~~**PROTECTED B**~~

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

File: 2200-B-2023-02

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*

JUNE 13, 2023

TABLE OF CONTENTS.

I. OVERVIEW

1. Cyber threats targeting Canadians and our federal institutions are a growing concern. Originating from cyber criminals or foreign state-sponsored actors, these attacks are increasing in number and in complexity. The Communications Security Establishment (CSE), Canada's national cryptologic agency, is the organization mandated to provide the Government of Canada with information technology security in the face of this increasing threat.

2. When carrying out its cyber protection activities, it may be necessary for CSE to contravene certain Canadian laws. In addition, when acquiring cybersecurity information related to the malicious activities occurring on federal information infrastructures, CSE may incidentally acquire communications or information that interfere with the reasonable expectation of privacy of a Canadian or a person in Canada.

3. However, conducting activities to protect federal institutions' electronic information and infrastructures from mischief and disruption by cyber threat actors should not provide CSE with a free pass to break Canadian laws and breach privacy interests of Canadians and persons in Canada. To that end, Parliament created a regime – cybersecurity authorization – with checks and balances that aims to provide CSE with the necessary latitude to be effective while ensuring respect for the rule of law and protection of Canadian privacy interests.

4. Specifically, this cybersecurity authorization regime allows CSE to contravene some Acts of Parliament or of any foreign state while conducting cybersecurity activities for the purpose of protecting electronic information and infrastructures belonging to federal institutions. In conducting its cybersecurity activities, the regime also allows CSE to acquire, use, analyse, retain and disseminate information related to Canadians and persons in Canada – but only if a number of conditions are met and specific steps are fulfilled. Past cybersecurity authorizations have shown that such retention and dissemination is extremely minimal, if not exceptional.
5. The authorization process originates with a written application by the Chief of CSE (Chief) to the Minister of National Defence (Minister) for a cybersecurity authorization that sets out, among other things, the grounds for which it is necessary as well as the activities that would

be authorized for CSE to carry out. The Minister may issue the cybersecurity authorization if, among other conditions, the Minister concludes the proposed activities are reasonable and proportionate.

6. A cybersecurity authorization becomes valid only after it is approved by the Intelligence Commissioner who must determine whether the Minister's conclusions on the basis of which the authorization was issued are reasonable.

7. On May 17, 2023, pursuant to subsection 27(1) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*), the Minister issued a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures (Authorization).

8. On May 18, 2023, 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*).

9. Based on my review and for the reasons that follow, I am satisfied that the Minister's conclusions made under subsection 34(1) and (3) of the *CSE Act* in relation to activities and classes of activities enumerated at paragraph 36 of the Authorization are reasonable.

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

II. LEGISLATIVE CONTEXT

A. *Communications Security Establishment Act*

11. In June 2019, *An Act respecting national security matters* (referred to as the *National Security Act, 2017*, SC 2019, c 13) came into force and established the Intelligence Commissioner. CSE's authorities and duties were also expanded through the creation of the *CSE Act*, which came into force in August 2019.

12. CSE is Canada's signals intelligence agency for foreign intelligence and technical authority for cybersecurity and information assurance. Its mandate includes cybersecurity and information assurance where CSE may, as described in section 17 of the *CSE Act*, provide advice, guidance and services to help protect federal institutions' electronic information and infrastructures – that is, federal systems – from cyber threats. Essentially, CSE may defend systems, devices and networks of federal institutions from the threat as well as provide advice and guidance that will strengthen their cybersecurity posture.

13. As defined by CSE, "federal systems" consist of networks and systems, and the devices connected to those networks and systems, and are additionally comprised of diverse combinations of hardware and software. "Federal institutions" include government departments, government agencies and Crown corporations.

14. While federal institutions rely on commercially available measures (e.g., anti-virus, firewall software) to protect their networks from a range of sophisticated cyber threat actors, they may also require the support of CSE to detect and protect malicious activities directed against these networks. To understand vulnerable entry points and compromises of federal systems, it is necessary to access, and acquire information on those systems. CSE accesses the systems and acquires this information for the purpose of helping the federal institutions only when requested, and must obtain the federal institutions' consent for doing so. The cybersecurity information acquired by CSE does not pertain to any particular person. Rather, it relates to the operation of, and threats to, information infrastructures.

15. As stipulated in subsection 27(1) of the *CSE Act*, CSE may access a federal institution's information infrastructure and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(e) of the *Criminal Code*, RSC 1985, c C-46 (*Criminal Code*), from mischief, unauthorized use or disruption. Paragraph 184(2)(e) of the *Criminal Code* renders inapplicable the offence of knowingly intercepting a private communication if the private communication is intercepted through a computer system and is

reasonably necessary for managing the quality of service of that computer system or to protect the computer system.

16. To access and acquire information passing through federal systems, CSE conducts technical cybersecurity activities using three types of sensors. The cybersecurity solutions are applied at different levels of the federal information infrastructure to detect and counter malicious cyber activity. They include: (1) host-based solutions (HBS) — sensors are installed on physical or virtual end-point devices (e.g., workstations, mobile devices and servers); (2) network-based solutions (NBS) — sensors are installed at the network perimeter thereby giving CSE access to all network traffic and automatically taking mitigation action; and (3) cloud-based solutions (CBS) — provides capabilities similar to HBS and NBS but sensors are deployed in a cloud environment. [describing how the data is processed] [redacted]

17. The *CSE Act* imposes a number of limitations and conditions on CSE when acquiring information on federal systems. Of significance, CSE's activities must not be directed at a Canadian or any persons in Canada. However, CSE may use and retain information relating to a Canadian or a person in Canada that was obtained in an incidental manner, that is when the information acquired was not itself deliberately sought (subsection 23(5) of the *CSE Act*). This incidental collection has been found to be exceptional as the results of past cybersecurity authorizations have shown. Also, pursuant to subsection 22(1) of the *CSE Act* the activities must not infringe the *Canadian Charter of Rights and Freedoms* (*Charter*). Furthermore, pursuant to section 24 of the *CSE Act*, CSE is required to have measures in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and information acquired through federal systems.

18. Finally, CSE's cybersecurity activities must not contravene any other Act of Parliament (section 50 of the *CSE Act* states that Part VI of the *Criminal Code* does not apply in relation to an interception of a communication under the authority of a cybersecurity authorization) or interfere with the reasonable expectation of privacy of a Canadian or a person in Canada unless,

as explicitly outlined in subsection 22(4) of the *CSE Act*, they are carried out under a cybersecurity authorization issued under subsection 27(1) of the *CSE Act* (subsection 22(3) of the *CSE Act*).

19. As a result, where CSE will contravene an Act of Parliament or interfere with the privacy of Canadians or persons in Canada while conducting cybersecurity activities, CSE must request that the Minister issue a cybersecurity authorization in accordance with subsections 22(4) and 27(1) of the *CSE Act*. In this written document, the Minister authorizes CSE to lawfully carry out the activities set out in the authorization even if they exceptionally may be found to contravene an Act of Parliament or interfere with a reasonable expectation of privacy of a Canadian or a person in Canada.

20. While section 33 of the *CSE Act* describes the requirements for CSE to apply for a ministerial authorization, subsections 34(1) and (3) of the *CSE Act* define the statutory conditions under which the Minister may authorize CSE's activities. The Minister may issue an authorization when satisfied that the statutory conditions have been met. This will be discussed further in the Analysis section of this decision.

21. The ministerial authorization is only valid once approved by the Intelligence Commissioner (subsection 28(1) of the *CSE Act*). It is only then that CSE may carry out the authorized activities specified in the authorization.

B. *Intelligence Commissioner Act*

22. Pursuant to section 12 of the *IC Act*, the role of the Intelligence Commissioner is to conduct 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.

23. Section 14 of the *IC Act*, relating to the issuance of a cybersecurity authorization, states that the Intelligence Commissioner must review whether the conclusions of the Minister made under subsections 34(1) and (3) of the *CSE Act*, on the basis of which the authorization was issued, are reasonable.

24. The Minister is required by law (section 23 of the *IC Act*) to provide to the Intelligence Commissioner all information that was before her as the decision maker. As established by the Intelligence Commissioner's jurisprudence, this also includes any verbal information reduced to writing, including ministerial briefings. The Intelligence Commissioner is not entitled to Cabinet confidences (section 26 of the *IC Act*).

25. In accordance with section 23 of the *IC Act*, the Minister confirmed in her cover letter that all materials that were before her to arrive at her decision have been provided to me. Thus, the record before me is composed of:

    a) The Ministerial Authorization dated May 17, 2023;
    b) The Chief's Application which includes four annexes dated April 28, 2023;
    c) The Mission Policy Suite for Cybersecurity approved February 28, 2022;
    d) The Briefing Note from the Chief of CSE to the Minister dated April 28, 2023;
    e) The Chief's Application which includes four annexes; and
    f) The Briefing Deck – Overview of the Activities.

III. STANDARD OF REVIEW

26. The *IC Act* instructs that the Intelligence Commissioner must review whether the Minister's conclusions are reasonable. The Intelligence Commissioner's jurisprudence establishes that the reasonableness standard, as applied to judicial reviews of administrative action, applies to my review.

27. The Supreme Court of Canada's decision in *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 [*Vavilov*], at paragraph 99, 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.

28. Relevant factual and legal constraints may 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*.

29. A review of the *IC Act* and the *CSE Act*, as well as legislative debates surrounding the creation of the Intelligence Commissioner, show that Parliament created the role of the Intelligence Commissioner as an independent mechanism by which to ensure that governmental action taken for the purpose of national security was properly balanced with the respect of 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 and as an overseer of ministerial authorizations.

30. This means that a quasi-judicial review by the Intelligence Commissioner must take into consideration the objectives of the statutory scheme as well as the roles of the Minister and the Intelligence Commissioner. I am to carefully consider and weigh the important privacy and other interests of Canadians and persons in Canada that may be reflected by the authorization under review.

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

32. In the context of a cybersecurity authorization issued pursuant to section 27(1) of the *CSE Act* – which is the matter before me – the Intelligence Commissioner's jurisprudence has established that the Intelligence Commissioner can "partially" approve an authorization.[1]

33. The Intelligence Commissioner's decision may be reviewable by the Federal Court of Canada on an application for judicial review, pursuant to section 18.1 of the *Federal Courts Act*, RSC, 1985, c F-7.

IV. ANALYSIS

34. On April 28, 2023, the Chief submitted a written Application for a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures (Application) in furtherance of its mandate. The Application describes the activities that can be used by CSE to access and acquire any information from the federal institutions infrastructure, originating from, directed to, stored on or being transmitted on or through that infrastructure to protect it from mischief, unauthorized use or disruption.

[1] *Intelligence Commissioner – Decision and Reasons,* June 27, 2022, File: 2200-B-2022-01, pages 10–11.

35. The Application also explains the benefits of deploying cybersecurity solutions on federal systems and putting in place multiple layers of defences that are informed by threat information and analysis of anomalous activity. In addition, the Application indicates how the information obtained under this ministerial authorization not only protects federal systems, but also non-federal systems of importance to the Government of Canada (e.g., energy, finance and telecommunications). Further, 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.

36. Based on the facts presented in the Application, and generally in the record, the Minister concluded, in accordance with subsection 33(2) of the *CSE Act*, 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.

37. As a result, the Minister authorized CSE to carry out the following activities set out at paragraph 36 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 a 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.

38. I must now review whether the Minister's conclusions – made in relation to the conditions found in subsections 34(1) and (3) of the *CSE Act* and 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*

i. The meaning of reasonable and proportionate

39. Pursuant to subsection 34(1) of the *CSE Act*, for the Minister to issue a cybersecurity authorization, she must conclude that "there are reasonable grounds to believe that any activity 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."

40. Determining whether an activity is "reasonable" under subsection 34(1) is part of the Minister's obligation and is distinct from the "reasonableness" review conducted by the Intelligence Commissioner. The Minister concludes that any activity that would be authorized by the Authorization is reasonable by applying her understanding of what the term means. The Intelligence Commissioner determines whether the Minister's conclusions are reasonable by conducting a quasi-judicial review and applying the reasonableness standard of review, explained previously.

41. Determining whether an activity is reasonable and proportionate under subsection 34(1) is also a contextual exercise. The Minister may be of the view that the context calls for a number of factors to be considered. Nevertheless, for the Minister's conclusions to be reasonable, I am of the view that her understanding of the meaning of these terms must at least reflect the following underlying considerations.

42. The Intelligence Commissioner's jurisprudence has stated that the notion of "reasonable" pursuant to subsection 34(1) of the *CSE Act* includes an activity that is fair, sound, logical, well-founded and well-grounded having regard to the objectives to be achieved. I add that the notion entails that the activity must be legal in the sense that it must be permissible under the statute. The Intelligence Commissioner's role is limited to reviewing the reasonableness of the ministerial conclusions concerning the requirements laid out at subsections 34(1) and (3) of the *CSE Act*. If a cybersecurity authorization included activities that the statute does not allow the Minister to include, I am of the view that such a conclusion would be reviewable under the "reasonable" criterion.

43. In essence, a reasonable activity is one that is authorized by the *CSE Act* and that has a rational connection with its objectives. The objectives of the activity must align with the legislative objectives. In the context of this Authorization, this means that the objectives of the activities that would be authorized must contribute to the furtherance CSE's cybersecurity and information assurance mandate.

44. As for the notion of "proportionate", it entails a balancing of the interests at play. A useful comparison is the balancing conducted in a reasonableness review where *Charter* rights are at issue. In that context, a decision maker must balance *Charter* rights with the statutory objectives by asking how those rights will be best protected in light of those objectives (see for example *Doré v Barreau du Québec*, 2012 SCC 12 at paragraphs 55-58). It is not sufficient to simply balance the protections with the statutory objectives. A reviewing court must consider whether there were other reasonable possibilities that would give effect to *Charter* protections more fully in light of the objectives (*Law Society of British Columbia v Trinity Western University*, 2018 SCC 32 at paragraphs 80-82).

45. Adopted to our context, it requires that the Minister perform the balancing exercise and finds that the activities that would be permissible under the Authorization be minimally impairing on the privacy interests of Canadians and persons in Canada. It is also important that the intrusive nature of the activity does not outweigh the activity's objectives. If necessary to achieve these purposes, measures should be in place to restrict the acquisition, retention and use of that information.

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

46. The Minister concluded, at paragraph 10 of the Authorization, that she had "reasonable grounds to believe that the activities authorized in this Authorization are reasonable given the objective to help protect federal systems from mischief, unauthorized use, or disruption."

47. I find that the Minister's conclusion is reasonable. There is a clear rational connection between those activities and their objective – to help protect federal systems. It is evident in the record that these specific cybersecurity activities contribute to CSE's cybersecurity and information insurance mandate. I also find that the Minister understood and explains how those activities are necessary to help protect federal systems.

48. I nevertheless think it is useful to add some comments with respect to one of the activities for which authorization is sought, namely to "conduct mitigation actions, as described in the Application, to counter cyber threats" (paragraph 36(d) of the Authorization). The Application describes a number of mitigation actions – [types of mitigation actions] [redacted]

49. CSE clearly has the authority to conduct mitigation actions (paragraph 23(3)(a) of the *CSE Act*). Indeed, the cybersecurity and information assurance aspect of its mandate specifically includes providing "services to help protect" federal systems, and there could be no cybersecurity without mitigations actions (paragraph 17(a)(i) of the *CSE Act*) . The question is whether mitigation actions should be included in a cybersecurity authorization under subsection 27(1) of the *CSE Act*, which sets out the following:

> The Minister may issue a Cybersecurity Authorization to the Establishment that authorizes it, despite any other Act of Parliament, to, in the furtherance of the cybersecurity and information assurance aspect of its mandate, access a federal institution's information infrastructure and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(e) of the *Criminal Code*, from mischief, unauthorized use or disruption. (emphasis added)

50. My role when it comes to the interpretation of the *CSE Act* is to determine whether the Minister's interpretation is reasonable (*Vavilov*, at paragraph 123). Based on the inclusion in the Authorization of mitigation actions activities, I infer that the Minister interpreted subsection 27(1) as not being restricted to the activities of "accessing" systems and "acquiring"

information, but of also including conducting mitigation actions. Although I recognize that one possible reasonable interpretation of the provision may be that the only activities that could be, or would need to be, authorized pursuant to a cybersecurity authorization are those related to "accessing" networks and "acquiring" information, reading the provision in its entirety, in the context of the cybersecurity mandate as set out in the *CSE Act*, I am satisfied that the Minister's interpretation is reasonable. Indeed, it is justified to understand that when read collectively and taking into account the purpose of seeking a ministerial authorization, the terms "access", "acquire" and "for the purpose of helping to protect" include mitigation actions.

51. To the extent that mitigation actions may contravene an Act of Parliament or infringe privacy interests of Canadians or persons in Canada, the Minister's interpretation may actually be the only reasonable interpretation. Ministerial authorizations, and reviews by the Intelligence Commissioner, are mechanisms by which to ensure that there is proper justification and accountability for any breach of a law or of privacy interests. Subsection 22(4) explicitly sets out this principle. As a gatekeeper, my role in the cybersecurity authorization regime is to ensure a proper balance between the need to protect federal systems and safeguard important interests. This means that when CSE wishes to conduct a cybersecurity activity that could impact the rule of law or privacy interests, the authorization by the Minister and review by the Intelligence Commissioner is necessary. Although I note that the Chief explains in her Application that CSE believes it is "unlikely" mitigation activities would constitute an offence, she acknowledges that there is a risk these actions may be found to contravene the *Criminal Code*. As a result, it seems those activities should indeed be authorized by the Minister and approved by the Intelligence Commissioner.

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

52. The Minister concluded at paragraph 13 of the Authorization that she had reasonable grounds to believe the activities authorized are "proportionate given the manner in which they are conducted."

53. I am satisfied that the Minister's conclusion in this respect is reasonable. The record clearly reveals that the Minister conducted a balancing exercise when she considered how the acquisition of information from federal systems and privacy protection are reflected in CSE cybersecurity policies and practices.

54. The Acts of Parliament that have the potential to be contravened, and specifically the provisions at issue of the Acts, are limited in number and in impact on the Canadian public. I also note that, especially since CSE will have the consent of the federal institutions to access their systems, the possible contraventions of Canadian laws are remote. Further, CSE proposes to carry out its activities in a way that will limit the potential offences. As such, I am satisfied that in the event an Act of Parliament is breached, the impact of the breach will be limited.

55. As indicated earlier, the information acquired by CSE does not pertain to any particular person. Should a private communication involving a Canadian be exceptionally intercepted, CSE explains it will only be retained pursuant to the limited conditions as allowed by the *CSE Act*. Also, 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.

56. The Minister was also clearly aware of the privacy interests at issue and laid out the measures in place to protect them. Consequently, she came to the conclusion that the proposed activities do not outweigh any potential impairment of Canadian privacy interests.

B. *Subsection 34(3) – Conditions for authorization – Cybersecurity*

57. Subsection 34(3) of the *CSE Act* provides that the Minister may issue an authorization for cybersecurity only if she concludes that there are reasonable grounds to believe that the four listed conditions 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 infrastructure; and

d) the measures referred to in section 24 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 infrastructure.

i. Information acquired will be retained for no longer than necessary

58. The Authorization describes how information assessed for the purpose of protecting federal systems is retained pursuant to CSE policies and in accordance with the *Library and Archives of Canada Act*, SC 2004, c 11 and the *Privacy Act*, RSC, 1985, c P-21. A retention schedule for the different categories of information that may be collected is included and the Minister concluded that the information will not be retained for longer than is necessary.

59. I understand that CSE's objective is to assess collected information without significant delay and to retain useful information only as long as it continues to be useful.

60. Once information is acquired, the Minister explains that a [redacted] retention period is necessary to provide CSE time to analyse the information in the case of a cyber event and examine its evolution over time. It also allows CSE to compare newly discovered vulnerabilities against its unassessed information and determine whether they exist within the Government of Canada federal networks.

61. Within the [redacted] period CSE assesses whether the information is necessary or essential. The "necessary" criterion applies to information that does not relate to a Canadian or person in Canada. As defined in the Authorization, this type of 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, [redacted]

[redacted] for the purpose of helping to protect federal systems. The "essential" criteria, for its part, applies to information that relates to a Canadian or a person in Canada. Information is considered essential when without it, CSE would be unable to identify, isolate, prevent, or mitigate harm to federal systems. Past authorizations have shown that information meeting the "essential" criteria has been extremely rare. Unassessed information and information not found to be necessary or essential is automatically deleted on or before the [redacted] anniversary of the date it was acquired.

62. 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." I understand this criterion as meaning that the information could be useful indefinitely, but will otherwise no longer be kept when it ceases to be useful for those purposes.

63. Given the important restrictions on accessing unassessed information, I find the Minister's conclusion regarding the [redacted] assessment period reasonable.

64. 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. Indeed, foreign threat actors and particularly state-sponsors treat actors often use the same tradecraft and indicators of compromise as long as it remains effective. Retaining information the length of time needed to respond to that threat is justified. I nevertheless note that this rests on the premise that the "until the information is no longer useful" criterion necessarily entails that periodic reviews of the information are conducted. It is unclear from the record whether CSE has procedures in place to monitor and review the usefulness or essentiality of retained information.

65. I raise an issue related to this in my remarks.

ii. The consent of all persons could not reasonably be obtained

66. As explained in the Authorization, prior to deploying its HBS, NBS and CBS cybersecurity solutions, CSE obtains the consent in writing of the federal institutions system owners. For its part, federal institutions must, in accordance with standard government practice, advise its users that their device and network activity are being monitored for cybersecurity and information assurance purposes. There are instances where it is impossible to obtain the consent of individuals prior to interacting with those federal information infrastructures. This would be the case of an external user who is in contact with a federal employee.

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

iii. Any information acquired is necessary to identify, isolate, prevent or mitigate harm to the federal system

68. The Minister's conclusions explain how threat actors disguise their malicious activities and behaviours to reduce the likelihood of detection. This is done through applications, emails, chat messages and processes which appear legitimate to the user/target but contain malicious codes or links leading to the exfiltration of sensitive information including the installation of malware on the targeted computer. Through the HBS, NBS and CBS solutions, [describing how the information is necessary] [redacted]

69. I find that the Minister's conclusion is reasonable. The examples provided show how any information acquired under the Authorization is necessary to identify, isolate, prevent or mitigate harm to federal institutions' electronic information or information infrastructure. Indeed, CSE needs to acquire specific information about federal systems it needs to protect.

iv. The measures in place ensure that information acquired on Canadians or persons in Canada will be used, analysed or retained only if it is essential to isolate, prevent or mitigate harm to federal systems

70. The Minister's conclusions describe the measures in place to protect the privacy interests of Canadians and persons in Canada. She specifies that access to the information acquired under the authorization is limited to those who are properly accredited to conduct cybersecurity activities and have received the training on information handling procedures, and that most of the analysis of the information is done through automated processes, limiting the employees' access to unassessed information.

71. The Minister also specifies that information relating to a Canadian or a person in Canada can only be retained if it is assessed to be essential. As previously outlined, information is defined as essential when CSE would otherwise be unable to identify, isolate, or prevent harm to federal systems. The record also states that the information is essential "where it provides insight [redacted] for the purpose of helping to protect federal systems". I am of the view that CSE's understanding of the term "essential" is not outside of acceptable interpretations.

72. The Mission Policy Suite for Cybersecurity – the collection of policies that apply to cybersecurity activities – included in the record indicates that it is an analyst who conducts the "essentiality test" of the information acquired (MPS 8.2.2). This is done either through manual or automated processes, prior to the retention of the information. Also, essentiality rationales must be recorded.

73. In addition to describing when information that may identify a Canadian is retained, the record provides information concerning how it can be disclosed, which mirrors the statutory obligation found at section 44 of the *CSE Act*. I note that the End of Authorization Reports that I receive pursuant to section 52 of the *CSE Act* show that it is extremely rare for such information to be retained, and it is my understanding this information has never been disclosed outside of CSE.

74. Given the above, I am of the view that the record reveals that CSE policies and practices take seriously the retention, analysis and use of information relating to a Canadian or a person in Canada. I am satisfied that the Minister's conclusions are reasonable that such scarce information will only be used, analysed or retained if essential to identify, isolate, prevent or mitigate harm to federal institutions' electronic information or information infrastructures.

V. REMARKS

75. I would like to recognize CSE's effort to integrate some remarks I made in my prior decisions. Specifically, the added explanation of CSE's retention timelines have been helpful in my review of the file. Furthermore, I appreciate CSE's commitment to notify me in the event of a contravention of an Act of Parliament that is not listed in the ministerial authorization as well as when solicitor-client communications have been used, analysed, retained, and/or disclosed. I also appreciate the additional details on who within CSE has access to any collected privileged communications.

76. With a view to complete the record of this decision, I would appreciate being informed, as is the Minister, when CSE deploys CBS mitigation capabilities during the period of validity of this Authorization and when CSE provides cybersecurity services to newly consenting federal institutions.

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

i. Former IC Decision – [redacted]

78. In the 2022-2023 application, CSE had requested ministerial authorization to [description of activity] [redacted] In his decision of June 27, 2022, the former Intelligence Commissioner (former IC) did not approve

this activity. He determined that there was a lack of information in the Minister's conclusions and in the record establishing how the authorized activity is covered by subsection 27(1) of the *CSE Act*.

79. Specifically, the former IC stated the following:

> The language of subsection 27(1) does not, *prima facie* (at first view), contemplate or permit the issuance of an authorization outside the scope of accessing a federal institution's information infrastructure, and acquiring any information originating from, directed to, stored on or being transmitted on or through that infrastructure. However, this subsection is suggested by the Chief of CSE in the application, and agreed to by the Minister, as the legislative authority for the authorized activity to [redacted]
>
> … the notion of [redacted] covers a much wider ambit than the notion of federal institution's information infrastructures found in the above provision.

80. In her Briefing Note to the Minister dated April 28, 2023, the Chief describes the former IC's decision as reflecting a legislative drafting oversight. Although [redacted] of the *CSE Act* directs CSE to seek a ministerial authorization in order to [redacted] subsection 27(1) of the *CSE Act* does not account for the activity. The Chief writes that the materials submitted to the former Intelligence Commissioner "did not sufficiently explain this incongruity to satisfy [him] that the activity could be authorized."

81. The Chief further explains that the inclusion of the activity in last year's application was done out of an abundance of caution. It was meant to cover any instances that could potentially trigger the need for a ministerial authorization. This would be an instance where [description of activity] [redacted]

82. Finally the Chief states that following the former IC's decision, "CSE's compliance program has since completed an analysis of [redacted] and, in consultation

with CSE's Department of Justice counsel, concluded that [redacted] As such, the activity was removed from the current Authorization before me.

83. I have two serious concerns regarding the explanation given by CSE regarding this important issue raised by the former IC. First, when making an application to obtain the Minister's authorization in relation to a proposed activity, CSE has the responsibility to convince the Minister that there are reasonable grounds to believe, among other conditions, that such activity must first be necessary, and secondly, reasonable and proportionate. This may include obtaining proper compliance analyses and legal advice, which subsequently may need to be included in the materials submitted to the Minister and myself if necessary to understand the issues at hand.

84. In this instance, it would appear from the Chief's explanations that a compliance analysis and consultation with legal counsel was done after the former IC did not approve that CSE [description of activity] [redacted]

85. Second, based on the record before me, I am left uncertain and perplexed as to why the activity in question, which I understand is currently being carried out, no longer requires ministerial authorization. Indeed, when a decision maker denies an application to conduct an activity and is thereafter informed the activity is nevertheless being conducted, I would expect an explanation to be reflected in the record, beyond a simple statement that CSE obtained a legal opinion, particularly in an *ex parte* context. I would have expected the same if the former Intelligence Commissioner had authorized the activity and over the course of the year CSE had amended its position and concluded the activity no longer needed ministerial authorization.

86. Further, and perhaps even more fundamental, understanding the rationale for amendments from past applications allows the Minister, and as a result the Intelligence Commissioner, to better comprehend the activities that are being authorized.

ii. Effect of mitigation actions on Canadian laws and privacy interests

87. The record describes a number of mitigation actions CSE may conduct pursuant to the Authorization. As indicated, the Chief opined that there was a risk that such actions could contravene an Act of Parliament. Future applications would benefit from a record that includes more information on how proposed mitigation actions may contravene Canadian laws or affect privacy interests of Canadians or persons in Canada, if at all.

iii. Retention period of necessary and essential information

88. The Mission Policy Suite for Cybersecurity does not set out the specific retention period for necessary and essential information, but rather states that it is retained "according to corporate retention schedules." It would be useful for the specific retention periods to be set out in the evergreen document or for the relevant corporate schedules to be included in a future application.

89. On a different note, the terms "essential" and "necessary" are used in the *CSE Act* in relation to different types of information. From my reading of the record, they are effectively given the same interpretation by CSE. Although minor, it may be an element to consider in the upcoming legislative review of the *National Security Act, 2017*.

iv. The retention criterion of "until the information is no longer useful for these purposes"

90. As indicated in my decision, the record is silent as to the procedures in place to review the use of information and delete any information that is "no longer useful". There is also no mention on how often periodic reviews occur.

91. Additional information relating to procedures in place and how often information is reviewed to determine that it remains operationally useful to protect federal systems would be helpful for me to be fully satisfied that CSE is retaining information that has a recognized privacy interest in accordance with the stated criteria.

v. References to the Mission Policy Suite for Cybersecurity

92. On a number of occasions, the record refers to the Mission Policy Suite for Cybersecurity, a document of more than 100 pages, with no references to the specific policy provisions. In judicial and quasi-judicial proceedings, it is common practice that such references be provided in order for the decision maker to have a proper understanding of the record. In the future, I would appreciate if such references were included.

VI. CONCLUSIONS

93. Based on my review of the record submitted, I am satisfied that the Minister's conclusions made under subsection 34(1) and (3) of the *CSE Act* in relation to activities enumerated at paragraph 36 of the Authorization are reasonable.

94. I therefore approve the Minister's Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures dated May 17, 2023, 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.

June 13, 2023

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner