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

File: CSE-2025-07

Office of the Intelligence Commissioner
Bureau du commissaire au renseignement

P.O. Box/C.P. 1474, Station/Succursale B
Ottawa, Ontario K1P 5P6
613-992-3044 • Fax 613-992-4096

INTELLIGENCE COMMISSIONER

DECISION AND REASONS

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

[...]

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 two non-federal entities (Authorization).

2. The Authorization sets out the identical activities approved by the Intelligence Commissioner in [...] (Decision CSE-2024-05) in relation to the same two non-federal entities – [...]. No new operational activities are being sought.

3. On [...], pursuant to subsection 27(2) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*), the Minister issued the Authorization and it was received by the Office of the Intelligence Commissioner (ICO) for my review and approval under the *Intelligence Commissioner Act*, SC 2019, c 13, s 50 (*IC Act*).

4. For the reasons that follow, I am satisfied that the Minister's conclusions made under subsections 34(1) and (3) of the *CSE Act* in relation to the activities and classes of activities enumerated at paragraph 75 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, CSE carries out cyber protection activities to defend certain electronic systems, devices, networks and the information they contain from criminal and state-sponsored cyber threats. CSE also provides advice and guidance to strengthen the cybersecurity posture of these systems (s 17, *CSE Act*).

7. In this instance, the systems belong to non-federal entities designated as being of importance to the Government of Canada – non-federal systems (s 27(2), *CSE Act*). To initiate the

process, the owner or operator of the systems must request CSE's help in writing (s 33(3), *CSE Act*).

8. To understand vulnerabilities and compromises, CSE accesses and acquires information from the systems. In so doing, CSE may have to contravene certain federal laws or collect information in a manner that interferes with the reasonable expectation of privacy of Canadians (Canadian citizens, permanent residents or corporations formed under Canadian or provincial law) or persons in Canada. A ministerial authorization is therefore required (ss 22(4), 27(2), *CSE Act*).

9. An authorization sets out the Minister's conclusions – effectively the reasons – supporting the activities or classes of activities that CSE may carry out. The Minister must, among other conditions, conclude that the proposed activities are necessary (s 33(2), *CSE Act*), reasonable and proportionate (s 34, *CSE Act*). An authorization is valid for up to one year following the Intelligence Commissioner's approval (s 36, *CSE Act*). It is only upon this approval that CSE may carry out the authorized activities.

10. Despite an authorization, the *CSE Act* imposes limits on CSE's cybersecurity activities. CSE is prohibited from directing the activities at Canadians or persons in Canada and from infringing the *Canadian Charter of Rights and Freedoms* (*Charter*) (s 22(1), *CSE Act*). However, when carrying out its activities, CSE may incidentally acquire information relating to Canadians or persons in Canada, meaning it was not deliberately sought (ss 23(4) and (5), *CSE Act*). To use, analyse, retain or disclose this information, CSE is statutorily required to have measures in place to protect the privacy of Canadians and of persons in Canada (s 24, *CSE Act*).

11. A description of the non-federal entities and the cybersecurity activities set out in the Authorization can be found in the classified annex to this decision (Annex A). The annex renders the eventual public version of the decision easier to read and ensures that the decision contains the nature of the facts that were before me, which otherwise would only be available in the record.

12. In accordance with section 23 of the *IC Act*, the Minister confirmed in his cover letter that he provided me with all of the 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 (Chief) to the Minister;
    c) The Chief's Application, containing fourteen annexes, including but not limited to:
        i. Letters of request from the non-federal entities;
        ii. Two ministerial orders;
        iii. Retention and Disposition Table;
        iv. Mission Policy Suite – Cybersecurity (MPS) approved February 14, 2025; and
        v. Outcomes Report for 2024-2025; and
    d) Briefing Deck – Overview of the Activities.

III. STANDARD OF REVIEW

13. The *IC Act* requires the Intelligence Commissioner to review whether the Minister's conclusions are reasonable. I will therefore apply the reasonableness standard, as applied in judicial reviews of administrative action.

14. As indicated by the Supreme Court of Canada, when conducting a reasonableness review, a reviewing court is to start its analysis by examining the reasons of the administrative decision maker. In *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 at paragraph 99, the Court succinctly describes what constitutes a reasonable decision:

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

15. Relevant factual and legal constraints can include the governing statutory scheme and the impact of the decision. The governing statutory scheme set out in the *IC* and *CSE Acts*

highlights the role of the Intelligence Commissioner as an independent mechanism to ensure that government action taken for the purpose of national security and intelligence is properly balanced with the respect of the rule of law and the rights and interests of Canadians.

16. When the Intelligence Commissioner is satisfied (*convaincu* in French) that the Minister's conclusions at issue are reasonable, he "must approve" the authorization (s 20(1)(a), *IC Act*). Conversely, where not satisfied the conclusions are reasonable, the Intelligence Commissioner "must not approve" the authorization (s 20(1)(b), *IC Act*). In both cases the Intelligence Commissioner must set out his reasons for doing so.

IV. ANALYSIS

17. On […], the Chief submitted an application to the Minister requesting authorization for the proposed activities (Application). The Application sets out a description of the non-federal entities, the cybersecurity activities that CSE wishes to conduct or continue, and describes how CSE will analyse, process and retain the acquired information, as well as the measures in place to protect the privacy of Canadians and persons in Canada in cases where it incidentally acquires information about them.

18. The Application also sets out the cybersecurity solutions to be continued or to be deployed on the non-federal systems – with the consent of the non-federal entities – which will allow CSE to securely acquire data and take mitigation actions, either manually or automatically. The solutions consist of: […]

19. The Minister concluded that there are 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. He issued the Authorization with a one-year validity period, subject to my approval.

A. Updated Record

20. In past decisions, I have made a number of remarks that raise legal or factual issues of concern to improve the content of future authorizations or highlight an issue for CSE's

consideration. I am pleased to note the responsiveness of the Minister and CSE towards these remarks, which strengthens the authorization regime.

21. The responses to the remarks in this record include additional detailed information about the types of information retained by CSE and the sharing of reports with international partners, as well as information about the reports shared with the non-federal entities it is supporting. The Authorization provides greater clarity and certainty around the types of information relating to Canadians or persons in Canada incidentally acquired by CSE. A rationale for CSE's continued presence on the non-federal systems has also been provided.

22. The letters of request from the non-federal entities have also been improved by including confirmations of the non-federal entities' legal authority to collect and share information for cybersecurity purposes. I note that in her Briefing Note to the Minister, the Chief also indicates that CSE is continuing to review options to include a summary of the measures taken by the non-federal entities to provide notice to, and obtain consent from, individuals whose information may be acquired for cybersecurity purposes in future authorizations. I look forward to being informed of any developments in future authorizations.

23. Finally, given the context of last year's authorization, I was of the view that it was in the public interest to render my decision on an expedited basis and that the preparation of my reasons should not delay the implementation of the cybersecurity solutions by CSE on the non-federal entities' systems (CSE-2024-05). I note that one of the approved cybersecurity solutions has yet to be deployed to one of the non-federal entities, but that the delay is not attributable to CSE.

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

24. The Minister concluded that he had reasonable grounds to believe that the activities are reasonable given the objective of helping to protect the non-federal entities' electronic information and infrastructure, as well as to potentially protect federal systems and other systems of importance from mischief, unauthorized use, or disruption.

25. The Minister acknowledges that the cybersecurity activities set out in the Authorization will result in CSE acquiring information in which Canadians or persons in Canada have a reasonable expectation of privacy. I agree with the Minister and this confirms the need for this Authorization. Following my review of the record, I am satisfied that the cybersecurity activities set out in the Authorization respect the statutory requirement that CSE's activities are not directed at Canadians or persons in Canada (s 22(1), *CSE Act*).

26. To justify the reasonableness of the activities in relation to the non-federal entities, the Minister relies on three grounds: 1) the effectiveness of the activities for which the Authorization is sought; 2) the need for CSE's support given the important roles of the non-federal entities; and 3) the threat to the non-federal entities' systems posed by cyber threat actors.

27. First, the activities set out in the Authorization are effective. The Minister's conclusions as well as other information in the record show that CSE has been successful in detecting and reporting vulnerabilities and compromises. Based on CSE guidance and advice, the non-federal entities have implemented and continue to implement the recommendations described in Annex A. The recommendations allow the non-federal entities to better defend their systems and protect against future threats.

28. As explained by the Minister, the non-federal entities hold vast amounts of data and given their nature, are attractive targets to malicious actors. In the case of [description of nature of Non-federal entity 1]. Continued deployment of CSE's cybersecurity solutions on [Non-federal entity 2's] systems, which act in tandem with commercial measures, will allow CSE to react with the necessary speed to effectively mitigate compromises. Ultimately, it will allow [Non-federal entity 2] to protect its systems from additional harm caused by threat actors.

29. To provide better cybersecurity, the Minister states that CSE's knowledge and cyber solutions allow for the capacity to respond to threats unknown to commercial cybersecurity providers. Indeed, CSE has specialized intelligence that provides unique insight into the capabilities and intentions of malicious actors. The activities set out in the Authorization allow CSE to provide sophisticated threat detection and to recommend mitigation actions or conduct mitigation actions, with the consent of the non-federal entities. The outcomes of last year's authorization also support the Minister's conclusion that the activities are effective and reasonable.

30. The second ground relied upon by the Minister is the critical roles played by the non-federal entities. According to the Minister, the systems of the non-federal entities must be secure in light of their important role in the lives of Canadians and persons in Canada. [Non-federal entity 1] provides critical programs and services to Canadians and is essential […]. For its part, [Non-federal entity 2], provides critical services to support […]. According to the Minister, […]. The importance of continually monitoring the threat landscape against numerous threat actors is further reinforced by previous compromises of other systems of importance to the Government of Canada […]. Similar to last year, I find that the description of the role played by the non-federal entities supports the Minister's conclusion that the activities set out in the Authorization are reasonable.

31. The third reason supporting the Minister's conclusion is the existing cyber threat landscape. The record describes the compromises and potential compromises to the systems belonging to the non-federal entities – information that I have included in Annex A. Based on the information provided by the Chief, the Minister concludes that the current state of the two non-federal entities' cybersecurity posture is not sufficient to identify and counter the sophisticated methods and capabilities deployed by advanced and persistent threat actors. CSE assesses that […]. Both non-federal entities will continue building their cybersecurity posture by implementing CSE's recommendations.

32. I am of the view that the Minister's conclusions establish a factual basis for CSE's assistance and 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 also a rational link

between the cybersecurity activities and the effectiveness of protecting the non-federal entities' systems. The Minister relies on the important roles played by the non-federal entities, which I find supports his conclusions. As a result, I find reasonable the Minister's conclusions that the activities set out in the Authorization are reasonable.

C. Are the Minister's conclusions proportionate (s 34(1), *CSE Act*)

33. The Minister also concluded that he had reasonable grounds to believe that the proposed cybersecurity activities authorized are "proportionate given the manner in which they are conducted, and because they are rationally connected to the objective and will minimally impair the rights and freedoms of third parties, and [those of the non-federal entities] and third parties' ability to access or use equipment or infrastructure."

34. The Minister identifies the reasons for which the activities are necessary and useful, notably for acquiring information to help protect non-federal systems and to support other CSE activities. He recognizes that the activities can lead to acquiring large volumes of information in order to identify cyber threats. Although Canadians and persons in Canada may have a reasonable expectation of privacy in some of the information, the Minister explains that CSE is interested in any anomalous behaviour related to the information, rather than the contents of the information. CSE retains only a very small percentage of the total amount of data initially acquired. I am satisfied that the Minister's conclusions are reasonable with respect to the authorized activities.

35. The Minister concludes that the activities are proportionate by relying on the internal measures and controls applied by CSE after the information is acquired. They are the same as those included in last year's authorization.

36. I can trace the Minister's rationale for relying on these measures. Access to acquired information is restricted to designated CSE employees who are trained to handle this type of information and use it on a need-to-know basis for their work. The Minister was cognizant of the privacy interests at issue and laid out the measures in place to protect them.

37. As for the Acts of Parliament that have the potential to be contravened, the Minister's balancing exercise is also evident. The Authorization indicates they are limited in number because the activities would take place only on systems where CSE has received the express consent of the non-federal entities. 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. As an additional safeguard, if there is a contravention of an Act of Parliament not listed in the Application, the Chief will inform both the Minister and the Intelligence Commissioner.

38. 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. He explains how the activities sought to achieve a reasonable balance between them. I find that his conclusions are justified and intelligible. I am satisfied that the Minister's conclusions in relation to the proportionality of the activities are reasonable.

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

39. After establishing that the activities are reasonable and proportionate pursuant to subsection 34(1) of the *CSE Act*, the Minister may issue an authorization if he concludes that there are reasonable grounds to believe that the following three conditions have been met (s 34(3), *CSE Act*):

    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 a Canadian and person 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))

40. As explained by Minister, the requirements set out in CSE's internal policies and retention schedule allow CSE to acquire large volumes of information generated by or residing on the non-federal entities' systems and to retain it for no longer than necessary. The retention schedule has been developed to reflect information management principles and incorporates minimum retention periods prescribed in the *Privacy Act,* RCS, 1985, c P-21 and the *Library and Archives of Canada Act*, SC 2004, c 11.

41. The Minister specifies that collected information is mainly processed by CSE through automated means. While some of the information is identified as "necessary" or "essential", all other information is considered to be unassessed, even though it has gone through the automated processes. The maximum retention period for unassessed information is 12 months in order to allow CSE to reach back to the origins of an event or examine its evolution over time.

42. Additionally, prior to the expiry of the 12-month period, unassessed information will automatically be deleted unless deemed "necessary" or "essential" to help protect the non-federal systems, or federal systems and other designated systems of importance. The Chief states in the Application that the non-federal entities are aware and agree to this use of the information.

43. As explained in the record, the "necessary" criterion applies to information that by its nature does not contain any elements relating to Canadian or a person in Canada. This information assists CSE in developing detection and prevention analytics and further strengthen the cyber defence ecosystem. Information is "necessary" when it is required for understanding malicious cyber activity, […] for the purpose of protecting non-federal systems.

44. In contrast, the "essential" criterion applies to information that relates to Canadians or persons in Canada such as […]. Without this information, CSE would be unable to identify, isolate, prevent, or mitigate harm to the non-federal systems. The record explains that most

of the analysis is done through automated processes, which flag abnormal behaviour and thereby limit employees' exposure to the content of the files.

45. Information that is determined to be necessary or essential may be retained "indefinitely or until the information is no longer useful for these purposes." This information is tracked in accordance with CSE's internal compliance program. On a quarterly basis, operational managers "must review" retained recognized information relating to Canadians or persons in Canada to revalidate whether it remains essential. I note that in response to remarks made in various decisions on this issue, the Minister clarifies that CSE's internal compliance program circulates quarterly reminders to cybersecurity analysts. Also, as an operational practice, this is undertaken through a reminder to operational managers, who are responsible to conduct the review. I appreciate that the MPS will be updated to reflect this requirement and trust that the responsibilities of cybersecurity analysts and operational managers will be clearly delineated to ensure proper compliance. I reiterate, that 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 (Decision CSE-2025-01, para 82).

46. The Minister also highlights that access to unassessed information is strictly controlled and limited to those authorized to conduct or support cybersecurity activities (s 10.2, MPS). Every query performed against acquired unassessed information is logged for audit and accountability purposes. Unassessed information cannot be shared beyond CSE. Finally, CSE's internal compliance program has an established process for responding to incidents where information is retained for longer than permitted.

47. I am of the view that the Minister's conclusions are reasonable. Information is retained for a length of time that reasonably allows CSE to effectively conduct cybersecurity activities and develop the required cyber responses to keep pace with the rapidly evolving tradecraft of malware threat actors. Further, the multiple layers of internal controls used by CSE limit access to unassessed information and ultimately allow for better protection of non-federal systems as well as federal systems.

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

48. Similar to last year's Authorization, the Minister specifies that since CSE cannot predict […], it must acquire a substantial amount information from the non-federal systems that is then assessed to identify malicious activities. In so doing, given that the systems are located in Canada, the Minister confirms that the cybersecurity activities set out in the Authorization will lead to the collection and retention of information in which Canadians or persons in Canada have a reasonable expectation of privacy.

49. The Application also explains that while the non-federal entities use commercial cybersecurity measures, their current cybersecurity postures "are insufficient to detect and counter the sophisticated methods and capabilities deployed by advanced and persistent threat actors". CSE's knowledge and expertise in cybersecurity has become more and more important in responding to complex cyber threats actors' tools and resources used to circumvent commercial defence measures. The Application indicates for example that the targeting of the Government of Canada's own networks has been consistent […].

50. Finally, the Minister provides 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 information acquired under the Authorization is subject to restrictions and conditions found in the MPS.

51. Based on the foregoing, I am satisfied that the Minister's conclusions are reasonable.

iii. Measures to protect privacy will ensure that information acquired under the authorization identified as relating to Canadians or persons in Canada will be used, analysed or retained only if it is essential to identify, isolate, prevent or mitigate harm to non-federal systems (s 34(3)(d))

52. 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 (IRtC) acquired under the cybersecurity aspect of its mandate.

53. The Minister reiterates that IRtC can only be retained if it is assessed to be essential. Essentiality rationales must be recorded by employees (s 8.2.2, MPS). In my view, these measures contribute to ensuring that CSE complies with its legislative obligation under section 24, and support the Minister's conclusions.

54. In order for CSE to disclose IRtC, the disclosure must be necessary to help protect non-federal systems, federal systems or other systems of importance. The Minister's conclusions and the record mirror the statutory obligation found at section 44 of the *CSE Act* which limits the disclosure of information to persons and classes of persons designated under the ministerial order issued in accordance with section 45 of the *CSE Act*. These include for example 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. In my remarks, I raise an issue regarding the designated recipients of IRtC.

55. Prior to disclosing IRtC, the MPS provides for measures that must be followed (s 24). Indeed, the MPS sets out the required disclosure approval levels, which must be documented. CSE suppresses identifying information such as the identity of an individual. I note in their letters of request to CSE that the non-federal entities each ask that all personal information, as well as all information that is proprietary to them, that is collected from their systems and retained be obfuscated before it is shared beyond the entity and CSE.

56. The MPS sets out elaborate policies to control and safeguard IRtC that is acquired pursuant to a cybersecurity authorization. In my view, when followed, these measures provide an

effective manner for CSE to respect the legislative requirement to sufficiently protect this information. Consequently, I find reasonable the Minister's conclusion that he has reasonable grounds to believe that IRtC will only be used, analysed or retained if essential to identify, isolate, prevent or mitigate harm to non-federal entities' systems.

V. REMARKS

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

A. Ensuring a complete record – Designating systems of importance

58. It is important for the Minister to have a complete understanding of how IRtC incidentally collected and retained by CSE could potentially be shared – in particular how it could be shared outside of Canada. I am of the view that this information should be more fully articulated in the record to the Minister.

59. As previously stated, section 44 of the *CSE Act* limits the disclosure of IRtC acquired under the cybersecurity aspect of CSE's mandate to persons and classes of persons designated under ministerial order issued in accordance with section 45 of the *CSE Act*. On June 13, 2023, pursuant to section 45 of the *CSE Act*, the Minister at the time issued the 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* (Recipients of IRtC Order). This order allows CSE to disclose IRtC for cybersecurity purposes to designated persons or classes of persons, including owners or operators of systems of importance.

60. As a result, the designation of systems of importance impacts how IRtC can be shared. The record includes a copy of the current *Order Designating Electronic Information and Information Infrastructures of importance to the Government of Canada* (SOI Order) dated August 25, 2020. In addition to designating classes of systems of importance (s 21, *CSE Act*), I note that it provides that the electronic information and/or information infrastructures of

entities specifically referenced in Annex 2 to the SOI Order are designated as of importance to the Government of Canada – although Annex 2 does not contain any designations.

61. However, the SOI Order does not appear to be the only order designating systems of importance. According to CSE's public 2022-2023 Annual Report, the electronic information and information infrastructures of Ukraine and Latvia were designated as important to the Government of Canada by two respective orders issued on March 17, 2022. This is described in the report as being the first time the Minister used their powers to designate entities outside of Canada as systems of importance. Further CSE's 2024-2025 Annual Report confirms that as of March 31, 2025, orders designating the electronic information and information infrastructures of the Governments of Ukraine and Latvia were in effect. The record does not include information concerning these orders or address any potential sharing of IRtC pursuant to them. Although it may not be necessary to include a copy of those orders in the record, the Minister should nevertheless have a complete picture of where IRtC could potentially be disclosed.

B. Contents of letters of request

62. In Decision CSE-2025-01, I made a remark that it would be beneficial for letters of request to provide a general outline of the reason(s) for which the non-federal entity is requesting CSE's support. In response, as acknowledged in Decision CSE-2025-06, the next record pertaining to an authorization for a non-federal entity incorporated request letters that included some information to this effect. These letters form part of the factual basis for the Minister to consider and are explicitly referenced as being relied upon by the Minister in existing authorizations.

63. I am of the view that the letters can be further modified to better reflect the circumstances of the request, in particular with respect to whether it is an original request or a renewal of an authorization. Without reference to the record, it is not clear from the current letters that the non-federal entities have already been benefiting from CSE's help pursuant to a prior authorization.

64. I remain cognizant of factors that may limit the level of detail that can be included in request letters, for example because of security reasons or simply because the non-federal entity may not yet fully understand the effect of a compromise. Nonetheless, as the first step that triggers the process leading to a cybersecurity authorization, a letter of request serves as a means to give the Minister and myself helpful context to better understand the rationale for the request, or why CSE's continued support is required.

65. Finally, I have noted that one the letters of request in the record is dated […], which is after the Authorization was signed and received by the ICO for my review. Moreover, both the Application and Authorization refer only to a single written request. While such apparent drafting oversights do not alone impact the reasonableness of the Minister's conclusions, I reiterate my previous remark that a sufficient accumulation of them could (Decision CSE-2023-05).

C. Fulfilment of notification requirement – [Deployment of Certain Cybersecurity Capabilities]

66. In a standalone briefing note dated […], provided to my office, the Chief informed the Minister that CSE had for the first time deployed [certain cybersecurity capabilities] The Chief's doing so fulfilled a notification requirement in several active authorizations.

67. I note, however, that both the Application – also dated […] – and Authorization have not been updated and continue to indicate that [the cybersecurity capabilities] have not yet been deployed. This underscores the importance of updating, or if necessary, correcting after the fact, records so that the Minister is presented with up-to-date information.

68. I look forward to receiving more information in the future on the deployment and impact of these capabilities.

VI. CONCLUSIONS

69. 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 75 of the Authorization are reasonable.

70. 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*.

71. 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.

72. 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.

[…]

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner