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-2022-06

IN THE MATTER OF AN APPLICATION BY THE COMMUNICATIONS SECURITY ESTABLISHMENT TO THE MINISTER OF NATIONAL DEFENCE FOR A *CYBERSECURITY AUTHORIZATION FOR ACTIVITIES ON NON-FEDERAL INFRASTRUCTURES* – [redacted]

PURSUANT TO SUBSECTION 27(2) OF THE *COMMUNICATIONS SECURITY ESTABLISHMENT ACT*

INTELLIGENCE COMMISSIONER

DECISION AND REASONS

December 8, 2022

Canada

TABLE OF CONTENTS

I. OVERVIEW

1. On [redacted], pursuant to subsection 27(2) of the *Communications Security Establishment Act*, SC 2019, c 13, s 76 (*CSE Act*), the Minister of National Defence (the Minister) issued the *Cybersecurity Authorization For Activities On Non-Federal Infrastructures* – [redacted] (the *Authorization*).

2. 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*).

3. In accordance with section 23 of the *IC Act*, the Minister confirmed in her cover letter that she provided me with all information that was before her when issuing the *Authorization*.

4. My review of the record confirms that before issuing the *Authorization*, the Minister received a written application (the *Application*) from the Chief of CSE, which includes amongst others the written request from the owner or operator of the information infrastructure, as required by subsections 33(1) and (3) of the *CSE Act*.

5. The *Application* sets out the facts that allowed the Minister to conclude, pursuant to subsection 33(2) of the *CSE Act*, that there are reasonable grounds to believe that the *Authorization* is necessary, and that the conditions set out in section 34 of the *CSE Act* are met.

6. Specifically, the Minister concluded pursuant to subsection 34(1) of the *CSE Act*, that she had reasonable grounds to believe that the proposed cybersecurity activities described in the *Authorization* are reasonable and proportionate, having regard to the nature of the objective and the nature of the activities.

7. The Minister also concluded that she had reasonable grounds to believe that the conditions, set out in subsection 34(3) of the *CSE Act*, were met.

8. For the reasons that follow, I am satisfied that the Minister's conclusions are reasonable. Consequently, pursuant to paragraph 20(1)(a) of the *IC Act*, I approve the *Authorization* in relation to [redacted] issued by the Minister.

II. BACKGROUND

9. [redacted]

10. [redacted]

11. As part of its responsibility for exercising such functions, [redacted], holds information of importance to the Government of Canada, including [redacted].

12. [redacted] electronic information and information infrastructure is a system of importance as defined in the *Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada* issued on August 25, 2020.

13. On [redacted] the Communications Security Establishment (CSE) received information from [redacted]

[redacted]

14. [redacted], also informed CSE that [redacted]

15. [redacted]

16. The record indicates that [redacted] More specifically, according to the record, [redaction] would almost certainly consist of [redacted]

17. [redacted]

18. [redacted]

19. [redacted]

20. [redacted]

21. On [redacted] CSE notified [redacted] of the compromise, based on the information received from [redacted]

22. On [redacted] the [redacted] Chief Information Officer of [redacted] – who has the authority to provide access to [redacted] electronic devices and networks – sent a written request to CSE. Essentially, the Canadian Centre for Cyber Security (CCCS) was asked to conduct cyber defence activities to assist [redacted] in the protection of the electronic information and information infrastructure under its control and supervision.

23. On [redacted] the Chief of CSE submitted an *Application* to the Minister of National Defence requesting approval of an *Authorization* to carry out activities that may contravene Acts of Parliament or that may risk interfering with the reasonable expectation of privacy of a Canadian or a person in Canada.

24. The *Application* explains that [redacted] current security posture cannot sufficiently identify and counter [redacted]

25. In fact, [redacted]

26. What is known is that the compromise [redacted]

27. As indicated in the *Application*, it is likely that [redacted]

28. [redacted]

29. As a result, the *Application* provides a rationale for [redacted] CSE cybersecurity solutions to be deployed: [redacted] solutions will ensure that gaps are identified and that [redacted] posture is well positioned to protect critical information.

30. These proposed cybersecurity solutions would acquire information to feed advanced intrusion detection and analysis solutions which will allow CSE to identify, isolate, prevent or mitigate harm to [redacted] electronic information and information infrastructure. They would also enable CSE to recommend mitigation actions to be implemented either by [redacted] or by CSE with [redacted] consent.

31. As specified in the *Application*, the cybersecurity solutions would be [redacted] information infrastructure. These solutions would [redacted] in retrieving relevant information.

32. By deploying the proposed cybersecurity solutions, CSE would provide [redacted] with an assessment of [redacted] CSE would also provide [redacted] with instructions and ongoing support during the deployment process. [redacted] would also be notified of any major incidents detected. This will position [redacted] to strengthen and improve its cybersecurity posture in the long term.

33. The *Application* also notes that in helping [redacted] CSE would also bolster its own understanding of [redacted] This would further help CSE in protecting federal institutions and other systems of importance to the Government of Canada.

34. The *Application* explains that the information acquired by CSE on [redacted] infrastructure would also be required for the understanding of malicious cyber activities, including [redacted]

35. In addition to noting the objectives to be achieved, the *Application* also describes how the information collected by the cybersecurity solutions would be stored, analyzed and retained. It also sets out the measures and safeguards in place to protect the privacy of Canadians and persons in Canada.

36. On [redacted] the Minister of National Defence issued the *Authorization*.

III. LEGISLATION

A. *Communications Security Establishment Act*

37. As described in subsection 15(1) of the *CSE Act*, CSE is Canada's national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance.

38. CSE has five aspects to its mandate, one of them being cybersecurity and information assurance. As set out in section 17 of the *CSE Act*, CSE may, under this aspect: a) provide advice, guidance and services to help protect electronic information and information infrastructure designated pursuant to subsection 21(1) of the *CSE Act* as being of importance to the Government of Canada; and b) acquire, use and analyse information from the global information infrastructure or from other sources in order to provide such advice, guidance, and services.

39. When engaging in these activities, CSE may contravene any other Act of Parliament, such as Part VI of the *Criminal Code* in relation to invasion of privacy. It may also conduct acquisition activities that may risk interfering with the reasonable expectation of privacy of a Canadian or a person in Canada, unless they are carried out under an authorization issued in accordance with subsection 27(2) of the *CSE Act*.

40. Subsection 27(2) of the *CSE Act* outlines the authorization regime for the cybersecurity and information assurance aspect of CSE's mandate for activities carried out on a designated non-federal infrastructure of importance to the Government of Canada. The designation is a prerequisite to the issuance of the authorization by the Minister.

41. Specifically, the subsection stipulates that the Minister may authorize CSE, despite any other Act of Parliament, to: 1) access an information infrastructure designated under subsection 21(1) of the *CSE Act* of importance to the Government of Canada, and 2) acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, from mischief, unauthorized use, or disruption, as described in paragraph 184(2)(e) of the *Criminal Code*, RSC 1985, c C-46.

42. The Minister issues the cybersecurity authorization when satisfied that the conditions in subsections 34(1) and (3) of the *CSE Act* have been met.

B. *Intelligence Commissioner Act*

43. Pursuant to section 12 of the *IC Act*, the Intelligence Commissioner is responsible for reviewing the conclusions on the basis of which certain authorizations are issued under the *CSE Act.* If those conclusions are reasonable, the Intelligence Commissioner approves the authorization in question and provides written reasons for doing so.

44. Section 14 of the *IC Act*, relating to the issuance of a cybersecurity authorization states that the Intelligence Commissioner must review whether the conclusions of the Minister on the basis of which the authorization was issued are reasonable.

45. As per subsection 23(1) of the *IC Act*, the Intelligence Commissioner's quasi-judicial review must be performed, on the basis of all the information, which was before the Minister when issuing the authorization. This includes all written or verbal information.

46. The Intelligence Commissioner approves the authorization if he or she is satisfied that the conclusions of the Minister are reasonable (subsection 20(1) of the *IC Act*.)

47. The authorization is only valid after it is approved by the Intelligence Commissioner (subsection 28(1) of the *CSE Act*). It is only then that the CSE may carry out the authorized activities described in the authorization.

48. The Intelligence Commissioner's decision may be reviewable by the Federal Court on an application for judicial review, pursuant to section 18 of the *Federal Courts Act*, RSC, 1985, c F-7.

IV. STANDARD OF REVIEW

49. As indicated previously, pursuant to sections 12 and 14 of the *IC Act*, the Intelligence Commissioner must review whether the Minister's conclusions are reasonable.

50. The term "reasonable" is neither defined in the *IC Act* nor in the *CSE Act*. However, it is a term that has been associated in administrative law jurisprudence with the process of "judicial review" of administrative decisions.

51. In accordance with subsection 4(1) of the *IC Act*, the Intelligence Commissioner must be a retired judge of a superior court. However, the Intelligence Commissioner is not a court of law. As such, he or she does not perform "judicial review" but rather "quasi-judicial review" of the Minister's conclusions, who is acting as an administrative decision maker. As established by the Intelligence Commissioner's jurisprudence, when Parliament used the term "reasonable" in the context of a quasi-judicial review of administrative decisions, it intended to give to that term the meaning it has been given in administrative law jurisprudence. For these reasons, I will apply the standard of reasonableness to my review.

52. The leading case regarding the standard of review to be applied in an administrative law context is *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65 [*Vavilov*]. In its decision, the majority of the Supreme Court of Canada clearly indicated that reasonableness is the presumptive standard of review when reviewing administrative decisions on their merits.

53. When making a determination as to whether the conclusions issued by the Minister are reasonable, I am guided by the following passage found at paragraph 99 in *Vavilov*.

> [99] 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: *Dunsmuir*, at paras. 47 and 74; *Catalyst*, at para. 13.

54. In its decision, the majority of the Supreme Court of Canada also stated that a reasonable decision is based on internally coherent reasoning and must be justified in light of the legal and factual constraints that bear on the decision.

55. In order to better understand the role of the Intelligence Commissioner when conducting a quasi-judicial review, it is important to refer to the objectives of Bill C-59 the *National Security Act, 2017*, SC 2019, c 13 and its Preamble, which led to the creation of the *IC Act*, the *CSE Act*, and made important amendments to the *Canadian Security Intelligence Service Act*, RSC, 1985, c C-23.

56. I have reproduced below the relevant portions which I consider relate directly to my role as Intelligence Commissioner:

> Preamble
>
> Whereas a fundamental responsibility of the Government of Canada is to protect Canada's national security and the safety of Canadians;

> Whereas that responsibility must be carried out in accordance with the rule of law and in a manner that safeguards the rights and freedoms of Canadians and that respects the *Canadian Charter of Rights and Freedoms*;
>
> Whereas the Government of Canada is committed to enhancing Canada's national security framework in order to keep Canadians safe while safeguarding their rights and freedoms;
> …
>
> Whereas enhanced accountability and transparency are vital to ensuring public trust and confidence in Government of Canada institutions that carry out national security or intelligence activities;
>
> Whereas those institutions must always be vigilant in order to uphold public safety;
>
> Whereas those institutions must have powers that will enable them to keep pace with evolving threats and must use those powers in a manner that respects the rights and freedoms of Canadians;

57. It is interesting to note in the excerpts of the Preamble quoted above the important balancing between national security interests and respect for the "rule of law" and the "rights and freedoms of Canadians". In seeking to preserve this balance, Parliament created the role of the Intelligence Commissioner as a gatekeeper and as an overseer of Ministerial Authorizations as they relate to cybersecurity in this matter.

58. In light of the above, I believe that in determining if the Minister's conclusions are reasonable in the context of national security, I am to carefully consider and weigh the important privacy and other interests of Canadians and persons in Canada. Therefore, I consider that this is the *raison d'être* of my role as the Intelligence Commissioner of Canada.

59. In support, I would like to quote from the Minister of Justice's *Charter Statement* which was prepared when Bill C-59 was tabled. My attention was drawn to the following passages which describes the role of the Intelligence Commissioner as follows:

> In addition, Part 2 of Bill C-59, the *Intelligence Commissioner Act*, would establish an independent, quasi-judicial Intelligence Commissioner, who would assess and review certain Ministerial decisions regarding intelligence gathering and cyber security activities. This would ensure an independent consideration of the important privacy and other interests implicated by these activities in a manner that is appropriately adapted to the sensitive national security context.
>
> …
>
> A key change proposed in Bill C-59 is that the activities would also have to be approved in advance by the independent Intelligence Commissioner, who is a retired superior court judge with the capacity to act judicially.

60. I recognize that my independent quasi-judicial review must take into consideration the reasonableness of the Minister's conclusions as they relate to the privacy interests of Canadians and persons in Canada with other relevant and important interests triggered by cybersecurity activities in the context of national security.

61. Let us now review the ministerial conclusions keeping in mind what is said above.

V. ANALYSIS

62. In accordance with section 14 of the *IC Act*, I must review whether the Minister's conclusions – made under subsections 34(1) and (3) of the *CSE Act* and on the basis of which the *Authorization* was issued under subsection 27(2) of the *CSE Act* – are reasonable.

63. Based on the facts presented in the *Application*, the Minister concluded on reasonable grounds that the *Authorization* is necessary and that the conditions of subsections 34(1) and (3) of the *CSE Act* were met.

64. The Minister also recognized that without the *Authorization* in question, the authorized activities referred to in paragraph 67 may be contrary to other Acts of Parliament, or may interfere with the reasonable expectation of privacy of a Canadian or a person in Canada.

65. That said, the Minister issued a one-year *Authorization*, which includes additional terms, conditions and restrictions.

i. 34(1) – Are the activities reasonable and proportionate?

66. Subsection 34(1) of the *CSE Act*, stipulates that the Minister must conclude, that there are reasonable grounds to believe that any proposed activity to be authorized is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities.

67. When assessing whether the activities are reasonable and proportionate, the Intelligence Commissioner's jurisprudence, defines the notion of "reasonable and proportionate" as set out with proportionality test developed by the Supreme Court of Canada in *R. v. Oakes*, [1986] 1 SCR 103.

68. The notion of "reasonable" includes an activity that is fair, sound, logical, well-founded and well-grounded having regard to the objective.

69. As for the notion of "proportionate", it requires that the activity be rationally connected to the objective, minimally impairing on the rights and freedoms of third parties as well as their equipment and infrastructures. Importantly, it entails that the acquisition of information does not outweigh the objective of helping to protect non-federal electronic information and information infrastructures of importance to the Government of Canada. Also, if necessary to achieve this purpose, measures should be in place to restrict the acquisition and/or the retention of information.

70. In the *Authorization*, the Minister indicated, at paragraph 31, that she had reasonable grounds to believe that:

> [T]he activities authorized in this Authorization are reasonable because they are a fair, sound, logical, and well-founded means of achieving the objective of helping to protect [redacted] electronic information and information infrastructure, as well as potentially protect federal systems

and other systems of importance to the GC from mischief, unauthorized use, or disruption.

71. Having carefully reviewed the conclusions of the Minister, I am satisfied that they are reasonable in determining that the described activities are indeed reasonable and proportionate, having regard to the nature of CSE's objective of helping to protect non-federal electronic information and information infrastructures, and the nature of those cybersecurity activities.

72. I come to this determination based on the following factors:

i. [redacted] is a non-federal system of importance to the Government of Canada;

ii. [redacted]

iii. [redacted]

iv. The cybersecurity activities are subject to measures and controls as described throughout the *Authorization*;

v. CSE recommends actions for implementation by [redacted] and CSE may only apply those measures with the consent of [redacted]

vi. The proposed cybersecurity solutions are reviewed for legal and policy compliance;

vii. Important safeguards are in place, should information acquired by CSE present a risk of interfering with the reasonable expectation of privacy of a Canadian or a person in Canada; and

viii. Every search performed on the acquired information is auditable to comply with CSE's *Mission Policy Suite Cybersecurity* and other corporate polices. Audit logs are retained and available for review and oversight purposes.

ii. 34(3) – Have the conditions been met?

73. As specified in subsection 34(3) of the *CSE Act*, the Minister may issue a cybersecurity authorization for activities on a non-federal infrastructure only if she concludes that there are reasonable grounds to believe that the three conditions listed in the subsection are met.

74. In the *Authorization*, the Minister described how (1) any information acquired under the *Authorization* will be retained for no longer than is reasonably necessary; (2) any information acquired under the *Authorization* is necessary to identify, isolate, prevent or mitigate harm to [redacted] electronic information and information infrastructures; and (3) the measures referred to in section 24 of the *CSE Act* will ensure that information acquired 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 [redacted] electronic information and information infrastructures.

75. I am satisfied that these conditions have been met.

iii. Are the Minister's conclusions reasonable?

76. When considering the record as a whole, my quasi-judicial review leads me to find that the Minister's conclusions are internally coherent. As per the guidance provided by the Supreme Court of Canada in *Vavilov*, the conclusions are justified, transparent and intelligible in relation to the relevant factual and legal constraints that bear on the decision.

77. The Minister's conclusions also demonstrated that she had reasonable grounds to believe, based on the credible and compelling information found in the *Application* and generally in the record, that all the conditions, found in subsections 34(1) and (3) of the *CSE Act*, for issuing the *Authorization* were met.

78. In light of the above, I am satisfied that the Minister's conclusions are reasonable with respect to the proposed cybersecurity activities described in the *Authorization*.

VI. REMARKS

79. In my previous decision dealing with a Cybersecurity Authorization for Activities on Non-Federal Infrastructures (2200-B-2022-05), I made four selected remarks.

80. My first remark was in regards to the statement made in the *Authorization* and *Application* regarding the additional use of information acquired under a cybersecurity authorization [redacted]

81. My second remark was in relation to the [redacted] and [redacted] retention periods of acquired information. My third and fourth remarks were in reference to the timing of when the Intelligence Commissioner ought to be advised of information relating to solicitor-client communications and the contravention of any other Act of Parliament.

82. I am of the view that the Minister and the Chief of CSE addressed these remarks to my satisfaction in the current *Authorization* and *Application*.

83. That being said, I would like to make the following two remarks to assist in informing future applications and authorizations.

i. Lapse of time

84. My first remark deals with the lapse of time between [redacted] which occurred on [redacted], and the reporting of this event [redacted] to CSE on [redacted] which is [redacted] after the incident.

85. The record does not explain this lapse of time, which raises some questions regarding the urgency for CSE to provide [redacted] For example, the

record could have indicated whether [redacted]

86. Obtaining more detailed information in this regard would have been beneficial to the Minister and myself. If CSE cannot account for this [redacted] lapse of time, an explanation should have been provided to the Minister and acknowledged in the ministerial conclusions.

ii. [redacted]

87. My second remark relates to [redacted]

88. The record provides substantial and useful information regarding this [redacted] One of the documents submitted by the Minister was prepared by the Canadian Centre for Cyber Security (CCCS) which describes [redacted] (i.e. Annex III). I note that the document is not dated. While there is the number at the bottom of the document ending with [redacted], it was not clear to me whether this was the date the document was disseminated.

89. Going forward, I trust that all documents contained in the record will be dated.

90. In addition, I noticed that the information contained in the CCCS document refers to [redacted]. While the *Application* repeats some of the information included in the document, it does not provide [redacted]

91. Given this noticeable gap in time, details are missing with respect to the [redacted]

92. I am of the view that, if available, an update on any [redacted] would have assisted the Minister, as the decision

maker, to bolster her conclusions in this matter. Conversely, if no further updated information was available, it should have been specified in the record.

93. Notwithstanding these two remarks, although important in themselves, they do not alter my findings regarding the reasonableness of the Minister's conclusions as they demonstrate transparency and intelligibility.

VII. CONCLUSIONS

94. Based on my review of the record submitted, I am satisfied that the conclusions of the Minister are reasonable with regard to the cybersecurity activities described at paragraph 67 of the *Authorization*.

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

96. 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.

97. 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.

December 8, 2022

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