting activities pursuant to an authorization, it is nevertheless 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 with respect to 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 letter from the Minister to the Intelligence Commissioner;
b) The Authorization;
c) The Briefing Note from the Chief to the Minister;
d) The Chief's Application, containing nine 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. The Mission Policy Suite for Cybersecurity (MPS) approved February 28, 2022; and
e) Briefing Deck – Overview of the Activities.

III. STANDARD OF REVIEW

12. Pursuant to section 12 of the *IC Act*, the Intelligence Commissioner conducts a 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 review 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 [*Vavilov*] at paragraph 99, the Court succinctly describes what constitutes a reasonable decision:

> A reviewing court must develop an understanding of the decision maker's reasoning process in order to determine whether the decision as a whole is reasonable. To make this determination, the reviewing court asks whether the decision bears the hallmarks of reasonableness – justification, transparency and intelligibility – and whether it is justified in relation to the relevant factual and legal constraints that bear on the decision.

15. Relevant factual and legal constraints can include the governing statutory scheme, 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 these 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. I must also 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. The Chief submitted to the Minister a written application for a cybersecurity authorization in relation to the non-federal entity (Application). The Application includes the written request from the non-federal entity for CSE's support in conducting cybersecurity activities.

19. As required by subsection 21(1) of the *CSE Act*, I am satisfied that the systems of the non-federal entity belong to a class of information infrastructures that are of importance to the Government of Canada, as designated in the *Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada* issued on August 25, 2020 – in particular as a […]

20. The Application describes the cybersecurity solutions that will be deployed by CSE. These consist of: […] and […]

21. A description of the non-federal entity, the context in which it 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 include 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.

22. The Minister recognized that without the Authorization, the cybersecurity activities set out at paragraph 76 of the Authorization may be contrary to other Acts of Parliament, or may interfere with the reasonable expectation of privacy of Canadians or persons in Canada. Based on the facts presented in the Application submitted by the Chief, 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. Consequently, the Minister issued a one-year Authorization.

23. I must now 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. Reviewing the Minister's conclusions that the activities are reasonable

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 concluded at paragraph 34 of the Authorization that there were such grounds given the objective of helping to protect the systems of the non-federal entity, and potentially federal systems and other systems of importance, from mischief, unauthorized use, or disruption.

26. 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.

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

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

29. 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 sophistication of cyber threats render them difficult to identify. Based on the information provided by the Chief, the Minister concludes that the non-federal entity's cybersecurity posture is not sufficient to identify and counter the sophisticated capabilities deployed by advanced and persistent threat actors.

30. CSE's cybersecurity solutions provide a separate and additional layer of defence to detect potential compromises. The Minister explains that CSE's knowledge and cyber solutions allow for detection and response to threats unknown to commercial providers of cybersecurity. Given the context in which the Authorization was issued, CSE's […] also supports the Minister's conclusion that the activities are effective and reasonable.

31. I agree with the Minister that the activities set out in the Authorization allow CSE to advise and better protect the non-federal entity's systems. Indeed, through the activities, CSE may recommend mitigation actions, and also conduct them with the consent of the non-federal entity. I also agree with the Minister that CSE's support is even more pressing given the non-federal entity's […].

32. The second reason put forward by the Minister for which CSE's activities are reasonable is the critical role played by the systems of the non-federal entity […] This role effectively consists of […]. […], the non-federal entity […], the non-federal entity constitutes an attractive target for cyber threat actors. […]

33. The third ground supporting the Minister's conclusion that the activities are reasonable is the existing cyber threat landscape. A purpose of a cybersecurity authorization is to help protect the systems and information of the non-federal entity (s 27(2), *CSE Act*). Protecting the systems does not require an existing cyber compromise. In contexts where cybersecurity activities are carried out for preventative or proactive purposes, the Minister needs to establish a factual basis for CSE's assistance (Decision CSE-2024-07, para 84). As indicated in my […] Decision, the Minister issued the Authorization on a proactive basis; there is no known compromise or specific threat to the non-federal entity. Nevertheless, the record

describes existing cyber threat actors in great detail, and provides information related to the likelihood of the non-federal entity's systems being the target of malicious cyber activities – information that I have included in Annex B.

34. The Minister does not state with certainty that the non-federal entity will be targeted by cyber threat actors. Rather, underpinning the Minister's rationale is that the cyber threat to the non-federal entity exists as a direct correlation to the critical role it plays. Indeed, CSE assesses that every Canadian province and territory has likely been targeted by cyber actors for the purposes of intelligence collection and that the [...]. At the same time, CSE assesses that under the current circumstances, the non-federal entity is [...]

35. I find the Minister's rationale convincing that the nature of the non-federal entity makes it a likely target for cyber threat actors. I am satisfied that the Minister has established a sufficient factual basis of the threat to the non-federal entity's systems. As a result, I find reasonable the Minister's conclusions that the activities set out in the Authorization are reasonable.

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

36. The Minister also concluded at paragraph 34 of the Authorization that he had reasonable grounds to believe that the activities authorized are "proportionate given the manner in which they are conducted."

37. 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, not the information's content.

38. To show that the activities are proportionate, the Minister sets out seven internal measures and controls applied by CSE to ensure protection of the information it acquires:

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.

39. 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 the potential impairment and privacy interests. I am satisfied that the interests of Canadians and persons in Canada were considered and the balancing conducted is reasonable.

40. The Minister's balancing exercise is also evident in his discussion of Acts of Parliament that have the potential to be contravened. The Minister indicates they are limited in number because the activities would take place only on systems where CSE has received the express consent of the owner to operate. Also, the activities must fall within the scope of those outlined in the Chief's Application and are restricted to the acquisition of information for the protection of non-federal systems and federal systems. Finally, if there is a contravention of an Act of Parliament not listed in the Application, the Chief will inform both the Minister and the Intelligence Commissioner.

41. The Minister's conclusions reflect his understanding of the privacy interests at issue and the measures in place to protect them. 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

42. 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; and

c) the measures in place ensure that information acquired under the authorization identified as relating to Canadians or a 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))

43. 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.

44. As it is not possible for CSE to determine what information will be helpful in identifying malicious activity, it acquires a large volume of information from the non-federal entity's systems. The Minister explains that CSE processes this information, mainly through automated means. This process may identify some of the information as "necessary" or "essential". All other information is considered to be unassessed information, even though it

has gone through the automated processes. The maximum retention period for unassessed information is [...].

45. The Minister explains that the effectiveness of CSE's activities depend on being able to cross reference and analyse multiple sources of information already acquired, including indicators of compromise that have been identified. 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 helps CSE develop better mitigation actions and cyber responses that can also be used not only for non-federal systems, but also for other designated systems of importance and for federal systems.

46. At the end of the [...] period, unassessed information will be automatically deleted unless deemed "necessary" or "essential" to help protect the non-federal system, federal systems, and other designated systems of importance. The Chief states in the Application that the non-federal entity is aware and agrees to this use of the information. 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.

47. The Minister specified that while unassessed information may be retained by CSE's for up to [...] from acquisition, the information is actually retained for a maximum of [...]. This means that if the daily automated retention scripts malfunction, analysts are alerted and can reinstitute them prior to the [...] assessment retention deadline. The Minister also highlights CSE's internal compliance program that has an established process for responding to incidents. This multi-layered approach allows CSE to maintain a strong ecosystem of privacy protection measures.

48. As explained in the record, the "necessary" criterion applies to information that does not relate to Canadians or persons in Canada whereas the "essential" criterion applies to information that relates to Canadians or persons 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. The purpose is to assist in developing detection and prevention analytics and further strengthen the cyber defence ecosystem.

49. 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.

50. Information that is determined to be necessary or essential to identify, isolate, prevent, or mitigate harm may be retained "indefinitely or until the information is no longer useful for these purposes." This information will be tracked in accordance with section 11.2 of the MPS and operational managers are reminded on a quarterly basis to review retained recognized information related to Canadians or persons in Canada to revalidate whether it remains essential. I will further address this issue in my remarks.

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

52. Given the multiple layers of internal controls to privacy and limited access to unassessed information, 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))

53. CSE cannot predict [...]. Therefore, to effectively monitor the non-federal entity's systems and mitigate any potential cyber threats, CSE must acquire a vast range of information. This

information is then assessed to identify malicious activity. The information includes [...]. As the non-federal systems are located in Canada, CSE will almost certainly incidentally acquire information that interferes with the reasonable expectation of privacy of Canadians and persons in Canada.

54. The Minister explains that while commercial cybersecurity platforms are currently used by the non-federal entity, CSE's cybersecurity solutions are required to offer better protection given the existence of sophisticated and persistent threat actors. CSE cannot achieve the same outcomes by using different cybersecurity solutions that acquire less information, specifically information related to Canadians.

55. 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. Before any information relating to Canadians or persons in Canada can be used, it must have been assessed to be essential for cybersecurity purposes. Further use, analysis, retention and disclosure of any information acquired under the Authorization is subject to restrictions and conditions set out in the MPS.

56. For these reasons, I am satisfied that the Minister's conclusions are reasonable. 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))

57. 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 67 of the Authorization, the Minister concludes that he has reasonable grounds to believe that the measures referred to in section 24 have been met.

58. The Minister reiterates that information relating to Canadians or persons 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, prevent, or mitigate 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 support the Minister's conclusions.

59. In Decision CSE-2024-05 related to other non-federal entities, I remarked that information that may be acquired by CSE when providing services to a non-federal entity "belongs" to that entity. Information in which there is a reasonable expectation of privacy shared on a non-federal entity's system may end up being retained for cybersecurity purposes by CSE, a Government of Canada agency. Although not explicitly required under the *CSE Act*, 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. In response to this remark, the Chief confirms in a Briefing Note to the Minister as well as in the Application that CSE has received verbal confirmation that the non-federal entity has the requisite legal authority to collect and use information related to Canadians or persons in Canada for cybersecurity purposes. For future authorizations, CSE endeavours to obtain the confirmation in writing. I add that it would be useful for this confirmation to include an overview about any measures taken by the non-federal entity to provide notice to, and obtain consent from, the users of its systems that their information may be collected and used for cybersecurity purposes.

60. In addition to concluding that Canadian-related information will only be used, retained and analysed if it satisfies the essentiality test, Minister's conclusions and the record also explain how information related to Canadians or persons in Canada can be disclosed. The explanation mirrors the statutory obligation found at section 44 of the *CSE Act*, namely that this disclosure must be necessary to help protect the non-federal system, federal systems or

other systems of importance. The information is only disclosed to persons or classes of persons designated under the *Ministerial Order Designating Recipients of Information Relating to a Canadian or Person in Canada Acquired, Used, or Analyzed Under the Cybersecurity and Information Assurance Aspect of the CSE Mandate* issued on June 13, 2023, in accordance with section 45 of the *CSE Act*. These include owners or administrators of computer systems or networks used by the Government of Canada or a non-federal entity, as well as authorized persons or classes of persons within foreign entities with which CSE has established arrangements.

61. 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.

62. I note that in its letter of request to CSE, the non-federal entity asked that all its proprietary, and all personal, information that may be collected and retained be obfuscated before it is shared. I raise some concerns in my remarks regarding this issue.

63. 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.

64. 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 the non-federal entity's systems.

V. REMARKS

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

A. Content of letter of request from system owner

66. To deploy cybersecurity solutions on non-federal systems, CSE must obtain the written request of the owner or operator of those systems. The request must be included in the application to the Minister (s 33(3), *CSE Act*) and therefore forms part of the factual matrix before the decision maker (*Vavilov,* paras 94 and 126). Indeed, in the Authorization, the Minister states that his conclusions are based not only on "the facts and submissions set out in the Application", but also "on the written request from the system owner".

67. The *CSE Act* does not prescribe the content of a letter of request. However, the MPS – Cybersecurity provides that letters of request must use a template drafted by CSE's Directorate of Legal Services (s 18.1.1). With the exception of a few minor amendments – and one notable addition which I address in my third remark – the letter in the record mirrors those received in previous cybersecurity authorizations.

68. Although a template letter from the non-federal entity can satisfy the legislative requirement, I make the following remark for consideration with the goal of improving the letter, and by consequence the information that is available to the Minister when examining whether to issue an authorization.

69. The template letter does not explain why the non-federal entity seeks CSE's support. Rather, it sets out a general request and includes a number of statements in which the non-federal entity acknowledges and accepts that CSE's cybersecurity solutions will be deployed on its systems. The template letter effectively constitutes the non-federal entity's consent. Indeed, the MPS states that the letter's objective is to "clearly capture the client's consent for CSE to access their infrastructure and acquire any information from it" (s.18.1.1). I agree that it is important for the Minister to be aware of the non-federal entity's consent.

70. The factual basis for CSE's support is therefore left to be provided in the Chief's Application to the Minister. In cybersecurity authorizations relating to non-federal entities, I have been satisfied that the Minister has understood why CSE's support was necessary, as required by subsection 33(2) of the *CSE Act*. Indeed, in the record before me, a briefing note from the Chief to the Minister stated that the non-federal entity "indicated concern regarding the existence of unknown vulnerabilities on their systems, since their current commercial cybersecurity products are not able to conduct vulnerability scanning."

71. Nevertheless, given that the Minister relies on the letter of request when allowing CSE to access the non-federal entity's systems, I believe that the record before the Minister would benefit from a letter that provides, at least minimally, a general outline of why the non-federal entity is requesting CSE's support. I acknowledge that there may be situations in which the non-federal entity may not be able to provide much information about a cyber threat or compromise in the letter. In some cases, CSE may also have access to additional information that it cannot share with the non-federal entity, and if so, it must continue its practice of providing this information to the Minister.

72. Including additional detail in the letter of request has the benefit of more clearly articulating the objectives to be accomplished and ensuring the consent of the requesting party is fully informed. It could also add weight to situations in which there may be urgency for the Minister to issue an authorization and the Intelligence Commissioner to conduct his review in a condensed timeframe.

B. Obfuscation of personal and proprietary information prior to disclosure

73. In my decision rendered on [...] in this matter, I noted that in its letter of request to CSE, the non-federal entity asked that all of its proprietary and all personal information be obfuscated before it is shared. The letter of request also includes an acknowledgement by the non-federal entity that information contained or shared on the non-federal entity's systems, "including personal information and private communications, may be incidentally acquired and used, analysed, retained or disclosed by CSE/CCCS [Canadian Centre for Cyber Security] for

cybersecurity purposes" (emphasis added). Such an acknowledgement has not been included in any previous letter of request from a non-federal entity.

74. I am of the view that there is lack of clarity in the letter with respect to whether the non-federal entity has a clear understanding of CSE's privacy protection measures. On the one hand, the non-federal entity requests obfuscation prior to information being disclosed, while on the other, acknowledges that CSE can disclose personal information – and according to the MPS, disclosure of Canadian-related information is authorized under specific conditions.

75. The lack of clarity is also evident in the Authorization. At paragraph 66 of the Authorization, the Minister states that: "Further use, analysis, retention or disclosure of information acquired under a cybersecurity authorization remains subject to restrictions for retained cybersecurity, including conditions imposed by clients or disclosing entities" (emphasis added). The MPS also provides that "the internal use, processing, handling of this information is also subject to all restrictions for retained cybersecurity information, including conditions imposed by clients or disclosing entities" (s. 26.2 MPS) (emphasis added). If the non-federal entity's obfuscation request constitutes a "client condition", I understand this information in the Authorization to mean that CSE could not share personal or the non-federal entity's proprietary information without this information first being obfuscated.

76. However, in paragraph 71 of the Authorization, the Minister indicates that CSE may disclose information outside of CSE that may have been derived from information acquired, used and analyzed in the course of the activities carried out under the Authorization. While the same paragraph specifies the disclosure must be necessary, and made only to persons designated under the appropriate ministerial order made under section 45 of the *CSE Act*, no reference is made to the suppression or obfuscation of information prior to sharing. Indeed, pursuant to the *CSE Act* and the ministerial order of June 13, 2023, Canadian-related information can be disclosed.

77. I am not privy to the discussions that occurred between CSE and the non-federal entity, and it may be clear to both parties in what manner personal and proprietary information collected pursuant to the Authorization can be disclosed. However, based solely on the information in

the record, the lack of clarity creates a risk of misinterpretation that could affect the consent of the non-federal entity. Future records should be clearer on how a request for obfuscation from a non-federal entity is operationalized and whether it is consistent with CSE policies relating to sharing Canadian-related information. Further, if CSE believes that there is indeed a risk that its understanding differs from of the non-federal entity's understanding with respect to disclosure of personal and proprietary information, it may be advisable for CSE to clarify this issue with the non-federal entity.

C. Change in Quarterly Review Provisions

78. My final remark concerns the review of retained information relating to Canadians and persons in Canada to revalidate whether it is still essential. The language used to describe the revalidation process has changed in recent authorizations without the change being addressed in the respective records. I am of the view that future authorizations could benefit from additional clarity.

79. In Decision CSE-2023-02, my remarks addressed the topic of the criteria of retention of information "until the information is no longer useful" (paras 89 and 90). I noted that the record was silent as to the procedures in place to review the use of information and deletion of information that is no longer useful, including no mention on how often periodic reviews occur.

80. In response, in the next application for authorization (Decision CSE-2023-05), the record indicated that "[o]n a quarterly basis, operational managers must review retained recognized IRtC to revalidate whether it is still essential. Information that is no longer essential must be deleted" (emphasis added). In addition, the application specified that this requirement was to be included in the next iteration of the MPS.

81. As of Decision CSE-2024-07, including in this matter before me, the respective records no longer state that the operational managers "must review" retained recognized IRTC to revalidate whether it is essential. They are rather "reminded to review" this information. Further, the record no longer references the inclusion of the review requirement in a future iteration of the MPS.

82. It is unclear to me whether the change in the language used in the record reflects an actual change in practice. For the purpose of my review, it is important that the information presented to the Minister accurately reflects how CSE conducts its operations, and that CSE's policy is clear for its employees. I note that both the Minister and I have relied on the fact that revalidation reviews are being performed in coming to our respective conclusions to issue authorizations and to approve them. I look forward to a future record providing additional clarity on this issue.

VI. CONCLUSIONS

83. 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.

84. 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.

[...]

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner