~~**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-2023-05

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 3, 2023

TABLE OF CONTENTS.

I. OVERVIEW

1. This is a decision reviewing the Minister of National Defence's (Minister) conclusions authorizing the Communications Security Establishment (CSE) to help protect electronic information and infrastructures (i.e., computer systems, devices and networks) belonging to a non-federal entity.

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 protecting 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. In some situations, CSE's cybersecurity activities may 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 to Help Protect Non-Federal Infrastructures (Authorization).

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 subsection 34(1) and (3) of the *CSE Act* in relation to activities and classes of activities enumerated at paragraph 54 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 to Help Protect 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 networks 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 sectors of importance to the Government of Canada.

13. To understand vulnerable entry points and compromises of non-federal systems, it may be necessary for CSE to access the systems and acquire information. These activities, conducted with the aim of protecting the system, 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 systems must initiate the process by asking CSE, in a written request, to carry out cybersecurity activities to protect the systems and their 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* define 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 systems for the purpose of helping to protect them, 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. Information acquired under the cybersecurity and information assurance aspect of its mandate may be used by CSE to enable activities under other aspects of its mandate, as long as any restriction placed on the information is respected.

17. 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, as it is not possible for CSE to determine what information is needed in advance, CSE may incidentally acquire information relating to a Canadian or a person in Canada. Incidental means that the information acquired was not itself deliberately sought (s 23(5), *CSE Act*).

18. In the context of a cybersecurity authorization, CSE explains that information relating to a Canadian or a person in Canada that may incidentally 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 in relation to an interception of a communication under the authority of authorization issued by the Minister.

19. 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*

20. 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.

21. 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*.

22. 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*).

23. 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 before me is therefore composed of:

    a) The letter to the Intelligence Commissioner from the Minister (not dated);
    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 seven annexes including but not limited to:
        i. The letter of request from the non-federal entity dated [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

24. 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.

25. 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). 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.

26. 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*.

27. 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.

28. 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*).

29. 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

30. On [redacted] the Chief submitted to the Minister a written Application for a Cybersecurity Authorization for Activities to Help Protect Non-Federal Infrastructures (Application) in furtherance of its mandate. [redacted]

31. The non-federal entity in question is 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 non-federal entity 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. Including this information in this 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.

32. In sum, the proposed activities consist of deploying [redacted] on the non-federal entity's systems. [description of activity] [redacted] acquired through the systems. [redacted]

[redacted]

33. Based on these facts in the Application, 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. Pursuant to subsection 34(1) of the *CSE Act*, for the Minister to issue a cybersecurity authorization, he 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."

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 legislation and have a rational connection with its objectives. As for the notion of "proportionate", it entails that 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 20 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 the [*sic* non-]federal systems from mischief, unauthorized use, or disruption."

38. The issuance of the Authorization reflects the Minister's conclusion that even though the activities would permit CSE to access systems that are in Canada, they do not contravene the legislative prohibition against directing CSE activities at Canadians or persons in Canada. The 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 that cybersecurity activities are not directed at individuals provided they focus on the cyber threat posed to the system. I find CSE's view, and consequently the Minister's conclusion, on this issue reasonable. Indeed, CSE's cybersecurity and information assurance mandate can only be fulfilled by accessing systems in Canada. I am also satisfied that the record shows the Minister is justified in implicitly concluding that the cybersecurity activities set out in the Authorization focus on the cyber threat, and not on individuals.

39. The Minister justifies that the activities are reasonable in two parts. First, the Minister explains that it is reasonable for CSE to be involved in the cybersecurity response. [redacted] based on information provided by the Chief, the Minister reports that the non-federal entity's systems [redacted]. As a result, the Minister concludes that the current state of the information systems' cybersecurity posture is insufficiently developed to [redacted] Indeed, the Minister explains that [description of activity] [redacted]

40. The Minister's justification sets out in broad terms the chronology of CSE's involvement, including that it [redacted] to the non-federal entity to establish and secure its cybersecurity posture. He explains that [redacted]

41. Second, the Minister explains that the activities for which approval is sought in the Authorization are reasonable because they would allow CSE to identify and better understand malicious cyber activity or other indicators of compromise in order to advise the non-federal entity on how to protect its systems and to conduct mitigation actions [redacted], as well as provide information that can help protect federal systems and other systems of importance. In essence, the activities would be reasonable because they would be effective.

42. The Minister relies on the Chief's Application to make conclusions with respect to the state of the non-federal entity's systems as well as the effectiveness of the proposed cybersecurity activities. I believe this to be reasonable. I do not expect the Minister, nor is it his role, to have that expertise. Indeed, the *CSE Act* specifically sets out that the Chief's Application "must set out the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it are met" (s 33(2), *CSE Act*). Nevertheless, a reasonable ministerial conclusion within the authorization framework must be justified and intelligible (*Vavilov*, para 99), which entails that even where the Minister adopts as his own the Chief's conclusions, he must exhibit an understanding of the rationale of his conclusions.

43. 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 non-federal entity's current needs and the proposed CSE activities. There is a clear rational connection between CSE's proposed cybersecurity activities and their objective, which is to help protect non-federal infrastructures - although I note that the record could have provided additional details on the relationship between [redacted]. 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 non-federal entity. 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

44. The Minister concluded at paragraph 30 of the Authorization that he had reasonable grounds to believe the activities authorized are "proportionate given the manner in which they are conducted and because they are rationally connected to the objective and minimally impair the rights and freedoms of third parties".

45. The activities for which authorization is sought would allow CSE to acquire a large volume of information generated by or residing with the non-federal entity. Indeed, the effectiveness of the activities rests on the acquisition of a large volume of information. The Minister therefore explains that the measures and controls in place render the activities proportional, as they help ensure that CSE uses and retains only the information necessary or essential to protect the non-federal systems, and safeguard any information that may contain a Canadian privacy interest. The notions of necessary and essential are analysed below in this decision.

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

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.

47. I note that the measures set out from a) to d) essentially mirror the statutory requirements found at subsection 34(3) of the *CSE Act* that are applicable to cybersecurity authorizations. I do not believe it is particularly helpful for the Minister to justify that a statutory condition has been met – in this case, that the activities are proportionate – by relying on satisfying separate statutory conditions that themselves have to independently be met (as set out at ss 34(3)(a), (c)(ii) and (d)(ii)).

48. I additionally note that whereas the measure set out at c) states that Canadian-related information can be retained when essential for the purpose of protecting the non-federal entity and/or other federal systems and systems of importance, paragraph 34(3)(d)(ii) of the *CSE Act* limits the retention of Canadian-related information for the purpose of protecting systems designated under subsection 21(1) as being of importance to the Government of Canada in the case of authorizations issued under subsection 27(2). I recognize that information acquired and retained pursuant to this Authorization can be used for other aspects of CSE's mandate, but point out that the initial retention must comply with the legislative requirements.

49. With respect to some of the other measures, the record lacks specific information. First, although "most of the analysis" is done through automated processes that limit employees' access, there is no information on what components of the analysis is conducted by employees. The Minister, and I as Intelligence Commissioner, should have an understanding

of the non-automated elements of the analysis, especially if they involve the information most likely to contain a privacy interest. This is important information in determining whether the activities are proportional.

50. Second, despite stating that the activities would only allow for the acquisition and use of information that is necessary to help protect the non-federal entity's systems, there is a lack of specification in the Minister's conclusions, and in the record as a whole, on what type of information is acquired. The Chief's Application describes classes of information that would be collected pursuant to the Authorization that do not appear to raise privacy interests. However, the Application also explains that CSE may incidentally acquire information that risks interfering with a reasonable expectation of privacy of a Canadian or a person in Canada, [types of information] [redacted]. The Application explains that this information is [redacted] I understand CSE is not interested in the content of the information in which there is a reasonable expectation of privacy [redacted], but rather in what it can reveal about [redacted] – and that it will only be retained when it is essential to protect the non-federal entity's systems. Nevertheless, given that the acquisition of information is automated, it is unclear when incidental collection of Canadian related information is acquired.

51. I do not, however, think that the lack of specifics is fatal to the reasonableness of the Minister's conclusions. I am of the view that the Minister's reliance on the measures and controls in place, aside from the measures that mirror the statutory requirements of subsection 34(3), support his conclusion that the activities are proportionate. Further, the Minister's conclusions clearly reflect his understanding that the specific cybersecurity activities allowing for the acquisition of information is necessary to attain the objective of protecting the system. To the extent that information that may contain a Canadian privacy interest is acquired and retained, access to it and its use would be limited.

52. 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 systems where CSE has received the express consent of the owner of the non-federal infrastructure to

operate. Since CSE will have the required consent to access the systems, the possible contraventions of Canadian laws are remote. In the event an Act of Parliament is breached, the impact of the breach will be limited and 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.

53. Section 5.3 of the 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 – indicates that CSE can demonstrate the necessity, reasonableness and proportionality of its cybersecurity activities through measures applied in the collection, use, analysis, retention and sharing of information. With respect to the proportionality of the activities, the MPS states: "using and analyzing retained information in a way that ensures the proportionality of the approach to the goal (e.g., using the least intrusive methods available; balancing operational needs with the privacy rights of Canadian and persons in Canada)." I am of the view that this balancing has been conducted.

54. In sum, the record reveals that the Minister was alive to the fact that the activities would allow for the acquisition of a large volume of information. He considered that given the objective of the activities, the nature of the information acquired, and the measures in place to limit access to the information, the balance weighed in favour of allowing CSE to conduct the proposed activities. I find that the Minister has sufficiently justified his conclusions and that they are supported by the record. As a result, I am satisfied that the Minister's conclusions in relation to the proportionality of the activities is reasonable.

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

55. 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 reasonably necessary

56. The Authorization describes how information assessed for the purpose of protecting non-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 acquired is included in the record. At paragraph 31, the Minister concluded that he had reasonable grounds to believe that the information will not be retained by CSE for longer than is reasonably necessary to achieve the cybersecurity aspect of its mandate. I note that the Chief indicates in the Application that the non-federal entity can, at any time, request that CSE delete the information it has acquired from or through its systems.

57. Since it is not possible for CSE to determine what information is needed in advance, the effectiveness of CSE's activities depend on the assessment, [redacted] of the large volume of information it acquires. The objective is to assess acquired information without significant delay to better understand and to retain useful information. However, given that some compromises may be identified after a malicious activity first began, the effectiveness of CSE's activities also depend on being able to assess information already acquired.

58. The Minister explains that a [redacted] retention period 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 its unassessed information and determine whether they exist within the Government of Canada federal networks and other systems of importance. After a [redacted] period,

information will be automatically deleted unless deemed necessary or essential to help protect the non-federal entity's systems, or federal systems and other systems of importance.

59. The "necessary" criterion applies to information that does not relate to a Canadian or 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 including behavioural patterns, capabilities, intentions, or vulnerability patterns, for the purpose of helping to protect federal institutions and non-federal systems of importance.

60. 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 institutions and the electronic information on those systems. Information related to Canadians that is retained is tracked internally in CSE in accordance with the policy requirements outlined throughout the MPS.

61. As per the *Retention and Disposition Table* included in the record, 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 otherwise no longer be kept when it ceases to be useful for those purposes.

62. With regard to information that is 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 whether it is still 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".

63. Given the important 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] assessment period reasonable. However, I note that in

a previous decision with respect to non-federal infrastructures, I suggested that CSE provide concrete examples to support its explanation for the [redacted] retention of unassessed information. The operational basis for what constitutes a "reasonable analysis period" should be set out more clearly for the Minister and myself. My comment is only reinforced given that CSE [redacted]

64. I also agree with the Minister's conclusion that information that is 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 dictated by the non-federal entity, as long as there is a periodic review with respect to information related to Canadians and persons in Canada. Retaining information the length of time needed to respond to that threat is justified.

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

65. Through its cybersecurity solutions, CSE is granted extensive access to the non-federal entity's information infrastructures for detection and further analysis of anomalous activity. The Minister's conclusions explain how [describing how the information is necessary] [redacted] It is not possible for CSE to predict [redacted] Therefore, CSE must acquire the vast range of information [redacted]

66. The Minister explains that any information acquired will be used by CSE's automated processes to help identify malicious activities. The cybersecurity activities will only be effective with the acquisition of the information. He provides examples that show how the information acquired under the Authorization is necessary to identify, isolate, prevent or mitigate harm to the non-federal systems. For these reasons, I find that the Minister's conclusion is reasonable.

iii. 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 the non-federal entity's systems

67. As previously indicated, when conducting cybersecurity activities CSE may incidentally acquire information relating to a Canadian or a person in Canada that may interfere with a reasonable expectation of privacy. 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 45 of the Authorization, the Minister concludes that he has reasonable grounds to believe that the measures referred to in section 24 have been met.

68. The Minister specifies that information relating to a Canadian or a person in Canada can only be retained if it is assessed to be essential. This condition is also 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 the non-federal entity's systems, or to federal systems and other systems of importance. I am of the view that CSE's understanding of the term "essential" is reasonable.

69. 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. I return to the subject of essentiality rationales in my remarks.

70. The Minister's conclusions specifies 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, most of the analysis of the information is done through automated processes, limiting the employees' access to unassessed information.

71. 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 under section 45 of the *CSE Act* [description of persons or classes of persons] To receive information disclosed by CSE that relates to a Canadian or person in Canada, the information must be necessary to help protect the electronic information or information infrastructure of the non-federal entity.

72. Canadian private communications, , that are incidentally acquired are accounted for in the End of Authorization Reports provided to the Minister, a copy of which is provided to the Intelligence Commissioner, pursuant to section 52 of the *CSE Act* (Section 52 Report). The latest Section 52 report shows that none were acquired, retained or shared.

73. 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. The policies and practices support the Minister's conclusions 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 the non-federal entity's systems. I find the Minister's conclusions to that effect reasonable.

V. REMARKS

74. Although I am satisfied that the Minister's conclusions are reasonable, I would like to make four remarks to assist in the consideration and drafting of future ministerial authorizations. These remarks do not alter my findings regarding the reasonableness of the Minister's conclusions.

i. Information related to Canadians or persons in Canada

75. Although the record sets out types of information related to a Canadian or a person in Canada that may be incidentally acquired and subsequently retained, there is no information with respect to what information has actually been retained. As indicated previously, essentiality rationales are recorded by CSE, but no information concerning these is presented to the Minister. [redacted] and I am of the view that CSE should have a solid grasp of the nature and volume of information that is retained and used, particularly with respect to information related to a Canadian or a person in Canada. This grasp should be even stronger when CSE is implementing the [redacted]

76. I would expect that CSE provide the Minister and myself with a greater understanding of the nature, frequency and volume of the retention of information where Canadian privacy interests are involved. Indeed, this information should be provided every time CSE requests approval of [redacted]. The manner in which activities have [redacted] may be a factor in determining whether an activity is reasonable and proportional.

77. I would also expect that this information be included in the Section 52 Report provided to the Minister within 90 days after the last period of validity of the authorization. I recognize that the number of intercepted private communications and solicitor-client communications is included. However, Canadian privacy concerns in the cybersecurity context go beyond these two categories. Finally, should information that will eventually appear in the Section 52 Report be known when the Chief submits an application to the Minister for the same activities, I am of the view that it should be submitted to the Minister and myself to provide us with a greater understanding of the actual impact on Canadian privacy interests.

ii. References to the Mission Policy Suite for Cybersecurity

78. I find it necessary to reiterate a remark made in my decision in File 2200-B-2023-02 issued on June 13, 2023. On a number of occasions, the record refers to the MPS, a document of more than 100 pages, with no references to the specific policy provisions. In judicial and quasi-judicial proceedings, in particular when there is no oral hearing, reference to the specific provisions of statutes and policies should be included in the written material to enable the decision maker to have a clear understanding of the matter before them. I am asking that this practice be implemented in future files.

79. Further, this version of the MPS has undergone several modifications in comparison to the previous version included in last year's authorization. I am asking that in future files, relevant amendments to the MPS be highlighted, in some way, in order to facilitate its review of evolving legal and policy developments.

iii. [redacted]

80. The [description of activity] [redacted] in the context of a cybersecurity authorization was dealt with at length in a remark made in File 2200-B-2023-02. In summary, the former Intelligence Commissioner had not approved a particular activity [redacted] and in the matter before me, CSE was no longer seeking authorization for the activity on the basis that ministerial approval for the activity was not necessary. I raised a concern that there was a lack of explanation in that record leading to that conclusion. I recognize that the file currently before me relates to subsection 27(2) of the *CSE Act* whereas File 2200-B-2023-02 was brought pursuant to subsection 27(1) of the *CSE Act*, but note that the wording of both provisions mirror each other. My concern remains unaddressed and I expect CSE to provide a satisfactory response in the context of a future request for a cybersecurity authorization.

iv. Documents supporting the Minister's determination

81. I have noted that the Minister's letter to myself is not dated. Further, the Authorization's signature block includes a line for "Issued at" which was not filled. Documents supporting the Minister's determination are subject to the Intelligence Commissioner's quasi-judicial review must be official documents duly completed by the decision maker. They constitute part of the justification and accountability framework established by Parliament regarding intelligence gathering and cyber security activities and I trust the Minister will address this issue in future files.

82. Further, paragraph 11 of the Authorization mistakenly indicates that "I, as Minister of National Defence, issued an authorization in [redacted] The Authorization has a few other discrepancies (such as paragraph 20 of the Authorization where the Minister concludes that he has reasonable grounds to believe that the activities authorized will help protect federal systems, instead of non-federal systems). Although I recognize that drafting oversights occur, an authorization containing too many could undermine the reasonableness of the Minister's conclusions.

VI. CONCLUSIONS

83. 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 54 of the Authorization are reasonable.

84. I therefore approve the Minister's Cybersecurity Authorization for Activities to Help Protect Non-Federal Infrastructures dated October 6, 2023, pursuant to paragraph 20(1)(a) of the *IC Act*.

85. 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.

86. 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.

87. 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 the non-federal entity's cybersecurity posture.

November 3, 2023

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner