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

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

File: 2200-B-2023-06

INTELLIGENCE COMMISSIONER

DECISION AND REASONS

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

November 30, 2023

TABLE OF CONTENTS.

I. OVERVIEW

1. This is a decision reviewing the conclusions of the Minister of National Defence (Minister) authorizing the Communications Security Establishment (CSE) to carry out cybersecurity activities to help protect electronic information and infrastructures (e.g., computer systems, devices and networks) belonging to [redacted]

2. CSE is Canada's national cryptologic agency and maintains the Government of Canada's cyber defences. CSE is mandated to provide the Government with information technology security in the face of cyber threats. CSE's mandate extends to helping protect the electronic information and infrastructure of entities that are not part of the Government of Canada where the non-federal infrastructures have been designated as being of importance to the Government.

3. To effectively conduct cybersecurity activities, CSE may have to contravene certain Canadian laws. Similarly, when acquiring cybersecurity information related to malicious activities, CSE may incidentally acquire information that interferes with the reasonable expectation of privacy of a Canadian or a person in Canada.

4. In situations where CSE wishes to conduct cybersecurity activities that fall outside the boundaries of the law and infringe on Canadian privacy interests, it must first obtain the required authorizations. Parliament created a regime with checks and balances to ensure that the need to protect electronic information and infrastructures of importance does not outweigh the respect of Canadian privacy interests and the rule of law.

5. The regime originates with a written application by the Chief of CSE (Chief) to the Minister for a cybersecurity authorization that sets out the activities CSE would be authorized to carry out. The Minister may issue the cybersecurity authorization if, among other conditions, the Minister concludes that the proposed activities are reasonable and proportionate. A cybersecurity authorization only becomes valid when it is subsequently approved by the Intelligence Commissioner.

6. On [redacted] pursuant to subsection 27(2) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*), the Minister issued a Cybersecurity Authorization for Activities on Non-Federal Infrastructures (Authorization) for [redacted] the Authorization is a [redacted]

7. On [redacted] 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*).

8. 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 70 of the Authorization are reasonable.

9. Consequently, pursuant to paragraph 20(1)(a) of the *IC Act*, I approve the ministerial Authorization for Cybersecurity Activities on Non-Federal Infrastructures.

II. LEGISLATIVE CONTEXT

A. *Communications Security Establishment Act*

10. 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.

11. CSE's mandate includes cybersecurity and information assurance. Pursuant to section 17 of the *CSE Act*, CSE may provide advice, guidance and services to help protect electronic information and infrastructures belonging to federal institutions as well as to entities that are not a part of the federal government, but have been designated by the Minister as being

of importance to the Government of Canada pursuant to section 21(1) of the *CSE Act* (non-federal systems), for example in the health, energy and telecommunications sectors.

12. Non-federal entities can rely on a number of services to protect their systems from a range of sophisticated cyber threat actors, such as commercially available measures (e.g., anti-virus, firewall software) and third party IT security companies. Nevertheless, Parliament is of the mind that CSE's expertise could be necessary to protect entities operating in sectors of importance to the Government of Canada. In recent years, this expertise has become significantly important in responding to sophisticated cyber threats from state-sponsored groups and non-state actors.

13. To understand vulnerable entry points and compromises of non-federal systems, it is necessary for CSE to access the systems and acquire information. These activities, conducted with the aim of protecting the systems, might nevertheless contravene certain laws as well as breach the reasonable expectation of privacy of Canadians and persons in Canada. The *CSE Act* requires a ministerial authorization, subsequently approved by the Intelligence Commissioner, whenever CSE's cybersecurity activities will contravene an Act of Parliament or will lead to acquiring information that interferes with the reasonable expectation of privacy of a Canadian or a person in Canada (ss 22(4), 27(2), *CSE Act*). The *CSE Act* sets out the process for CSE to obtain a cybersecurity authorization.

14. The owner or operator of the non-federal system must initiate the process by asking CSE, in a written request, to carry out cybersecurity activities to protect the system and its electronic information (s 33(3), *CSE Act*). The Chief must then present a written application to the Minister setting out the facts that would allow him to conclude that there are reasonable grounds to believe that the Authorization is necessary (s 33(2), *CSE Act*). Subsections 34(1) and (3) of the *CSE Act* set out the statutory conditions under which the Minister may issue a cybersecurity authorization. The ministerial authorization is valid once approved by the Intelligence Commissioner (s 28(1), *CSE Act*). Only then can CSE carry out the authorized activities specified in the authorization.

15. As specified in subsection 27(2) of the *CSE Act*, pursuant to a cybersecurity authorization, the Minister may authorize CSE to acquire any information originating from, directed to, stored on or being transmitted on or through the non-federal system for the purpose of helping to protect it, in circumstances described in paragraph 184(2)(e) of the *Criminal Code*, RSC 1985, c C-46, from mischief, unauthorized use or disruption. Paragraph 184(2)(e) generally applies to persons who manage the quality of service of a computer system or its protection.

16. Despite any cybersecurity authorization, the *CSE Act* imposes limitations on CSE activities. CSE must not direct any of its activities at a Canadian or any person in Canada or infringe the *Canadian Charter of Rights and Freedoms* (*Charter*) (s 22(1), *CSE Act*). However, in conducting activities pursuant to an authorization, it is lawful for CSE to incidentally acquire information relating to a Canadian or a person in Canada. Incidentally means that the information acquired was not itself deliberately sought (s 23(5), *CSE Act*).

17. In the context of a cybersecurity authorization, CSE explains that information relating to a Canadian or a person in Canada that may be acquired includes but is not limited to personal information as defined in section 3 of the *Privacy Act*, solicitor-client communication, business information (e.g., intellectual property, trade secrets), domain name, email address and IP address. It may also include private communications that originate or terminate in Canada, and where the originator has a reasonable expectation of privacy. I note that while it is a criminal offence to intercept private communications, section 50 of the *CSE Act* provides an exemption and stipulates that Part VI of the *Criminal Code* (Invasion of Privacy) does not apply when a communication is intercepted under the authority of an authorization issued by the Minister.

18. When acquired, strict legislative and policy measures must be followed to use, analyse and retain this information. Indeed, CSE is required to have measures in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of information related to them (s 24, *CSE Act*).

B. *Intelligence Commissioner Act*

19. 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 are issued to determine whether they are reasonable.

20. Section 14 of the *IC Act* specifies that for a cybersecurity authorization, the Intelligence Commissioner reviews the Minister's conclusions made under subsections 34(1) and (3) of the *CSE Act*.

21. The Minister is required to provide to the Intelligence Commissioner all information that was before him as the decision maker (s 23, *IC Act*). 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 (s 26, *IC Act*).

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

    a) The letter to the Intelligence Commissioner from the Minister dated [redacted];
    b) The Ministerial Authorization dated [redacted];
    c) The Briefing Note from the Chief to the Minister dated [redacted];
    d) The Chief's Application dated [redacted], which includes twelve annexes including but not limited to:
        i. The letters of request from [redacted]
        ii. The Mission Policy Suite for Cybersecurity approved February 28, 2022;
        iii. Two ministerial orders; and
    e) The Summary Deck – Overview of the Activities.

III. STANDARD OF REVIEW

23. The *IC Act* requires the Intelligence Commissioner to review whether the Minister's conclusions are reasonable. The Intelligence Commissioner's jurisprudence establishes that the reasonableness standard that applies to judicial review of administrative action is the same standard that applies to reviews conducted by the Intelligence Commissioner.

24. In conducting a reasonableness review, a reviewing court is to start its analysis with the reasons of the administrative decision maker (*Mason v Canada (Citizenship and Immigration)*, 2023 SCC 21, para 79 [*Mason*]). 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.

25. 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*.

26. A review of the *IC Act* and the *CSE Act*, as well as legislative debates, shows that Parliament created the role of the Intelligence Commissioner as an independent mechanism 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 of the intelligence and national security activities related to the authorization regime.

27. When the Intelligence Commissioner is satisfied (*convaincu* in French) 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

28. On [redacted], the Chief submitted to the Minister a written Application for a Cybersecurity Authorization (Application) for the systems belonging to [redacted] in furtherance of its mandate. [redacted] Although not an issue in this matter, it may be that including [redacted] enlarges its scope which could add complexity to the Minister's conclusions and the Intelligence Commissioner's review.

29. [redacted] requested CSE's assistance in writing. The Application sought ministerial authorization for [redacted] the Application constitutes a [redacted]

30. The [redacted] considered to be of importance to the Government of Canada, as defined in the *Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada* issued on August 25, 2020. A description of the [redacted] as well as the activities set out in the Authorization can be found in the annex to this decision (Annex A), which is not intended for public release at this time to ensure that the activities can be carried out successfully. Including this information in the annex renders the eventual public version of this decision easier to read and ensures that the decision contains the nature of the facts that were before me, which otherwise would only be available in the record.

31. Briefly, the proposed activities consist of deploying [description of activity] [redacted] on the [redacted] systems. [redacted] acquired through the systems. [redacted]

32. The Authorization authorizes that cybersecurity activities be carried out on the systems of [redacted] Annex X, XI and XII of the record lists agencies that use [redacted] systems and would therefore be eligible to receive CSE's cybersecurity services pursuant to the Authorization. CSE has adopted the protocol used in the federal cybersecurity ministerial authorization to notify the Minister and the Intelligence Commissioner when CSE onboards new agencies. I see no legal impediment at this time for CSE to proceed in this manner, as long as the agencies use the systems described in the Authorization. I understand that the agencies are not onboarded without their involvement.

33. Based on these facts, the Minister concluded that the statutory conditions set out in subsections 34(1) and (3) of the *CSE Act* were met and issued the Authorization. I must now review whether the Minister's conclusions are reasonable.

A. Subsection 34(1) of the *CSE Act*

i. Determining whether the activities are reasonable and proportionate

34. To issue a cybersecurity authorization, the Minister 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" (s 34(1), *CSE Act*).

35. Determining whether an activity is "reasonable" is distinct from the "reasonableness" review conducted by the Intelligence Commissioner. 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. Nevertheless, I am of the view that the understanding of both thresholds must minimally reflect certain fundamental elements. A reasonable activity must be authorized by a reasonable interpretation of the legislation and have a rational connection with its objectives. As for the notion of "proportionate", it entails conducting a balancing of the interests at play, which in the context of a cybersecurity authorization will include the protection of systems and the impact on Canadian privacy interests.

36. The Intelligence Commissioner must determine whether the Minister's conclusions, which include his understanding of the thresholds, are "reasonable" by conducting a quasi-judicial review and applying the reasonableness standard of review, explained previously.

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

37. The Minister concluded at paragraph 34 of the Authorization that he had reasonable grounds to believe that the activities authorized in the Authorization are reasonable given the objective of helping to protect federal systems and systems of importance from mischief, unauthorized use, or disruption.

38. In issuing the Authorization, 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*). The CSE Mission Policy Suite Cybersecurity, approved on February 28, 2022 (MPS) – the collection of policy principles and requirements to guide CSE personnel working under the cybersecurity aspect of CSE's mandate – states at section 5.2.1 that cybersecurity activities are not considered to be directed at individuals provided they focus on the cyber threat posed to the system. This position logically entails that any

information related to Canadians or persons in Canada acquired through these activities is not deliberatively sought, but rather incidentally acquired.

39. To be clear, CSE will necessarily acquire information related to Canadians or persons in Canada when conducting the cybersecurity activities set out in the Authorization. The systems of [redacted] are located in Canada and the information stored on the systems, 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 [redacted], but also includes information from members of the Canadian public who, for example, communicate with [redacted] by email.

40. I find CSE's position that the activities are not directed at Canadians, and consequently the Minister's conclusion, reasonable. Indeed, the Minister's conclusion aligns with subsection 23(3) of the *CSE Act* that specifically states that despite the prohibition on directing activities to Canadians or persons in Canada, CSE may carry out activities on systems in order identify or isolate malicious software, prevent malicious software from harming the systems, and mitigating any harm. The Minister's conclusion is also coherent with the cybersecurity and information assurance aspect of CSE's mandate that can only be fulfilled by accessing systems in Canada. I am satisfied that the record supports the Minister's conclusion that the activities carried out by CSE focus on acquiring information about cyber threats and are not directed at Canadians, and therefore respect the legislative prohibition.

41. The Minister justifies that the activities are reasonable for two main reasons: CSE's involvement in the cybersecurity response is required given the key role played by [redacted]; and the activities for which the authorization is sought are effective.

42. With regard to the first reason, [redacted] deliver, [redacted] The Minister also explains that [redacted] play a central role in [redacted]

[redacted]

43. The record explains that [description of threats] [redacted] CSE assesses that [redacted] CSE also assesses that [redacted] the system of [redacted], which led to the current cybersecurity authorization to help protect its system.

44. Based on information provided by the Chief, the Minister reports that even with the help currently provided by CSE to [redacted] Indeed, CSE has observed [redacted] According to the Minister, [redacted] of cybersecurity solutions on the system of [redacted] is reasonable given the [redacted]

45. With regard to [redacted] CSE observed [redacted] CSE was informed [redacted]

[redacted] CSE assesses that [redacted].

46. As a result, the Minister concludes that the current state of [redacted] cybersecurity posture is not sufficient to identify and combat [nature of the threat] [redacted] The Minister also supports his conclusion by relying on the [redacted] of [redacted] and the [redacted] where [redacted] are located. I note that the record does not provide information about the anticipated duration of CSE's presence on [redacted] systems beyond the one-year validity period sought for the Authorization.

47. The Minister's second ground supporting the conclusion that the activities are reasonable is that they would be effective. Cyber threats can be difficult to detect and compromises can have a devastating and rapid result. The objective of the activities is to help [redacted] identify [redacted] indicators of compromise, remove the presence of any identified threat actor, and strengthen cybersecurity posture to protect against future threats. The activities would allow CSE to identify and better understand malicious cyber activity or other indicators of compromise in order to advise [redacted] on how to protect their systems. The activities would also allow CSE to conduct mitigation actions [redacted]

48. The record includes evidence of the effectiveness of the activities. [redacted] reports of malicious activities. Further, CSE provided [redacted] with recommendations to [redacted] CSE also continues to provide further recommendations based on [redacted] security architecture.

49. The Minister appropriately relies on the Chief's Application to make conclusions with respect to the state of [redacted] systems as well as the effectiveness of the proposed cybersecurity activities (s 33(2), *CSE Act*). Indeed, The Minister is not expected to have CSE's technical expertise. Nevertheless, a reasonable ministerial conclusion must be justified, transparent and intelligible (*Vavilov*, para 99). This means the Minister must exhibit an understanding of the rationale of his conclusions.

50. I am of the view that the Minister's conclusions exhibit that understanding. His conclusions reflect that he considered and was satisfied with the link between the current needs of [redacted] and the proposed cybersecurity activities. There is a clear rational connection between CSE's proposed cybersecurity activities and their objective, which is to help protect non-federal systems. The Minister relies on the critical and strategic role played by [redacted] which I find supports his conclusion. It is also evident in the record that the cybersecurity activities are well-founded and contribute to CSE's cybersecurity and information assurance mandate in relation to the systems of [redacted] Considering the nature of the objective and the information in the record with respect to the nature of the activities, I find reasonable the Minister's conclusion that the activities are reasonable.

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

51. The Minister concluded at paragraph 45 of the Authorization that he had reasonable grounds to believe the authorized activities are proportionate because they are rationally connected to the objective, and minimally impair the rights and freedoms of third parties as well as the ability for [redacted] systems to be accessed and used. According to the Minister, there is minimal impairment on account of the following measures in place to protect any information related to Canadians or persons in Canada that would be incidentally acquired:

    a. only information that is necessary to protect the systems is acquired;

b. information is retained only if it assessed as necessary to identify, isolate, prevent, or mitigate harm to the system and/or to federal systems and other systems of importance;
c. information identified as related to a Canadian or a person in Canada is retained only if it is assessed as essential to identify, isolate, prevent, or mitigate harm to the system and/or to federal systems and other systems of importance;
d. unassessed information is retained for no longer than [redacted];
e. most of the analysis and mitigation is done through automated processes that limit CSE employees' access to the information;
f. access to information acquired under the Authorization is restricted to authorized CSE employees who have received the appropriate training and have a need to know for the purpose of their work;
g. all information is protected in accordance with the MPS;
h. every search performed on the acquired unassessed information is auditable to comply with the MPS and other corporate policies; and
i. the technology used is reviewed for legal and policy compliance.

52. The Minister supported his conclusion on proportionality by relying on the same measures found in Decision 2200-B-2023-05, which also dealt with a cybersecurity authorization for a non-federal entity (*Non-Federal Cybersecurity Decision*). I recognize that the Minister did not yet have the benefit of my comments made in *Non-Federal Cybersecurity Decision* prior to issuing this Authorization. In that decision, I noted that the measures set out from a) to d) essentially mirror the statutory requirements found at subsection 34(3) of the *CSE Act* that must be satisfied in a cybersecurity authorization. These measures do not provide much support to the Minister's conclusion that the activities are proportionate because this is a distinct statutory condition that must be separately satisfied (s 34(1), *CSE Act*). I also noted that certain measures set out by the Minister lacked specific information, namely with respect to details concerning what type of information falls outside of "most of the analysis" that is done through automated processes, and the nature of the information.

53. I also commented that the measure set out at c) that states that Canadian-related information can be retained when essential for the purpose of protecting the [redacted] and/or federal systems and other systems of importance. However, in the case of authorizations issued under subsection 27(2) – cybersecurity authorizations for non-federal systems – paragraph 34(3)(d)(ii) of the *CSE Act* states that the retention of Canadian-related information must be for the purpose of protecting systems designated under subsection 21(1) as being of importance to the Government of Canada (non-federal systems). I pointed out that the initial retention must comply with the legislative requirements. My comments are applicable to this Authorization as well.

54. The measures in place to control information after it is acquired is the central issue in support of the Minister's proportionality conclusion. I agree that it can be reasonable to lean on policy and practices that limit access, use and disclosure of acquired information to conclude that activities are proportionate. These limits can be particularly relevant when cybersecurity activities allow for the acquisition of a large amount of information, including information in which there is a reasonable expectation of privacy. Nevertheless, in the administrative law context, a decision maker must be alert and sensitive to all key issues (*Mason*, para 74). The Minister's reliance on the strict measures to control information that has been acquired raises the question of whether he has sufficiently grappled with other key issues in arriving at his conclusion on proportionality.

55. The ministerial responsibility to identify and to be alert and sensitive to key issues is onerous in the non-adversarial context, which includes when the Minister decides whether to issue an authorization. The Supreme Court of Canada has emphasized the importance of identifying and dealing with key issues, stating that "a decision maker's failure to meaningfully grapple with key issues or central arguments raised by the parties may call into question whether the decision maker was actually alert and sensitive to the matter before it" (*Mason*, para 74). However, under the authorization regime, the Minister does not benefit from the submissions of adversarial parties.

56. The Intelligence Commissioner's quasi-judicial review includes determining whether the Minister has sufficiently considered the key issues. Indeed, jurisprudence from the

Intelligence Commissioner has repeatedly emphasized that for ministerial conclusions to be reasonable, they must demonstrate an understanding of the activities and their effects on the rule of law and Canadian privacy interests (see for example Decision 2200-B-2023-01, para 78; Decision 2200-A-2023-02, para 61). The reasonableness review that I must conduct logically extends to considering whether the Minister has simply failed to identify a key issue. The Intelligence Commissioner's oversight function in a context where no party is opposing the Minister's authorization requires that I do so. Further, courts recognize that judges determining matters in *ex parte* proceedings must play an active role to ensure that the relevant issues are canvassed and considered, especially in the national security context (*Canada (Citizenship and Immigration) v Harkat*, 2014 SCC 37, para 46). Although not a judge, I am of the view that the same principles apply with respect to the Intelligence Commissioner's role.

57. Ensuring that a reasonable ministerial authorization meaningfully considers all of the key issues is also entirely coherent with the legislative scheme. Indeed, issuing an authorization is a ministerial responsibility that cannot be delegated. It is a heavy responsibility because authorized activities could contravene Canadian laws and intrude on the privacy interests of Canadians. Parliament is asking the Minister no less than to personally confirm that CSE is justified in carrying out unlawful activities.

58. This responsibility takes on additional weight given the constitutional dimension associated with CSE activities that breach the reasonable expectation of privacy of Canadians and persons in Canada. A breach of a reasonable expectation of privacy by the state – in this case CSE as a representative of the Government – may amount to a search or seizure. Section 8 of *Charter* protects Canadians and persons in Canada from unreasonable searches and seizures by the state. Effectively, to issue an authorization, Parliament is also asking the Minister to confirm that activities that could amount to a search or seizure are compliant with the *Charter*. The gravity of the consequences of a ministerial authorization must be reflected in the ministerial conclusions, which demands that key considerations not be glossed over or disregarded.

59. Finding a ministerial authorization unreasonable because a key issue has not been sufficiently considered is analytically distinct from conducting a disguised "correctness review" by independently deciding what the key issues should be. Key issues must be rooted in the record, not invented or conjured.

60. Returning to the matter before me, the record shows that to determine that the activities are proportionate, the Minister did not grapple with and rely only on the measures to control information that has been acquired. He considered other key issues. First, the Minister recognizes that the activities would lead to the acquisition of information in which Canadians and persons in Canada have a reasonable expectation of privacy, which is necessary for the cybersecurity activities to be effective. Indeed, in the Application, the Chief states that CSE [will necessarily acquire information in which there is a reasonable expectation of privacy] [redacted] The Minister confirms that CSE [redacted] Second, he also recognizes that the activities provide access to large amounts of information [redacted]

61. Thus, even though the Minister does not analyse any specific context where the acquisition of information would breach a reasonable expectation of privacy, he does acknowledge that particular sensitive types of information [redacted] will be acquired. Similarly, although the Minister's conclusions do not provide details about the volume of information related to a Canadian or a person in Canada that will be acquired, they reflect his understanding that there will be large amounts given that information is acquired from non-federal systems in Canada.

62. Considering the record holistically and contextually, I am of the view that the Minister considered the key issues rooted in the record in conducting a balancing exercise in his

proportionality analysis. Although the back-end measures set out in CSE's policies to control the acquired information weighed heavily in favour of finding the activities proportionate, his conclusions show that he was alive – at least generally – to the issues related to the front-end information acquisition activities, most notably with respect to the volume and nature of the information. In conducting my reasonableness review, the Minister's conclusions must not be assessed against a standard of perfection and need not necessarily include the details that I, as Intelligence Commissioner, would have preferred (*Vavilov*, para 91). While I am of the view that a more thorough consideration of the key issues would have enhanced the Minister's reasoning process, I find that his balancing is justified given the factual context.

63. As for the Acts of Parliament that have the potential to be contravened, the Authorization indicates they are limited in number as the activities would take place only on non-federal systems where CSE has received the express consent of the owner to operate. Since CSE will have the required consent to access the systems, the possible contraventions of Canadian laws are remote. In the event that an Act of Parliament is breached, the impact of the breach will be limited given the use made by CSE of the acquired information. Further, if an Act of Parliament that is not listed in the Chief's application is contravened, the Chief will inform both the Minister and the Intelligence Commissioner.

64. In light of the above, I find that the Minister has sufficiently justified his conclusion and that it is supported by the record. He understood and considered the key issues and conducted a balancing that is justified by the facts in the record. As a result, I am satisfied that the Minister's conclusion in relation to the proportionality of the activities is reasonable.

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

65. Subsection 34(3) of the *CSE Act* provides that the Minister may issue an authorization for cybersecurity only if he concludes that there are reasonable grounds to believe that the three listed conditions are met, namely:

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

b. any information acquired under the authorization is necessary to identify, isolate, prevent or mitigate harm to the non-federal systems; and

c. 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 the non-federal systems.

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

66. Information assessed for the purpose of protecting non-federal systems is retained pursuant to CSE policies. A *Retention and Disposition Table* for the different types of information that may be acquired is included in the record (Annex VIII). I note that the Chief indicates in the Application that [redacted] described in the Authorization can, at any time, request that CSE delete the information it has acquired from or through their systems.

67. As it not possible for CSE to determine what information will be helpful in identifying malicious activity, the activities set out in the Authorization allow for the acquisition of a large volume of information. The Minister explains that CSE processes this information, mostly through automated means. This process may identify some of the information as "necessary" or "essential". All other information is considered to be unassessed information, even though it has gone through the automated processes.

68. The "necessary" criterion applies to information that does not relate to a Canadian or a person in Canada. As defined in the Authorization and the Definition Section of the MPS, information is considered necessary when it is required for the understanding of malicious cyber activities [redacted] for the purpose of helping to protect federal institutions and non-federal systems of importance.

69. For its part, the "essential" criteria defined in the Authorization and the Definition Section of the MPS applies to information that is incidentally acquired that relates to a Canadian or a person in Canada. Information is deemed essential when, without it, CSE would be unable to help protect non-federal systems of importance, federal systems and the electronic information on those systems. Information related to Canadians or persons in Canada that is retained is tracked internally in accordance with the policy requirements outlined throughout the MPS.

70. Pursuant to CSE's *Retention and Disposition Table*, the information that is determined to be necessary or essential may be retained "until no longer useful for these purposes, or unless dictated by client imposed restrictions." I understand the criterion "until no longer useful" as meaning that the information could be useful indefinitely, but will not be kept when it ceases to be useful for those purposes.

71. Regarding the information deemed "essential" – that is related to a Canadian or a person in Canada – operational managers must review the information on a quarterly basis to revalidate that it remains essential. Information that is no longer essential must be deleted. The record does not indicate that CSE conducts periodic reviews of information that has been assessed as "necessary" – not related to a Canadian or a person in Canada.

72. As for the retention period for unassessed information, the Minister explains that some compromises may be identified after a malicious activity first began. Therefore, the effectiveness of CSE's activities depend on being able to cross reference and analyse multiple sources of information already acquired, including identified indicators of compromise. He explains that a [redacted] retention period for unassessed information provides a "reasonable analysis period" to allow CSE time to reach back to the origins of a cyber event and examine its evolution over time. It also allows CSE to compare newly discovered vulnerabilities against this unassessed information and determine whether they exist within federal systems and other systems of importance.

73. After a [redacted] period, unassessed information will be automatically deleted unless deemed "necessary" or "essential" to help protect [redacted] systems, or

federal systems and designated systems of importance. Section 10.2 of the MPS states that access to unassessed information [redacted] must be strictly controlled and limited to those authorized to conduct or support cybersecurity activities. The list of personnel with approved access to unassessed information is tracked for accountability purposes. Unassessed information cannot be shared beyond CSE.

74. Once retained as necessary or essential, the information is used to protect the non-federal systems in this instance as well as federal systems and other systems of importance to the Government of Canada. The Chief states in the Application that [redacted] in this instance is aware and agrees on the use of this information.

75. Given the important CSE policy restrictions on accessing unassessed information and the reality that malicious cyber activity may only be detected after the passage of time, I find the Minister's conclusion regarding the [redacted] retention period reasonable. In a previous decision concerning non-federal infrastructures (Decision 2200-B-2022-05), I suggested that CSE provide operational examples to illustrate that the [redacted] retention period of unassessed information is reasonably necessary. My comment is only reinforced given that CSE was [redacted].

76. I also find that the Minister's conclusion is reasonable that information determined to be necessary or essential to identify, isolate, prevent, or mitigate harm to non-federal systems may be retained until it is no longer useful or unless otherwise dictated by the non-federal entity, as long as there is a periodic review with respect to the usefulness of essential information. The record clearly reflects that [redacted]

ii. Any information acquired is necessary to identify, isolate, prevent or mitigate harm to the non-federal systems

77. This condition underpins the activities for which authorization is sought. The use of the specific cybersecurity solutions set out in the Authorization would result in the acquisition of a large amount of information, regardless if almost all of the information does not reveal the existence of a cyber threat. This raises the question of whether it is necessary for CSE to acquire all of the information when most of it does not contain information about threats and will simply be deleted after the [redacted] retention period.

78. The Minister relies on the Chief's assessment that this acquisition is necessary to identify, isolate, prevent or mitigate harm to [redacted] systems. Although the Minister is not a technical expert, his conclusions provide, in my view, a compelling and easy to understand justification for which acquiring the information is necessary. He explains that it is not possible for CSE to predict [how the systems will be affected] [redacted] Therefore, to effectively mitigate the sophisticated cyber threats described in this matter, CSE must acquire a vast range of unassessed information to identify [redacted].

79. Further, there is nothing in the record to suggest that CSE can achieve the same cybersecurity outcomes by using different cybersecurity solutions that acquire less information, specifically information related to Canadians.

80. I am therefore satisfied that the Minister's conclusions are reasonable that he has reasonable grounds to believe that the acquisition of the information is necessary to identify, isolate, prevent or mitigate harm to the systems

iii. The measures in place ensure that information acquired identified as relating to Canadians or persons in Canada will be used, analysed or retained only if it is essential to identify, isolate, prevent or mitigate harm to the non-federal systems

81. Section 24 of the *CSE Act* requires CSE to have measures in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of

information related to them acquired in the course of its cybersecurity and information assurance aspects of its mandate. At paragraph 61 of the Authorization, the Minister concludes that he has reasonable grounds to believe that the measures referred to in section 24 have been met.

82. The Minister reiterates that information relating to a Canadian or a person in Canada can only be retained if it is assessed to be essential. This condition is set out throughout the MPS. As previously outlined, information is defined as essential when CSE would otherwise be unable to identify, isolate, or prevent harm to [redacted] systems, or to federal systems and other systems of importance.

83. Section 8.2.2 of the MPS indicates that an authorized CSE employee conducts the "essentiality test" of the information acquired. This is done either through manual or automated processes. Essentiality rationales must be recorded by the employee. In my view, this measure contributes to compliance with the legislative obligation under section 24 of the *CSE Act* and supports the Minister's conclusions.

84. The Minister's conclusions specify that access to the unassessed information acquired under the Authorization is limited to authorized CSE employees who are properly accredited to conduct cybersecurity activities and have received the mandatory training on information handling procedures. Further, given that most of the analysis of the information is done through automated processes, the employees' access to the content of the information is therefore limited.

85. The Minister's conclusion and the record also explain how information related to Canadians or persons in Canada can be disclosed, which mirrors the statutory obligation found at section 44 of the *CSE Act*. The information is only disclosed to persons or classes of persons designated under the *Ministerial Order Designating Recipients of Information Relating to a Canadian or Person in Canada Acquired, Used, or Analyzed Under the Cybersecurity and Information Assurance Aspect of the CSE Mandate* issued on June 13, 2023 in accordance with section 45 of the *CSE Act*. [redacted]

[redacted] To receive information disclosed by CSE that relates to a Canadian or person in Canada, the information must be necessary to help protect federal systems or systems of importance.

86. As outlined in section 24 of CSE's MPS, privacy measures are in place to protect the privacy of Canadians and persons in Canada when information related to Canadians is disclosed. For example, personal information may be suppressed so that any reporting does not identify the identity of an individual. The MPS sets out the required disclosure approval levels accompanying different types of information. The approvals must be documented.

87. I note that [in requesting CSE's assistance] [redacted] asked that all personal or proprietary information be obfuscated before it is shared and that information that is not relevant to CSE's mandate must be deleted in accordance with CSE's retention schedule. It is therefore my understanding that any disclosure of information acquired under the Authorization will first have to satisfy this direction.

88. The MPS sets out elaborate policies to control and safeguard information related to Canadians and persons in Canada that is acquired pursuant to a cybersecurity authorization. As a reminder, these policies and CSE practice weighed heavily in the Minister's conclusion that the activities are proportionate. The policies establish processes that require CSE employees to document rationales for retention, use and disclosure of information related to Canadians and persons in Canada. If followed, these measures should, in my view, provide an effective manner for CSE to respect the legislative requirement to sufficiently protect this information.

89. I am therefore satisfied that the Minister's conclusion is reasonable that he has reasonable grounds to believe that information related to Canadians or persons in Canada will only be used, analysed or retained if essential to identify, isolate, prevent or mitigate harm to [redacted] systems.

V. REMARKS

90. In Decision 2200-B-2022-06 that I rendered on December 8, 2022, I remarked that a document included in that record that had been prepared by the Canadian Centre for Cyber Security [redacted] was not dated. I requested that all documents in the record be dated in future applications. In addition, I indicated that any available updated information [redacted] should be provided to assist the Minister in his decision making. Indeed, decisions should be based on the most accurate information possible. Conversely, if no updated information was available, the record should so specify.

91. This remark was not addressed in the matter before me. The same undated document was included, but the record shows that [there is updated information] [redacted]

Further, during a presentation by CSE to myself and my staff under section 25 of the *IC Act*, [updated information was provided] [redacted]

Ensuring that the information is as current as possible is necessary for the Minister to fulfill his responsibility.

92. I also note that I made remarks in *Non-Federal Cybersecurity Decision*, which, as previously stated, the Minister did not have prior to issuing this Authorization. Those remarks are equally applicable here. I expect that they will be reflected in future authorizations. In particular, I underline again the importance of providing references to the specific sections of the MPS relied on by CSE in the Chief's Application to the Minister, as well as providing details on the impact on Canadian privacy rights. To that effect, the record in this Authorization referred to [redacted] reports of malicious activities. In the context where CSE seeks authorization for the [redacted] it is helpful for the Minister to have an understanding of whether detecting the malicious threat activities required retaining Canadian-related information and whether considerations related to privacy appeared in reports. CSE had access to this information

from the reports and did not provide it to the Minister. I see no reason for which it should not be included. Indeed, this information helps the Minister better understand the impact of the authorization he would be issuing and may be a key issue to consider in determining the reasonableness and proportionality of activities.

93. Although I am satisfied that the Minister's conclusions are reasonable, I would like to make a remark to assist in the consideration and drafting of future ministerial authorizations. This remark does not alter my findings regarding the Minister's conclusions.

A. Use of acquired information across CSE's mandate

94. I wish to comment on the use of information by CSE across the various aspects of its mandate. The Authorization states that "[i]nformation acquired by CSE under one aspect of the mandate can then be used within CSE to serve other aspects of its mandate, so long as it is relevant to that aspect and meets any particular requirement of the *CSE Act* that may need to be followed, such as applying measures to protect the privacy of a Canadian or person in Canada." This is CSE's position in all cybersecurity and foreign intelligence ministerial authorizations.

95. A plain reading of this general blanket statement suggests that unassessed information acquired under a cybersecurity authorization that has not been determined to be necessary or essential could, [redacted] be accessed, analyzed, used and retained if it was found to be "relevant" to other aspects of CSE's mandate. Given that the activities set out in the Authorization will allow for the acquisition of a large volume of information with the knowledge that some information will benefit from a reasonable expectation of privacy and the majority of it will not be assessed as necessary or essential, the general statement raises concerns that the Minister's conclusions do not address.

96. First, subsection 34(3)(d) of the *CSE Act* specifically states that information related to a Canadian or a person in Canada acquired pursuant to a cybersecurity authorization can only be used, analyzed or retained if it is essential to isolate, prevent or mitigate harm to the non-federal systems that have been designated as of importance to the Government of

Canada. This seems to suggest that even if information related to a Canadian is acquired pursuant to a cybersecurity authorization, the information should not be used to serve other aspects of its mandate unless it has first been retained as essential to identify, isolate, prevent or mitigate harm for cybersecurity purposes.

97. The second issue is that the use of the information by CSE may be a factor in determining that a cybersecurity authorization is reasonable and proportional. This means that using the information in a way that was not clearly reflected in ministerial conclusions may fall outside of what is allowed under the authorization.

98. For example, incidentally acquiring a large quantity of information, knowing some of it benefits from a reasonable expectation of privacy and a lot of it will not be assessed as useful, may be reasonable and proportional on the basis that it is necessary for effective cybersecurity. However, this conclusion may change if the information is also to be used for other purposes or other aspects of CSE's mandate. Canadians may accept that an email from a grade 12 student to a teacher could be acquired by a non-federal entity responsible for cybersecurity of the school's system because of potential malware. At the same time, Canadians may think the CSE, on behalf of the federal government, is intruding if that legally acquired email containing no malware appears in foreign intelligence reporting. The Minister does not consider the impact of CSE's legal authority to use information across the five aspects of its mandate in his conclusions.

99. However, upon reviewing the record in its entirety, and specifically section 26 of the MPS in relation to access and use of information within CSE, it seems that the general blanket statement made in the Authorization is limited in practice. It is my understanding from the MPS that any access to and use of unassessed information acquired pursuant to a cybersecurity authorization must be "consistent" with the cybersecurity aspect of the mandate.

100. Further, information related to a Canadian or a person in Canada cannot be retained unless it is found to be essential to identify, isolate, prevent or mitigate harm to systems. Therefore, even if unassessed information can be accessed and used for other aspects of

CSE's mandate – as long as it is consistent with cybersecurity – any Canadian-related information identified through this access could not be retained or used unless it met the essentiality requirement.

101. I add that the examples in the record of using information across the different aspects of CSE's mandate suggest that it is done only with respect to information that has already been determined as necessary or essential, suggesting that CSE is not using unassessed information for these other aspects. For example, the Chief states that information acquired under a cybersecurity authorization regarding [redacted] – essential or necessary information – would be relevant to the foreign intelligence aspect of CSE's mandate.

102. The general blanket statement purports that CSE has free rein to use all of the information it acquires for all aspects of its mandate as long as it is relevant to that aspect. However, the policy framework and CSE's practices, at least my review and understanding of them, show that access and use of the unassessed information in this case is limited and must be consistent with cybersecurity purposes. In my view, the general statement requires that additional details explaining these limitations be clearly set out in the record. It is imperative for the Minister and I to understand how CSE is acting within limits imposed by the law. I expect that will be the case in future authorizations.

VI. CONCLUSIONS

103. 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 70 of the Authorization are reasonable.

104. I therefore approve the Minister's Cybersecurity Authorization for Activities to Help Protect Non-Federal Infrastructures dated [redacted], pursuant to paragraph 20(1)(a) of the *IC Act*.

105. 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.

106. 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.

107. If the passage of time allows for it, I am of the view that the public would benefit from knowing that CSE played a major role in supporting and rebuilding [redacted] cybersecurity posture. Disclosure of past activities contributes to allowing the public to tangibly see the importance and value of CSE's role and, as a result, creates an aura of confidence essential to any national security agency.

November 30, 2023

(Original signed)
The Honourable Simon Noël, K.C.
Intelligence Commissioner