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

File: CSE-2025-03

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 TO HELP PROTECT FEDERAL INFRASTRUCTURES
PURSUANT TO SUBSECTION 27(1) OF THE
COMMUNICATIONS SECURITY ESTABLISHMENT ACT AND
SECTION 14 OF THE *INTELLIGENCE COMMISSIONER ACT*

APRIL 16, 2025

Canada

TABLE OF CONTENTS

I. OVERVIEW 1
II. CONTEXT 2
III. STANDARD OF REVIEW 3
IV. ANALYSIS 4
A. Updated record 6
B. Subsection 34(1) of the *CSE Act* – Determining whether the activities are reasonable and proportionate 7
i. Reviewing the Minister's conclusions that the activities are reasonable 7
ii. Reviewing the Minister's conclusions that the activities are proportionate 10
C. Subsection 34(3) of the *CSE Act* – Conditions for issuing an authorization 12
i. Any information acquired under the authorization will be retained for no longer than is reasonably necessary (s 34(3)(a)) 12
ii. The consent of all persons whose information may be acquired could not reasonably be obtained (s 34(3)(b)) 14
iii. Any information acquired under the authorization is necessary to identify, isolate, prevent, or mitigate harm to federal systems(s 34(3)(c)) 15
iv. Measures to protect privacy will ensure that information acquired under the authorization identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to identify, isolate, prevent or mitigate harm to the federal institutions' electronic information or information infrastructures (s 34(3)(d)) 16
V. REMARKS 17
A. Clarification of remark made in Decision CSE-2024-02 17
VI. CONCLUSIONS 19

I. OVERVIEW

1. This is a decision reviewing the conclusions of the Minister of National Defence (Minister) in relation to a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures (Authorization) issued on February 23, 2025, pursuant to the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*). The Authorization is a renewal of authorized activities approved by the Intelligence Commissioner in Decision CSE-2024-02, and no new operational authorities are being sought.

2. The Communications Security Establishment (CSE) has the mandate to carry out cyber protection activities to defend the Government of Canada's 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 institutions of Parliament and the Government of Canada – for example federal departments, government agencies and Crown corporations.

3. To effectively engage in cyber protection activities, CSE may have to contravene certain Canadian laws. It may also incidentally acquire communications and information that interfere with the reasonable expectation of privacy of Canadians or persons in Canada. 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.

4. On February 24, 2025, the Office of the Intelligence Commissioner received the Authorization for my review and approval under the *Intelligence Commissioner Act,* SC 2019, c 13, s 50 (*IC Act*). Pursuant to the *IC Act*, the Intelligence Commissioner must provide a written decision either within 30 days after the day on which the authorization is received, or within any other period agreed to with the Minister (s 20(3)). For this authorization, the Minister and I agreed that I would provide my decision by April 18, 2025. This was done in order to better align with the previous authorization, which was not set to expire until May 13, 2025.

5. For the reasons that follow, I am satisfied that the Minister's conclusions in relation to activities and classes of activities enumerated at paragraph 50 of the Authorization are reasonable.

6. Consequently, pursuant to paragraph 20(1)(a) of the *IC Act*, I approve the Authorization.

II. CONTEXT

7. CSE is the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance (s 15(1), *CSE Act*). A detailed legislative context for CSE's cybersecurity activities is set out in past Intelligence Commissioner decisions relating to cybersecurity found on the ICO's website.

8. To understand vulnerabilities and compromises of federal systems, it is necessary for CSE to access and acquire information from those systems. A ministerial authorization grants CSE the lawful authority to carry out cybersecurity activities that contravene a federal law or that lead to the incidental acquisition of information that interferes with the reasonable expectation of privacy of Canadians or persons in Canada (ss 22(4), 27, *CSE Act*).

9. To issue the authorization, the Minister must, among other conditions, conclude that the proposed activities are reasonable and proportionate, and that measures are in place to protect the privacy of Canadians (ss 24, 34, *CSE Act*). The authorization is valid for up to one year following the Intelligence Commissioner's approval (s 36, *CSE Act*).

10. 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*). It is only then that CSE may carry out the authorized activities.

11. Despite an authorization, the *CSE Act* imposes limits on CSE's cybersecurity activities. CSE must not direct any of its cybersecurity activities at Canadians or persons in Canada or infringe the *Canadian Charter of Rights and Freedoms* (*Charter*) (s 22(1), *CSE Act*). However, CSE may incidentally acquire information relating to Canadians or persons in

Canada (s 23(4), *CSE Act*). Incidentally means that the information acquired was not itself deliberately sought (s 23(5), *CSE Act*).

12. 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 dated February 23, 2025;
    b) The Chief of CSE's Application dated February 20, 2025, including the following annexes:
        i) List of federal institutions receiving cybersecurity services from CSE;
        ii) Ministerial Order – designations for the purpose of section 45, *CSE Act* dated June 13, 2023;
        iii) CSE's Network Monitoring Notice;
        iv) Outcomes Report for 2024;
        v) Assessment of a compromise of a federal institution;
        vi) Retention and Disposition Table;
        vii) Updated Mission Policy Suite for Cybersecurity (MPS) approved February 14, 2025;
        viii) Record of changes to MPS; and
        ix) […];
    c) Briefing Note from the Chief of CSE to the Minister dated February 20, 2025;
    d) Briefing Deck – Overview of the Activities; and
    e) Supplementary materials for the record including Deck presentations to the Intelligence Commissioner and staff in January 2025.

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, the impact of the decision and principles of statutory interpretation. The governing statutory scheme found in the *IC* and *CSE Acts*, as well as legislative debates show 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 the respect of the rule of law and the rights and freedoms 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 unreasonable, the Intelligence Commissioner "must not approve" the authorization (s 20(1)(b), *IC Act*).

IV. ANALYSIS

17. On February 20, 2025, the Chief of CSE submitted a written application for a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures (Application) to the Minister. The Application sets out the cybersecurity activities that CSE wishes to carry out to access and acquire information from systems of federal institutions, originating from, directed to, stored on or being transmitted on or through their information infrastructures in order to protect them from mischief, unauthorized use or disruption.

18. The Application describes the cybersecurity solutions deployed on federal systems – with the consent of the federal institutions – which will allow CSE to securely acquire data and take mitigation actions, either manually or automatically. The solutions consist of: (1) host-based solutions (HBS) – sensors installed on physical or virtual end-point devices (e.g., workstations and servers); (2) network-based solutions (NBS) – sensors installed at the network level which copy network traffic; and (3) cloud-based solutions (CBS) – capabilities similar to HBS and NBS in a cloud environment.

19. The Application also describes how the Chief proposes CSE will analyse, process and retain the acquired information and the measures in place to protect the privacy of Canadians and of persons in Canada in cases where it incidentally acquires information about them.

20. Based on the facts presented in the Chief's Application, 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.

21. Consequently, the Minister issued a one-year authorization for CSE to carry out the activities set out at paragraph 50 of the Authorization:

    a) access a federal system and deploy, when requested by a federal client, HBS, NBS, and CBS;
    b) acquire any information, using HBS, NBS, and CBS, including information identified as relating to a Canadian or person in Canada originating from, directed to, stored on or being transmitted on or through federal systems;
    c) use, analyse, retain, or disclose information acquired under this Authorization for the purpose of identifying, isolating, preventing or mitigating harm to federal systems; and,
    d) conduct mitigation actions, as described in the Application, to counter cyber threats.

22. The cybersecurity activities set out in the Authorization are the same as those I approved last year. Nevertheless, as established by the Intelligence Commissioner's jurisprudence, the Minister must be provided with the best available information when determining whether to authorize activities. This means that the information in the Authorization, as well as supporting materials, must be updated to reflect the most current operational activities

undertaken by CSE. How the activities have been undertaken in the past may be a factor in determining whether the Minister's conclusions are reasonable.

A. Updated record

23. I am satisfied that the current record reflects that this is a new and distinct authorization. The record also contains new information that addresses the remarks I made in my 2024 decision (CSE-2024-02).

24. In response to my remark relating to the language used in notices to users to inform them of the potential use of information shared on federal systems, CSE has included a copy of its own revised Network Monitoring Notice. In line with my remark, the revised notice is now explicit about the potential acquisition and use of information for cybersecurity purposes, stating that "[p]ersonal information collected through monitoring practices […] could also be collected, used, analyzed, retained, or disclosed for cybersecurity purposes." I understand from the record that the same notice will be used by CSIS and that CSE is recommending that federal partners review their own login notices to ensure they are similarly clear.

25. In response to my remark that it would be helpful to include more detailed information regarding the sharing of reports outside CSE, the Outcomes Report now includes specific information on the number of cyber defence reports shared with international partners and how many of these reports contained information relating to Canadians or persons in Canada (IRtC). I further appreciate the inclusion of information on the caveats and other measures put in place in accordance with the MPS to further limit the disclosure of IRtC. The Application also provides greater detail on the "multi-layered" internal controls used by CSE employees to ensure that the retained information complies with the Authorization.

26. With regard to my remark noting the importance of clearly reporting on any incidentally acquired solicitor-client communications, the Outcomes Report in the record now includes a section clearly indicating whether recognized solicitor-client communications were used, analysed, retained, or disclosed (none were, and I trust that if any such communications were incidentally acquired and immediately deleted that would also have been noted). A

corresponding update to the MPS now confirms that the Chief will inform me if they decide to use, analyse, retain or share any solicitor-client communications.

27. With respect to the updated MPS, the record includes a table indicating which sections have been amended. This is helpful and reflects a remark I made in Decision CSE-2023-05, asking that any relevant changes to the MPS be highlighted to the Minister and myself.

28. Finally, I note that both the previous and current authorizations contain a condition that CSE shall inform the Minister when it accepts a request to conduct activities under the authority of the authorization from a federal institution that does not currently receive cybersecurity services from CSE, and that CSE will also subsequently inform me. I have been receiving this information in the statutorily required end of authorization reports (s 52, *CSE Act*).

29. As set out in section 14 of the *IC Act* relating to the issuance of a cybersecurity authorization, I must review whether the Minister's conclusions on the basis of which the Authorization was issued are reasonable.

B. 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

30. 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*). The Minister concluded, at paragraph 15 of the Authorization, that he had reasonable grounds to believe that the activities were reasonable given the objective of helping protect federal systems from mischief, unauthorized use, or disruption.

31. The Minister explains that the cybersecurity activities set out in the Authorization risk CSE acquiring information in respect of which Canadians or persons in Canada have a reasonable expectation of privacy. Federal systems are [...] and the vast majority

of information stored on them relates to Canadians and persons in Canada. Further, the information on the systems is not limited to the information of the employees of the federal institutions receiving cybersecurity assistance from CSE, but also includes information from members of the Canadian public who, for example, communicate with the institutions by email. This underscores the need for the Authorization as well as the effective implementation of privacy control measures by CSE. I note that the activities set out in Authorization are nevertheless aimed at cyber threats and are neither directed at Canadians nor persons in Canada.

32. The Minister justifies the authorized activities by relying on the same two main reasons as last year: 1) the effectiveness of the activities for which the Authorization is sought; and 2) the need for CSE's involvement in the cybersecurity response given the threats to the federal systems.

33. First, CSE's activities consist of deploying advanced malware analysis tools and automated cybersecurity capabilities. The information acquired through these activities helps CSE to protect the federal systems. The Minister explains that CSE's knowledge and cyber solutions allow it to detect and respond to threats unknown to commercial cybersecurity providers. CSE's specialized intelligence on malicious actors and deployment of its unique tools and capabilities at the earliest opportunity also supports the Minister's conclusion that the activities are effective and reasonable.

34. I agree with the Minister that the activities set out in the Authorization allow CSE to advise and better protect the federal systems. Through the activities, CSE may recommend mitigation actions, and also conduct them with the consent of the federal institutions. The Outcomes Report indicates the number of malicious events detected on federal systems from May 2024 to October 2024, and confirms the effectiveness of CSE's cybersecurity solutions. I note that the number of detected malicious events has nearly tripled since the 2023–2024 authorization, and appreciate CSE's inclusion of an explanation (in line with a remark I made in last year's decision regarding contextualizing changes in the volume or nature of detected threats) that this is the result of multiple factors including an increase in scanning activity and the development of new analytics to identify malicious events.

35. I also take note of specific examples included in the Chief's Application identifying ways in which the cybersecurity solutions to be deployed were used to detect and respond to cybersecurity incidents. As the Minister notes, in the last few years, CSE's cybersecurity solutions have been instrumental in detecting several compromises to federal systems. Nevertheless, despite the effectiveness of the cybersecurity solutions, federal systems can still be compromised. Indeed, the record includes information on the compromise of [...] network between [...] even though CSE's cybersecurity solutions had been deployed and eventually led the detection of the breach.

36. The second reason supporting the Minister's conclusions that the activities are reasonable relates to the existing cyber threat landscape. As explained by the Minister, cyber threats from sophisticated criminals and state-sponsored actors against federal systems are becoming more frequent and more sophisticated. Threat actors employ effective techniques and leverage a multitude of entry points and methods to infiltrate the information infrastructures at the host, network or cloud level.

37. Further, federal systems are large and complex, having been created and maintained for different purposes and by various parties over the years. Information security practices in each federal institution differ considerably, creating an increased risk from cyber threats. By using the large amounts of information it acquires through its cybersecurity solutions and through further analysis of anomalous activity, CSE is able to detect and proactively protect against threats that federal institutions would not be able to identify on their own. As stated by the Minister, this results in "an across-the-board hardening of federal systems and [designated] systems of importance. CSE's cybersecurity techniques form part of a protective ecosystem, where the identification of one threat results in protection to everyone."

38. I am satisfied that the Minister has established a sufficient factual basis of the threat to the federal systems. The conclusions demonstrate that there is a rational connection between the activities specified in the Authorization and the objective of protecting federal systems from mischief, unauthorized use or disruption. The record also shows that CSE's activities are not only necessary to help protect federal systems but that they also serve as a privacy protection

measure given their effectiveness in preventing and mitigating compromises. 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

39. The Minister concluded at paragraph 20 of the Authorization that he had reasonable grounds to believe the activities authorized at paragraph 50 of the Authorization are "proportionate given the manner in which they are conducted." The Minister puts forward the same measures and controls listed in last year's authorization (CSE-2024-02), now divided into statutory requirements and additional internal measures and controls. He identifies the reasons for which the activities are necessary and useful, notably for acquiring information to help protect federal systems and to support other CSE activities. He recognizes that the authorized activities can lead to large volumes of information being acquired across multiple platforms in order to look for threats. However, the Minister notes that CSE retains only a very small percentage of the total amount of data initially acquired. I am satisfied that the Minister's conclusions in this regard are reasonable with respect to the authorized activities.

40. With regard to the measures and controls, I can trace the Minister's rationale for relying on them and I am satisfied that they are reasonable. First, the Minister recognizes that CSE is granted extensive access to federal systems. To be effective in conducting cybersecurity activities, CSE must acquire a large amount of information including files, emails and chat messages in which Canadians and persons in Canada have a reasonable expectation of privacy. The measures that support his conclusions relating to proportionality will be applied subsequent to the acquisition of information because CSE must first acquire the information for the cybersecurity solutions to be effective.

41. Second, CSE employs multiple layers of internal controls to protect the information it acquires. For example, access to the 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, and CSE's internal compliance program has established a process for responding to incidents.

42. When considering the objective and nature of the activities, the Minister also conducted a balancing exercise of what he considers are important interests, namely the acquisition of information and the protection of privacy of Canadians and persons in Canada. He explains how the activities seek to achieve a reasonable balance between cybersecurity objectives and the potential impairment of privacy interests. The Minister was aware of the privacy interests at issue and laid out the measures in place to protect them. Should information in which Canadians or persons in Canada have a privacy interest be acquired and retained, access to it and its use would be limited.

43. Finally, the Minister's balancing exercise is evident in his discussion of federal laws that have the potential to be contravened. He explains that there is a remote possibility that offences of the *Criminal Code* 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. He indicates that they are limited in number because the activities would take place only on the systems of consenting federal institutions. 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 federal systems and designated systems of importance to the Government of Canada. If there is a contravention of an Act of Parliament not listed in the Application – for example where CSE knows beforehand that the activities will result in a contravention of an Act of Parliament not listed in the Application or when CSE contravenes an Act of Parliament not listed, without prior knowledge – the Chief will inform both the Minister and the Intelligence Commissioner.

44. For these reasons, I am satisfied that the privacy interests of Canadians and persons in Canada were considered and the balancing conducted is reasonable. Also, I am satisfied that when an Act of Parliament is breached, the impact of the breach will be limited. Consequently, I find that the Minister's conclusions in relation to the proportionality of the activities are reasonable.

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

45. When the Minister finds that the activities are reasonable and proportionate pursuant to subsection 34(1) of the *CSE Act*, the Minister may issue a cybersecurity authorization if he concludes that there are reasonable grounds to believe that the four conditions set out at subsection 34(3) of the *CSE Act* are met, namely that:

i. any information acquired under the authorization will be retained for no longer than is reasonably necessary;
ii. the consent of all persons whose information may be acquired could not reasonably be obtained;
iii. any information acquired under the authorization is necessary to identify, isolate, prevent or mitigate harm to federal institutions' electronic information or information infrastructures; and
iv. the measures referred to in section 24 of the *CSE Act* will ensure that information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to identify, isolate, prevent or mitigate harm to federal institutions' electronic information or information infrastructures.

i. Any information acquired under the authorization will be retained for no longer than is reasonably necessary (s 34(3)(a))

46. The Minister's conclusions establish a connection between the types of information and their retention period. They also explain why the different retention periods are necessary for operational reasons. Information is retained in accordance with requirements set out in the MPS as well as the *Privacy Act,* RCS, 1985, c P-21 and the *Library and Archives of Canada Act*, SC 2004, c 11, and is governed by a retention schedule.

47. CSE employs multiple internal measures to ensure protection of the information it acquires and to maintain strong privacy protection. Acquired information initially goes through automated processes to determine whether CSE should retain it because it is necessary or essential for cybersecurity purposes. If the information is not initially flagged as necessary or essential, it is classified as unassessed information. The Minister explains that unassessed information is retained for a maximum of […] to allow CSE to use it to examine newly discovered vulnerabilities over time. The Minister outlines safeguards in place to ensure that this retention period is respected.

48. Pursuant to the MPS, this information must be strictly controlled and access limited to approved personnel authorized to conduct or support cybersecurity activities. Further, the list of personnel is tracked for accountability purposes and unassessed information cannot be shared beyond CSE.

49. The "necessary" criterion applies to information that does not relate to Canadians or persons in Canada, while the "essential" criterion applies to information that does. In essence, information is considered necessary to identify, isolate, prevent, or mitigate harm to federal systems when it is required for the understanding of malicious cyber activity, […], for the purpose of helping to protect federal systems. This information […].

50. IRtC is considered essential when without it, CSE would be unable to identify, isolate, prevent, or mitigate harm to federal systems. It may include […]. The information acquired may be highly sensitive to Canadians and persons in Canada and most analysis is done through automated processes, which flag abnormal behaviour and limit employees' exposure to the contents of the files.

51. Information that is determined to be necessary or essential may be retained until the information is no longer useful for these purposes, […]. Pursuant to the MPS, this information must be tracked. In addition, CSE's internal compliance program responds to incidents and circulates quarterly reminders to cybersecurity analysts to ensure that information that has not been assessed as necessary or essential is deleted within […] of acquisition. In addition, operational managers "must review" retained recognized IRtC on a quarterly basis to revalidate whether it is still essential. Information that is no longer essential must be deleted.

52. I note that there remains a discrepancy with the updated MPS which now includes a reference to the quarterly review indicating that operational managers "are reminded to review" recognized IRtC to revalidate whether it is still essential. I have previously raised that the record could benefit from greater clarity with respect to the different language used in relation to the quarterly review in an earlier cybersecurity decision (CSE-2025-01).

53. 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 evolving tradecraft of malware threat actors. This allows for better protection of federal systems as well as designated systems of importance.

54. Given the measures to protect IRtC and to limit 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 federal systems may be retained until it is no longer useful.

ii. The consent of all persons whose information may be acquired could not reasonably be obtained (s 34(3)(b))

55. Prior to deploying its cybersecurity solutions, CSE obtains the consent in writing of the owners of the federal systems who provide CSE permission to access their systems. Also, in accordance with standard government practice, federal system owners must advise their users – notably, employees – that their work devices and network activities are being monitored for cybersecurity and information assurance purposes.

56. As explained by the Minister, "[b]y acknowledging this notification, users demonstrate their consent to the federal system owner with whom CSE has an agreement to provide these cybersecurity services." However, there are instances where it is impossible to obtain the consent of individuals whose information may be acquired by CSE while conducting cybersecurity activities. This includes for example consent of individuals communicating with federal government employees by email or through a chat-based application. To address this issue which was raised in my previous decision CSE-2024-02, CSE has endeavoured to assess the feasibility of providing notice to external users, which in my view would be valuable.

57. I find that the Minister's conclusion with respect to this condition is reasonable.

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

58. CSE cannot predict which network traffic, files or processes will be, or are, maliciously used. To effectively monitor the federal systems and mitigate any potential cyber threats, CSE must acquire a vast range of information including network traffic, files, emails and chat messages. While the contents of files and communications may appear legitimate to the recipient, they may include malicious code or links that allow the threat actor to install malware on a target's computer.

59. The Minister explains and provides examples of how threat actors disguise their malicious activities and behaviours to reduce the likelihood of detection. CSE cannot achieve the same outcomes by using different cybersecurity solutions that acquire less information, IRtC included. Accordingly, the cybersecurity solutions are effective only because of the acquisition of "any" information.

60. The Minister's conclusions provide examples of 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. However, before IRtC 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.

61. The Minister has explained why he has reasonable grounds to believe that the acquisition of the information is necessary to identify, isolate, prevent or mitigate harm to the federal systems. Consequently, I am satisfied that the Minister's conclusions to that effect are reasonable.

iv. Measures to protect privacy will ensure that information acquired under the authorization identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to identify, isolate, prevent or mitigate harm to the federal institutions' electronic information or information infrastructures (s 34(3)(d))

62. As the federal systems are located in Canada, CSE will certainly incidentally acquire IRtC, including information that interferes with the reasonable expectation of privacy of Canadians and persons in Canada. Section 24 of the *CSE Act* requires CSE to have measures in place to protect the privacy of Canadians and persons in Canada in the use, analysis, retention and disclosure of information related to them acquired in the course of the cybersecurity aspect of its mandate. At paragraph 41 of the Authorization, the Minister concludes that he has reasonable grounds to believe that the measures referred to in section 24 will ensure that IRtC will be used, analysed, or retained only if it is essential.

63. As explained by the Minister, the MPS sets out elaborate policies to control and safeguard IRtC that is acquired pursuant to a cybersecurity authorization. Prior to handling this type of information, CSE employees must receive training, covering the applicable legal and policy requirements. Appropriate access to unassessed information is also granted to a limited number of personnel in governance and accountability roles. IRtC is also only provided to CSE employees on a need-to-know basis for the purpose of their work. IRtC acquired under the Authorization must be assessed as "essential" prior to being used, analyzed or retained, and the rationale for retention must be recorded. Determining whether information is essential can be the result of either a manual or an automated process.

64. The MPS also outlines the privacy measures that are in place to protect the privacy of Canadians and persons in Canada when information related to them is disclosed to other government departments or partners. For example, personal information may be suppressed so that any reporting does not identify the identity of an individual. Further, IRtC may only be disclosed if the recipient or class of recipients have been designated by Ministerial Order (s 45, *CSE A*ct), and CSE concludes that the disclosure is necessary to protect federal institutions and designated systems of importance (s 44, *CSE Act*).

65. In my view, when followed, these measures provide an effective manner for CSE to respect its legal and policy obligations to safeguard the privacy of Canadians and persons in Canada and ensure information relating to them is used only where essential. Consequently, I am satisfied of the reasonableness of the Minister's conclusion that he has reasonable grounds to believe that information related to a Canadian or a person in Canada will only be used, analysed or retained if essential to identify, isolate, prevent or mitigate harm to the federal institutions' systems.

V. REMARKS

66. I would like to make the following remark to assist in the consideration and drafting of future of ministerial authorizations. It is intended to clarify a previous remark and does not alter either my current or past findings regarding the reasonableness of the Minister's conclusions.

A. Clarification of remark made in Decision CSE-2024-02

67. CSE included in the record […] a remark I made in last year's decision that I would like to clarify.

68. The remark acknowledged and summarized the rationale CSE put forward in response to an earlier remark I made in Decision CSE-2023-01. That earlier remark raised the issue that CSE was no longer seeking a ministerial authorization for a certain activity that the previous Intelligence Commissioner had not approved, but that CSE was apparently nevertheless conducting. Certain elements of CSE's rationale, in my view, could have been interpreted as suggesting that if CSE determined that an activity did not involve the acquisition by CSE of information from the global information infrastructure (GII), it could proceed not only without a ministerial authorization, but also without considering whether the acquisition of that information would interfere with the reasonable expectation of privacy of Canadians or persons in Canada. I therefore emphasized that where CSE determines that activities do not require a ministerial authorization because they do not involve the acquisition by CSE of information from the GII – and are therefore not subject to the Intelligence Commissioner's

review – CSE must nevertheless still also examine whether those activities will lead to the acquisition of information that would interfere with the reasonable expectation of privacy.

69. In explaining my remark, at paragraph 81 of last year's decision (CSE-2024-02), I stated that "publicly available information acquired for the purposes of section 17 of the CSE Act cannot incidentally contain Canadian-related information. Indeed, pursuant to subsection 23(4), the lawful authority to incidentally collect Canadian-related information is limited to activities carried out under an authorization" (emphasis added). […], I recognize that this passage should have referred not to "Canadian-related information", but instead more specifically to "information in respect of which Canadians or persons in Canada have a reasonable expectation of privacy" (emphasis added). The former is admittedly a broader category of information than the latter. The latter reflects what my remark sought to communicate. Correspondingly, the reference to subsection 23(4) should properly have been a reference to subsection 22(4).

70. I thank CSE and the Minister for including […] highlighting the need for clarification. As remarks are made to improve the content of future authorizations or to highlight an issue for consideration by CSE, the clarification does not affect my assessment of the reasonableness of the Minister's conclusions under review in that decision.

71. The main thrust of my remark also does not change: where an activity does not require a ministerial authorization, the issue of whether it will lead to the acquisition of information that interferes with the reasonable expectation of privacy of Canadians or persons in Canada must nevertheless remain central to CSE's decision to conduct the activity or not. Indeed, this analysis is required to determine whether rights under section 8 of the *Charter* – which offers protections against unreasonable searches and seizures – could be infringed. […], there is an explicit recognition that appropriate measures must be in place to prevent the incidental acquisition of information that interferes with the reasonable expectation of privacy of Canadians when conducting activities outside of the framework of a ministerial authorization.

72. [...] also provides examples of certain activities and corresponding measures to prevent such incidental acquisition. Without suggesting in any way that this was CSE's intent, I wish to clarify that the fact such examples are present in the record before me does not mean that they have a stamp of approval from the Intelligence Commissioner. I end by reiterating a comment I made in last year's remark, which is that in situations where there may be uncertainty as to whether an authorization is required or not, it is reasonable to err on the side of caution.

VI. CONCLUSIONS

73. Based on my review of the record, I am satisfied that the Minister's conclusions made under subsections 34(1) and (3) of the *CSE Act* in relation to activities and classes of activities enumerated at paragraph 50 of the Authorization are reasonable.

74. I therefore approve the Minister's Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures dated February 23, 2025, pursuant to paragraph 20(1)(a) of the *IC Act*.

75. 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.

76. 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.

April 16, 2025

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner