~~SECRET//CEO~~

File: 2200-B-2024-02

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*

MAY 14, 2024

Canada

TABLE OF CONTENTS

I. OVERVIEW

1. This is a decision reviewing the conclusions of the Minister of National Defence (Minister) in relation to a cybersecurity authorization issued pursuant to the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*).

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. In addition, when conducting cybersecurity activities to protect federal infrastructures, CSE may incidentally acquire communications and information that interfere with the reasonable expectation of privacy of a Canadian or a person in Canada.

4. Prior to proceeding with activities that may have these effects, CSE is required to obtain a cybersecurity authorization issued by the Minister and approved by the Intelligence Commissioner. Pursuant to the *Intelligence Commissioner Act*, SC 2019, c 13, s 50 (*IC Act*), the Intelligence Commissioner approves the activities or classes of activities specified in the ministerial authorization if satisfied that the Minister's conclusions are reasonable.

5. On April 18, 2024, pursuant to subsection 27(1) of the *CSE Act*, the Minister issued a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures (Authorization). It is the sixth year the Minister has issued an authorization for this purpose.

6. On April 19, 2024, the Office of the Intelligence Commissioner received the Authorization for my review and approval under the *IC Act*.

7. Based on my review and for the reasons that follow, I am satisfied that the Minister's conclusions made under subsections 34(1) and (3) of the *CSE Act* in relation to activities and classes of activities enumerated at paragraph 42 of the Authorization are reasonable.

8. Consequently, pursuant to paragraph 20(1)(a) of the *IC Act*, I approve the ministerial Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures.

II. CONTEXT

9. 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 of CSE's cyber protection activities carried out to protect federal systems – consisting of networks and systems, the devices connected to them and diverse combinations of hardware and software – is set out in past Intelligence Commissioner decisions relating to cybersecurity.

10. As part of the cybersecurity and information assurance aspect of its mandate, CSE may obtain a ministerial authorization that allows it to access a federal institution's infrastructure (federal systems) to conduct cybersecurity activities to protect the institution's electronic information and infrastructure from mischief, unauthorized use and disruption. The ministerial authorization also allows CSE to acquire, use, analyse, retain and disseminate information originating from, directed to, stored on or being transmitted on or through that infrastructure including information related to Canadians and persons in Canada (s 27(1), *CSE Act*), which must be treated with special attention (s 34(3)(d) *CSE Act*).

11. A ministerial authorization grants CSE the lawful authority to carry out cybersecurity activities that contravene laws of Canada or that lead to the incidental acquisition of information that infringes on the reasonable expectation of privacy of a Canadian or a person in Canada (s 22(4), *CSE Act*). Indeed, to understand vulnerable entry points and compromises of federal systems, it is necessary for CSE to access and acquire information on those systems.

12. 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 (s 34, *CSE Act*). The authorization is valid for up to one year following the Intelligence Commissioner's approval (s 28(1), *CSE Act*). It is only then that CSE may carry out the authorized activities.

13. Even with a cybersecurity authorization, CSE is prohibited from directing its activities at a Canadian or any person in Canada and infringing a right guaranteed by the *Canadian Charter of Rights and Freedoms* (*Charter*) (s 22(1), *CSE Act*). Past cybersecurity authorizations have confirmed that CSE's cybersecurity activities target cybersecurity threats rather than any particular individual.

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

    a) The Authorization dated April 18, 2024;
    b) Briefing Notes from the Chief of CSE to the Minister dated March 22, 2024 and December 11, 2023;
    c) The Chief of CSE's Application dated March 22, 2024, including five 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) Outcomes Report for 2023;
        iv) Mission Policy Suite for Cybersecurity approved February 28, 2022; and
        v) Retention and Disposition Table.
    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 2024.

III. STANDARD OF REVIEW

15. Pursuant to section 12 of the *IC Act*, the Intelligence Commissioner conducts a quasi-judicial review of the Minister's conclusions on the basis of which certain authorizations, in this case a cybersecurity authorization, are issued to determine whether they are reasonable.

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

17. As indicated by the Supreme Court of Canada, when conducting a reasonableness review, a reviewing court is to start its analysis by examining the reasons of the administrative decision maker (*Mason v Canada (Citizenship and Immigration)*, 2023 SCC 21 at para 79). In *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 [*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.

18. Relevant factual and legal constraints can include the governing statutory scheme, the impact of the decision and principles of statutory interpretation. Indeed, to understand what is reasonable, it is necessary to take into consideration the context in which the decision under review was made as well as the context in which it is being reviewed. It is therefore necessary to understand the role of the Intelligence Commissioner, which is an integral part of the statutory scheme set out in the *IC* and *CSE Acts*.

19. A review of the *IC Act* and the *CSE Act*, 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 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 important privacy

and other interests of Canadians and persons in Canada were appropriately considered and weighed as well as to ensure that the rule of law is fully respected.

20. When the Intelligence Commissioner is satisfied (*convaincu* in French) that the Minister's conclusions at issue are reasonable, he "must approve" the authorization (s 20(1)(a), *IC Act*). Conversely, where unreasonable, the Intelligence Commissioner "must not approve" the authorization (s 20(1)(b), *IC Act*).

IV. ANALYSIS

21. On March 22, 2024, 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 that infrastructure to protect it from mischief, unauthorized use or disruption. As these activities may contravene Canadian laws or interfere with the reasonable expectation of privacy of Canadians or persons in Canada, an authorization issued by the Minister, and approval by the Intelligence Commissioner, is required.

22. The Application describes the nature and objectives of the cybersecurity solutions deployed by CSE on federal systems. These consist of deploying three types of sensors (referred to as cybersecurity solutions) to different levels of the federal systems to gather raw client data (i.e., unassessed data acquired under an authorization or obtained through client disclosures). They include: (1) host-based solutions (HBS) – sensors installed on physical or virtual end-point devices (e.g., workstations, mobile devices and servers); (2) network-based solutions (NBS) – sensors installed at the network level thereby giving CSE access to all network traffic and automatically taking mitigation actions; and (3) cloud-based solutions (CBS) – capabilities similar to HBS and NBS in a cloud environment.

23. The raw client data is then […]. CSE obtains the federal institutions' consent prior to deploying its sensors on their systems.

24. The cybersecurity solutions provide multiple layers of defence that are informed by threat information and analysis of anomalous activity. In addition, the Application 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.

25. Based on the facts presented in the Application submitted by the Chief of CSE, the Minister concluded, in accordance with subsection 33(2) of the *CSE Act*, that there were 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.

26. As a result, the Minister authorized CSE to carry out the activities, which are set out at paragraph 42 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.

27. The cybersecurity solutions set out in the Authorization are the same as those I approved in last year's ministerial authorization. As established by the jurisprudence of the Intelligence Commissioner and reiterated recently in my decision in another matter relating to CSE (Decision 2200-B-2024-01), the fact that some of the same activities have been approved in the past does not change the legal requirements that have to be satisfied for the Intelligence Commissioner to find the Minister's conclusions reasonable. The Minister must be provided with the best available information when determining whether to authorize activities. Indeed, the record should reflect the fact that it is a new and distinct authorization and include the most current operational activities undertaken by CSE. When determining the reasonableness

of the Minister's conclusions, the Intelligence Commissioner may consider how the record addresses past remarks made in prior decisions.

28. When compared to the record received last year, I am satisfied that the current record does in fact reflect that this is a new and distinct authorization. I recognize the efforts made by CSE to address not only past remarks made in this file but also those made in other cybersecurity and foreign intelligence matters. The record reflects key updates relating to additional details on the nature, frequency, and volume of retained information relating to a Canadian or a person in Canada; the impacts of automated malware testing and clarification of the mitigation measures implemented; and clarification on how consent is obtained by users of the Government of Canada electronic information systems.

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 made under subsections 34(1) and (3) of the *CSE Act*, on the basis of which the authorization was issued under subsection 27(1) of the *CSE Act*, are reasonable.

A. Subsection 34(1) of the *CSE Act* – Determining whether the activities are reasonable and proportionate

i. The meaning of reasonable and proportionate

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*).

31. The Minister must conclude that any activity that would be authorized by the Authorization is reasonable and proportionate by applying his understanding of what those thresholds entail. Determining whether an activity is reasonable and proportionate is a contextual exercise and the Minister may consider a number of factors. The Intelligence Commissioner must determine whether the Minister's conclusions, which include his understanding of the

thresholds, are "reasonable" by applying the reasonableness standard of review, explained previously.

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

32. The Minister concluded, at paragraph 13 of the Authorization, that he had reasonable grounds to believe that the activities were reasonable given the objective to help protect federal systems.

33. To fulfill its mandate related to cybersecurity and information assurance, CSE must acquire information located on the federal institutions' electronic infrastructures in Canada. In issuing the Authorization, as in previous cybersecurity authorizations for activities on non-federal infrastructures, the Minister implicitly accepted that the cybersecurity activities would not contravene the legislative prohibition against deliberately seeking information relating to, and directing activities at, a Canadian or a person in Canada (ss 22(1), 23(4) and (5), *CSE Act*.) As indicated in Decision 2200-B-2023-06 this logically entails that any information related to Canadians or persons in Canada acquired through these activities is not deliberatively sought, but rather incidentally acquired. This is a reasonable interpretation, in my view.

34. Nevertheless, it is important to note that the federal systems are located in Canada and the vast majority of information stored on them, by its nature, 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, but also includes information from members of the Canadian public who, for example, communicate with the institutions by email. As a result, CSE's cybersecurity activities will necessarily lead to the acquisition of Canadian-related information and effective implementation of measures, safeguarding and protecting this information is paramount.

35. The Minister justifies that the authorized activities are reasonable for two main reasons: CSE's involvement in the cybersecurity response is required as compromises are becoming

increasingly difficult to detect and combat, leaving the cyber posture of federal systems at risk; and the activities for which the authorization is sought are effective.

36. With regard to the first reason, the Minister explains and the record shows that cyber threats from sophisticated criminals and state-sponsored actors on federal institutions 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 infrastructure at the host, network or cloud level. Further, federal systems are large and complex having been created and maintained by various parties over the years. Information security practices in each federal institution differ greatly and therefore present an increased risk from cyber threats. With the large amount of information acquired through its cybersecurity solutions and further analysis of anomalous activity, CSE is able to detect and defend against threats that federal institutions would not be able to identify on their own. As part of a protective ecosystem, the information acquired through CSE's activities not only benefits federal systems, but is also beneficial for non-federal systems receiving assistance from CSE.

37. As for the effectiveness of CSE's activities, advanced malware analysis tools and automated cybersecurity capabilities provided by CSE allow for multiple layers of defence to detect and prevent intrusions. The information acquired through these activities help CSE to identify, isolate, prevent or mitigate harm to federal systems.

38. As indicated in the Outcomes Report which provides some details about the effectiveness of the cybersecurity solutions over the course of the previous cybersecurity authorization for federal infrastructures, CSE detected [...] malicious events on federal systems. The effectiveness of the cybersecurity solutions is critical for CSE to prevent or mitigate compromises. As indicated in the jurisprudence of the Intelligence Commissioner (Decision 2200-B-2023-02), CSE may not only access federal systems and acquire information, but it also has the legal authority to conduct mitigation actions (s 23(3)(a), *CSE Act*).

39. With respect to the activities described at paragraph 42 of the Authorization, I find reasonable the Minister's conclusions that they are reasonable. 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 shows that the specific activities contribute to CSE's cybersecurity and information assurance mandate. The Minister understood and explains how the activities set out in the Authorization are necessary to help protect federal systems.

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

40. The Minister also concluded at paragraph 16 of the Authorization that he had reasonable grounds to believe the activities authorized are "proportionate given the manner in which they are conducted."

41. I am again satisfied that the Minister's conclusions in this regard are reasonable with respect to the authorized activities described at paragraph 42 of the Authorization. The Minister identifies the reasons for which the activities are necessary and useful, notably for acquiring information to help protect federal systems and support other CSE activities. He recognizes that the activities can lead to acquiring large volumes of information across multiple platforms to look for threats. However, the Minister notes that CSE retains only a very small percentage of the total amount of data initially acquired.

42. The Minister puts forward the following measures and controls to show that the activities are proportionate:

a) the cybersecurity solutions acquire and use information that is necessary for identifying, isolating, preventing, or mitigating harm to federal systems;
b) acquired information is copied and stored by CSE where cybersecurity analysts can identify malicious activity and search retroactively for instances of the same malicious activity occurring elsewhere. No unassessed information is retained for longer than […] from the date upon which it was acquired;
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 operational policy;

d) while CSE's cybersecurity solutions acquire a broad range of information in order to better protect federal systems, CSE retains less than 1% of the total amount of data initially acquired through cybersecurity solutions;
e) acquired information identified as related to a Canadian or person in Canada will be used, analysed, and retained only if it is assessed as essential to identify, isolate, prevent, or mitigate harm to federal systems;
f) acquired information that does not relate to a Canadian or person in Canada will be retained only when the information is assessed as necessary to identify, isolate, prevent, or mitigate harm to federal systems;
g) every search performed on the acquired unassessed information is auditable to comply with section 11.3 of the Mission Policy Suite for Cybersecurity (MPS Cybersecurity) – the collection of policies that apply to cybersecurity activities. Audit logs are retained for a minimum of […] for review and oversight purposes;
h) using security controls, 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;
i) all cybersecurity tools are reviewed for legal and policy compliance; and,
j) the same conditions apply to information used by CSE for the purposes of identifying, isolating, preventing, or mitigating harm to systems of importance [non-federal systems].

43. As indicated in two decisions on cybersecurity authorization for a non-federal entity (Decisions 2200-B-2023-05 and 2023-06), the measures set out in paragraphs a) b) e) and f) do not provide much support to the Minister's conclusions that the activities are proportionate because they are distinct statutory conditions that must be separately satisfied at subsection 34(3) of the *CSE Act*. The Minister cannot satisfy one statutory requirement (the activities are proportionate at 34(1)) by relying on satisfying separate statutory requirements (information will only be acquired if necessary; information will not be retained

longer than necessary; information will only be retained if necessary; Canadian-related information will only be retained if essential at 34(3)).

44. As evidenced by the other measures in the list, the Minister largely relies on the measures applied to information after it has been acquired to support his conclusion on proportionality. This raises the question of whether the Minister sufficiently considered whether measures could be applied prior to acquiring the information in determining whether the cybersecurity activities are proportionate.

45. A reasonable decision is one that is justified in light of the facts (*Vavilov*, para 126). Even where there is no explicit mention of certain facts in the decision, a reviewing court must be able to trace the decision maker's reasoning (*Vavilov*, para 102). In the case at hand, I find that I can trace the Minister's rationale for relying on measures to be applied after acquiring the information in his proportionality analysis, rather than on measures that could be applied prior to this acquisition.

46. First and foremost, he recognizes that 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 after the information is acquired because it is necessary to acquire the information in the first place. Second, access to the information acquired 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 aware of the privacy interests at issue and laid out the measures in place to protect them. Consequently, he came to the conclusion that the proposed activities justify any potential impairment of Canadian privacy interests.

47. I am satisfied that the Minister conducted a balancing exercise taking into account the objective and nature of the activities where he identified what he considers are important interests, namely the acquisition of information and the protection of privacy of Canadians and persons in Canada. He also explains how the activities sought to achieve a reasonable

balance between them. I am satisfied that the interests were considered and the balancing conducted is reasonable.

48. I also find that the Minister considered the effects of the activities on the rule of law. He explains that there is a remote possibility that offences beyond those listed in the Application may be committed, and other Acts of Parliament may be contravened, depending on the circumstances of the activity undertaken. Should CSE know beforehand that the activities will result in a contravention of an Act of Parliament not listed in the Application, the Minister will be notified by the Chief and she will subsequently inform me. The record identifies the provisions of the various Acts of Parliament that have the potential to be contravened and as indicated in previous cybersecurity decisions, since CSE will have the consent of the federal institutions to access their systems, the potential offences are limited in number and in impact on Canadians and persons in Canada. I am satisfied that when an Act of Parliament is breached, the impact of the breach will be limited.

49. Finally, the Minister's conclusions clearly reflect his understanding of the privacy interests at issue and the measures in place to protect them. Should information that may contain a Canadian privacy interest be acquired and retained, access to it and its use would be limited. As a result, I am satisfied that the Minister's conclusions in relation to the proportionality of the activities is reasonable.

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

50. 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 authorization for cybersecurity to help protect federal systems 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:

a) any information acquired under the authorization will be retained for no longer than is reasonably necessary;

b) the consent of all persons whose information may be acquired could not reasonably be obtained;

c) any information acquired under the authorization is necessary to identify, isolate, prevent or mitigate harm to federal institutions' electronic information or information infrastructures; and

d) 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))

51. The Minister explains that information will only be retained to further the cybersecurity and information assurance aspect of CSE's mandate. The information is retained in accordance with requirements set out in CSE policies and governed by a retention schedule for the different categories of information that may be acquired. He also 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.

52. The Minister's rationale establishes a connection between the types of information and their retention period and explains why the different retention periods are necessary for operational reasons. Even though acquired information initially goes through automated processes to determine whether CSE should retain it because it is necessary or essential for cybersecurity purposes, the Minister explains CSE must be able to retain information that has not been identified as useful for a […] period. A […] assessment period is needed for CSE to analyse the information in the case of a cyber event and examine its evolution over time.

53. As explained in the record, keeping the information for a […] period allows CSE to compare newly discovered vulnerabilities against its unassessed information and determine whether they exist within the federal systems. The record provided an example where the ability for CSE to "go back in time" enabled CSE analysts, following an identified vulnerability within the impacted federal systems to identify the threat and take immediate mitigation actions. Comparing a compromise against unassessed data or undetected threat activities helps CSE develop better mitigation actions and defences that can also be used for federal systems and non-federal systems.

54. Unassessed information will automatically be deleted prior to the expiry of the […] period. In addition, CSE's internal compliance program circulates quarterly reminders to cybersecurity analysts to ensure that information that has not been assessed as necessary or essential is deleted within […] of acquisition.

55. While the "necessary" criterion applies to information that does not relate to a Canadian or a person in Canada, the "essential" criterion applies to information that relates to a Canadian or a person in Canada.

56. As defined in the Authorization, 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. By its nature, this information is inherently less sensitive than information determined to be "essential" as it does not contain any information relating to Canadians or persons in Canada. Indeed, it includes […]. This type of information assists in developing detection and prevention analytics and further strengthens the cyber defence ecosystem. Hence, this information can retain its usefulness indefinitely.

57. 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 federal systems. This may include […]. The information acquired may be highly sensitive to Canadians and most analysis is done through automated processes, which flag abnormal behaviour and limit employees' exposure to the content of the files.

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

59. Given the important restrictions on accessing unassessed information and the quarterly reminders sent to cybersecurity analysts through CSE's internal compliance program to assess the information within […] of its acquisition, I find the Minister's conclusion regarding the […] assessment period reasonable.

60. 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. Retaining information the length of time needed gives CSE the tools required to develop cyber defences that keep pace with the rapidly evolving tradecraft of malware threat actors. This allows for better protection of federal systems as well as non-federal systems.

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

61. 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.

62. Federal system owners must, in accordance with standard government practice, advise their users – notably, employees of federal institutions – that their electronic devices and network activities are being monitored for cybersecurity and information assurance purposes. 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."

63. According to the Minister, there are, however, instances where it is impossible to obtain the consent of individuals whose information may be acquired by CSE while conducting cybersecurity activities. Indeed, consent of individuals communicating with federal government employees by email or through a chat based application cannot reasonably be obtained.

64. 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))

65. This condition underpins the activities for which authorization is sought. Given that it is not possible to know in advance which electronic information on the federal systems may be used maliciously, CSE must acquire a range of information including information that does not reveal the existence of a cyber threat. In so doing, CSE may incidentally acquire information that interferes with the reasonable expectation of privacy of Canadians and persons in Canada.

66. As indicated in the jurisprudence of the Intelligence Commissioner, the Minister is not a technical expert and he may rely on the Chief's assessment that this acquisition is necessary to identify, isolate, prevent or mitigate harm to federal systems when making conclusions. The Minister explained how threat actors disguise their malicious activities and behaviours to reduce the likelihood of detection and provided examples. The information acquired through the cybersecurity solutions are used to [...]. In sum, the cybersecurity solutions are effective only because of the acquisition of the information.

67. The Minister's conclusion and the record do not indicate whether CSE can achieve the same cybersecurity outcome by using different cybersecurity solutions that acquire less information related to Canadians. If such cybersecurity solutions were available and operationally feasible, I would expect CSE to provide that information to the Minister, as it would be an important element in his decision to issue an authorization, as well as impact my reasonableness review.

68. I am required to conduct my review based on the Authorization before me, and to determine whether the factual context justifies the Minister's conclusions on this issue. I am satisfied that 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. As a result, 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))

69. The Minister concludes that he has reasonable grounds to believe that the measures referred to in section 24 of the *CSE Act* will ensure that the information acquired that is identified as relating to Canadians or persons in Canada will be used, analysed, or retained only if essential to identify, isolate, prevent, or mitigate harm to federal systems or systems of importance to the Government of Canada.

70. The Minister's conclusions describe the measures in place to protect the privacy interests of Canadians and persons in Canada. He explains that in accordance with the *CSE Act*, when CSE's activities may involve the acquisition by CSE of information from the global information infrastructure (GII) that interferes with a reasonable expectation of privacy of Canadians and persons in Canada, it must conduct the activities under the authority of an authorization. To be clear, although the Authorization allows CSE to access federal systems – which are part of the GII – paragraph 42 of the Authorization does not seek authorization for CSE to acquire information from other parts of the GII. I will address this further in my remarks.

71. The Minister specifies that information relating to a Canadian or a person in Canada can only be retained if it is assessed to be essential. CSE restricts access to unassessed information to analysts working under the cybersecurity and information assurance aspect of its mandate. Further, all information is restricted using specified access controls. First, all persons must be employed by CSE, secondees, contractors, integrees, and personnel appointed to perform the powers, duties, and functions of CSE under the *CSE Act*. The information is provided on a need-to-know basis for the purpose of the person's work. Second, information that has not yet been assessed for necessity or essentiality is further limited to the persons or classes of persons listed in the Authorization who have a need-to-know for the purpose of conducting the activities specified in the Authorization. Prior to accessing this unassessed information, CSE employees must receive training, covering the legal and policy requirements that apply

to handling this type of information. Finally, appropriate access to the information is granted to a limited number of personnel in governance and accountability roles.

72. The MPS Cybersecurity sets out the measures that must be applied by CSE for the retention, use and disclosure of information related to Canadians or persons in Canada. Pursuant to section 8.2.2, CSE analysts conduct an "essentiality test" prior to the retention of the information acquired and records essentiality rationales. Determining whether information is essential can be the result of either a manual or an automated process. As set out in the Retention and Disposition Table, on a quarterly basis, operational managers must review the retained information and revalidate whether it is still essential. Information that is no longer essential must be deleted. As per the record, the Table will be incorporated in a future version of the MPS. Finally, CSE also has a compliance program which monitors that its operations comply with the MPS Cybersecurity as well as the conditions of the Authorization under which they are carried out.

73. 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 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, unsuppressed information may only be disclosed if the recipient or class of recipients have been designated by Ministerial Order (s 45, *CSE A*ct), and the disclosure is essential to international affairs, defence, security or cybersecurity, pursuant to section 43 of the *CSE Act*. I am of the view that the Minister's conclusions and the record would benefit from further explanation on the use of suppression measures when releasing Canadian identifying information.

74. Given the above, I am satisfied that Minister's conclusions are reasonable: there are appropriate measures in place for CSE to meets its legal and policy obligations to safeguard the privacy of Canadians and persons in Canada.

V. REMARKS

75. I would like to make four additional remarks to assist in the consideration and drafting of future of ministerial authorizations, which do not alter my findings regarding the reasonableness of the Minister's conclusions.

A. […]

76. In last year's decision relating to cybersecurity for federal infrastructures, I made a remark about […]. In summary, the former Intelligence Commissioner had not approved a particular activity […] and in the matter before me at that time, CSE was no longer seeking authorization for the activity on the basis that ministerial approval for the activity was not necessary – although CSE was conducting the activity in question. I raised a concern that there was a lack of explanation in that record explaining why CSE had abandoned its request for authorization for the activity that it was nevertheless carrying out. In Decision 2200-B-2023-05 relating to an authorization for cybersecurity for non-federal infrastructures, I noted that my concern remained unaddressed and that I expected CSE to provide a satisfactory response in the context of a future request for a cybersecurity authorization.

77. CSE has provided a response in the record before me by including information that aims to explain the basis of CSE's decision that it can carry out the activity without an authorization. In particular, the record includes a briefing note to the Minister from the Chief explaining the process undertaken by CSE following the previous IC's decision in June 2022 to determine that an authorization was not necessary, as well as two brief legal opinions supporting this position.

78. CSE's process was to […], obtained via disclosure or otherwise ingested by CSE for purposes of section 17 of the *CSE Act*. The purpose of this exercise was to determine which sources constituted […]. Based on the legal opinions, CSE concluded that […].

79. CSE identified […]. CSE then determined that the information acquired thus far […] does not risk interfering with a reasonable expectation of privacy, and the manner in which CSE queries the information […] does not risk interfering with the reasonable expectation of

privacy of a Canadian or a person in Canada. CSE also explains that in the unlikely event such information was acquired, it would be identified and deleted, as well as reported to the internal compliance team.

80. As indicated in the Analysis Section of this decision, […] is not included in the Authorization as an activity for which the Intelligence Commissioner's approval is required. In that sense, it falls outside my jurisdiction in this review. CSE has responded to my request to explain why it no longer sought ministerial authorization for […]. CSE has explained that the information it […] for cybersecurity purposes does not require a ministerial authorization.

81. I want to reiterate, however, that when CSE determines whether it may conduct an activity without a ministerial authorization, the *CSE Act* makes it clear that the primary concern is that no information in which Canadians have a reasonable expectation of privacy be collected. Thus, determining that the information was not […] would not necessarily be sufficient. Publicly available information, as defined by section 2 of the *CSE Act*, cannot include information in which Canadians or persons in Canada have a reasonable expectation of privacy. As a result, although subsection 23(4) of the *CSE Act* allows CSE to incidentally collect information related to a Canadian or a person in Canada when carrying out activities under a cybersecurity authorization, publicly available information acquired for the purposes of section 17 of the *CSE Act* cannot incidentally contain Canadian-related information. Indeed, pursuant subsection 23(4), the lawful authority to incidentally collect Canadian-related information is limited to activities carried out under an authorization.

82. I understand that the authorization for this activity was originally sought out of "an abundance of caution," in particular because there is an incongruity between sections 17 and 22(4) on the one hand, and section 27 on the other hand, of the *CSE Act*. CSE wishes to conduct its activities lawfully and it is reasonable to err on the side of caution when there may be uncertainty with regard to whether an authorization is required. Nevertheless, the required analyses should be conducted prior to seeking a ministerial authorization. When carrying out activities without a ministerial authorization, the appropriate measures must be in place to prevent the incidental acquisition of information that interferes with the

reasonable expectation of privacy of Canadians and persons in Canada. Reporting it to the internal compliance team after the fact is not sufficient.

83. I also note that I do not disagree with the Chief's assessment that there is an incongruity in the *CSE Act* and that a legislative amendment would bring clarity to CSE's activities in this sphere.

B. The language used in notices to users to obtain consent

84. The record does not include the actual language used in the notices to the users of the federal systems that the Minister relied on to demonstrate that the users of the federal systems had provided their consent for their information to be acquired for cybersecurity purposes. I am of the view that transparency towards all system users and those communicating with them is important. Thus, the notice to users should be clear that the information contained or shared on federal government devices and computer networks – including personal information – may be incidentally acquired and could be used, analysed, retained and disclosed for cybersecurity purposes. This includes private communications for which the originator has a reasonable expectation of privacy. While this statement may sound alarming, it is important for the users to understand what type of personal information may be retained and disclosed and the measures currently in place to protect their privacy. For example, although emails may be collected through the cybersecurity solutions, CSE's interest is in any anomalous behaviour related to emails rather than to their content. Further, prior to sharing information that is Canadian-related, CSE must conclude that the disclosure is necessary to help protect federal systems (s 44(1)(a), *CSE Act*) and meet its legal and policy obligations to safeguard the privacy of Canadians.

85. Therefore, I trust that CSE ensures that the owners of the federal systems are using language in their notices that inform their users of the extensive reach of the cybersecurity activities which could include the acquisition of private information.

86. Similarly, although I found reasonable the Minister's conclusions that consent may not reasonably be obtained from individuals whose information may be acquired by CSE while

conducting cybersecurity activities, I would encourage thinking of ways that notice to external users could be provided.

C. Outcomes – results and reports sent outside of CSE

87. The Outcomes Report sets out some details, including empirical data, about the outcomes of the authorization issued by the Minister and approved by me in 2023 – up to the time the Chief's Application was prepared. It provides a better understanding of the malicious events observed. The Report indicates that CSE issued […] cyber defence reports based on malicious activity and vulnerabilities identified through its cybersecurity solutions. The vast majority of the cyber defence reports, […] contained Canadian-related information, such as Canadian […]. As this is the first time that CSE provides the number of cyber defence reports issued and those containing Canadian-related information, I am unable to make comparisons with previous years. However, the Report indicates that during the authorization period, CSE detected […] malicious events on federal systems. In the outcomes report provided in last year's authorization, CSE had indicated that it had detected […] malicious events. I am of the view that if the volume or nature of the detected threats vary year over year, an explanation in the record would be useful for the Minister and myself as an element to consider in our respective decisions.

88. The Report indicates that when deemed necessary to help protect federal systems or systems of importance, CSE disclosed the reports to designated recipients (ss 44 and 45, *CSE Act*). However, there is no information with respect to the volume or the recipients of reports disclosed. I raised a similar issue in my decision rendered this year respecting foreign intelligence (Decision 2200-B-2024-01). While the Outcomes Report in that file contained a chart indicating which departments viewed the reports, there was no information on whether they were shared with international partners. I am similarly of the view here that the inclusion of more detailed information regarding the sharing of reports, particularly if they are shared with international partners and the treatment of the Canadian-related information when reports are shared, would be beneficial to the Minister and myself.

D. End of Authorization Report – Solicitor-client communications

89. As a legislative requirement, ninety days after the end of an authorization period, CSE must provide the Minister and the Intelligence Commissioner with a report on the outcomes of the activities carried out under the ministerial authorization (s 52(2), *CSE Act*).

90. During the review of this matter, my office requested CSE to provide me with a copy of the end of authorization report that was sent to the Minister following the end of the 2022 authorization period, which, I understand, had not yet been provided to me due to an oversight at CSE. I recognize that the report was not before the Minister when issuing the ministerial authorization (s 23, *CSE Act*). Nevertheless, I consider this report to be valuable to my review as it provides contextual content applicable in the matter before me and therefore make the following comments.

91. In the end of authorization report, CSE indicates that in 2023, it incidentally acquired solicitor-client communications. I note that it is the first time that CSE reports the incidental collection of solicitor-client communications in the context of a cybersecurity authorization. The report indicates that upon recognition of the communications, CSE engaged with internal policy and compliance, and the communications were immediately deleted and were not retained, used and analysed. I note that this incidental acquisition of communication was not described in the Outcomes Report, nor included in the record before me this year or last year. I would expect that such information be included in the record for the awareness of the Minister and myself.

92. I have stressed in previous decisions the importance of solicitor-client privilege and emphasized that whenever it must be pierced, the privilege be impaired in as minimal a way as possible (Decisions 2200-B-2022-05 and 2200-B-2023-01). I acknowledge that the incidental acquisition of communications occurred during the 2022 authorization period and CSE has since added details to the internal process to be followed when incidentally acquiring solicitor-client communications, namely to specify that access to the communications during the evaluation should be limited. From the brief and general process described in the end of authorization report – that internal policy and compliance team was

engaged – it is unclear whether the established process (in place at the time) was followed. The Minister issues authorizations, and the Intelligence Commissioner approves them, accepting that CSE's internal processes are appropriate to deal with solicitor-client privilege, and expects those processes to be followed. End of authorization reports should make it clear whether these processes were followed or not.

VI. CONCLUSIONS

93. 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 42 of the Authorization are reasonable.

94. I therefore approve the Minister's Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures dated April 18, 2024, pursuant to paragraph 20(1)(a) of the *IC Act*.

95. 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.

96. 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.

May 14, 2024

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner