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

~~PROTECTED B~~

File: 2200-B-2022-05

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

November 14, 2022

Canada

TABLE OF CONTENTS

I. OVERVIEW 3
II. BACKGROUND 4
III. LEGISLATION 6
A. What is the Role of the Minister? 6
B. What is the Role of the Intelligence Commissioner? 7
IV. STANDARD OF REVIEW 8
V. ANALYSIS 13
A. Are the Minister's conclusions reasonable? 13
i. 34(1) – Are the activities reasonable and proportionate? 14
ii. 34(3) – Have the conditions been met? 16
iii. Am I satisfied that the Minister's conclusions are reasonable? 16
VI. REMARKS 17
i. Use of Information Acquired Under a Cybersecurity Authorization for Other Aspects of CSE's Mandate 17
ii. Retention of Acquired Information 18
iii. Solicitor-Client Communications 19
iv. Other Acts of Parliament 22
VII. CONCLUSIONS 22

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 must provide me with all information that was before her when issuing the *Authorization*. The Minister's cover letter dated [redacted], confirms that such information was provided. My review of the record indicates that it is complete.

4. As per subsection 33(1) of the *CSE Act*, the Chief of CSE provided the Minister with a written application (*the Application*) setting out the facts allowing her 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* for issuing it are met.

5. With regard to subsection 34(1) of the *CSE Act*, the Minister concluded 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. 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.

6. 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

7. As part of Canada's [redacted] is a non-federal entity considered to be of importance to the Government of Canada, as defined in the *Ministerial Order Designating Electronic Information and Information Infrastructure of Importance to the Government of Canada* issued on August 25, 2020.

8. The record indicates that [redacted]

9. [redacted]

10. On [redacted], CSE was first notified [redacted] that they had been a [redacted] Following a request from [redacted]

11. On [redacted], the Honourable Jean-Pierre Plouffe ("the former Intelligence Commissioner") [redacted]

12. On [redacted] request to CSE [redacted] in the protection of the electronic information and information infrastructure under its control and supervision.

13. On [redacted], the Chief of CSE submitted to the Minister an *Application* to obtain [redacted] *Authorization* in relation to [redacted]

14. The *Application* explains the rationale for the CSE cyber solutions deployed, the objectives to be achieved, and the supporting activities such as the analysis and retention of information. It also indicates how all these activities fulfill the objective of helping to protect [redacted] electronic information and information infrastructures, considered of importance to the Government of Canada. It also sets out the measures and safeguards in place to protect the privacy of Canadians and persons in Canada.

15. CSE's proposed cybersecurity activities, which have been requested from [redacted] involve accessing the non-federal institution's electronic information and information infrastructure and acquiring any information originating from, directed to, stored on, or being transmitted on or through those infrastructures for the purpose of helping to protect them.

16. As such, this would require the [redacted]

17. According to CSE, the [redacted] necessary while [redacted] CSE indicates that [redacted] by the combined effort of both CSE and [redacted] cybersecurity efforts. Despite [redacted] CSE

informs the Minister that [redacted]

18. Furthermore, CSE notes that [redacted]

19. CSE is of the view that issuing [redacted] *Authorization* in relation to [redacted] will allow CSE to [redacted] This will also give [redacted] the opportunity to ensure that any gaps identified in its current monitoring are addressed, and that its cybersecurity posture is sufficiently advanced to protect its systems [redacted]

20. Finally, CSE indicates that it will assess [redacted] progress throughout the course of the *Authorization* to determine when it can [redacted]

III. LEGISLATION

A. What is the Role of the Minister?

21. CSE has five aspects to its mandate, one of them being the cybersecurity and information assurance aspect, set out in section 17 of the *CSE Act*.

22. The Minister may, pursuant to subsection 27(2) of the *CSE Act*, issue to CSE an authorization for cybersecurity activities on non-federal infrastructures.

23. Specifically, the authorization allows CSE to, despite any other Acts of Parliament and in furtherance of its cybersecurity and information assurance aspect of its mandate, to access an information infrastructure designated under subsection 21(1) of the *CSE Act* as being of importance to the Government of Canada and to acquire any information originating from,

directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(e) of the *Criminal Code*, RSC 1985, c C-46, from mischief, unauthorized use, or disruption.

24. Before issuing the authorization, the Minister must first receive a written application from the Chief of CSE, which must include a written request from the owner or operator of the information infrastructure (subsections 33(1) and (3) of the *CSE Act*). The record confirms that this was done.

25. In addition, the application must, as stipulated in subsection 33(2) of the *CSE Act*, 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 found in subsections 34(1) and (3) of the *CSE Act* for issuing it are met.

26. In summary, subsection 34(1) of the *CSE Act* establishes 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.

27. As for, subsection 34(3) of the *CSE Act*, it specifies that the Minister may issue the authorization only if he or she concludes that there are reasonable grounds to believe that the specific conditions listed in the subsection are met.

28. It must be noted that the authorization is only valid if, pursuant to section 28 of the *CSE Act*, it is approved by the Intelligence Commissioner.

B. What is the Role of the Intelligence Commissioner?

29. Pursuant to section 12 of the *IC Act*, the Intelligence Commissioner is responsible in 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.

30. In this instance, pursuant to section 14 of the *IC Act*, the Intelligence Commissioner must review whether the conclusions of the Minister on the basis of which the *Authorization* in relation to [redacted] was issued are reasonable.

31. As stipulated in 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 cybersecurity authorization on non-federal infrastructure in question. This includes all written or verbal information.

32. Following this review, the Intelligence Commissioner, in accordance with paragraph 20(l)(a) of the *IC Act*, approves the authorization if he or she is satisfied that the conclusions at issue are reasonable. If the Intelligence Commissioner is not satisfied that the conclusions are reasonable, he or she must not approve the authorization, as per paragraph 20(1)(b) of the *IC Act*.

33. The authorization is only valid, pursuant to section 28 of the *CSE Act*, once the Intelligence Commissioner provides the Minister with a written decision indicating its approval. It is only then that the CSE may carry out the authorized activities described in the authorization.

IV. STANDARD OF REVIEW

34. Pursuant to sections 12 and 14 of the *IC Act*, the Intelligence Commissioner must review whether the Minister's conclusions are reasonable.

35. 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.

36. I concur with the former Intelligence Commissioner that when Parliament used the term "reasonable" in the context of a quasi-judicial review of administrative decisions by a retired judge of a superior court, it intended to give to that term the meaning it has been given in administrative law jurisprudence.

37. 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 it sought to provide guidance on how to conduct reasonableness review:

> [73] This Court's administrative law jurisprudence has historically focused on the analytical framework used to determine the applicable standard of review, while providing little guidance on how to conduct reasonableness review in practice.
>
> [74] In this section of our reasons, we endeavour to provide that guidance. The approach we set out is one that focuses on justification, offers methodological consistency and reinforces the principle "that reasoned decision-making is the lynchpin of institutional legitimacy": factum of the *amici curiae*, at para. 12.

38. I recognize that the review by the Intelligence Commissioner is not, as such, a judicial review – the Intelligence Commissioner not being a court of law-even though he or she has to be a "retired judge of a superior court" as per subsection 4(1) of the *IC Act*. Rather, the Intelligence Commissioner is responsible for performing a quasi-judicial review of the Minister's conclusions, who is acting as an administrative decision maker. I am of the opinion that the Intelligence Commissioner's decisions are reviewable by the Federal Court as a judicial review pursuant to section 18 of the *Federal Courts Act*, RSC, 1985, c F-7.

39. Given my legislative mandate to determine 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.

40. 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. Specifically it states that:

> *(1) A Reasonable Decision is Based on an Internally Coherent Reasoning*
>
> [102] To be reasonable, a decision must be based on reasoning that is both rational and logical. It follows that a failure in this respect may lead a reviewing court to conclude that a decision must be set aside. Reasonableness review is not a "line-by-line treasure hunt for error": *Irving Pulp & Paper*, at para. 54, citing *Newfoundland Nurses*, at para. 14. However, the reviewing court must be able to trace the decision maker's reasoning without encountering any fatal flaws in its overarching logic, and it must be satisfied that "there is [a] line of analysis within the given reasons that could reasonably lead the tribunal from the evidence before it to the conclusion at which it arrived": *Ryan*, at para. 55; *Southam*, at para. 56. ...
>
> [103] While, as we indicated earlier (at paras. 89-96), formal reasons should be read in light of the record and with due sensitivity to the administrative regime in which they were given, a decision will be unreasonable if the reasons for it, read holistically, fail to reveal a rational chain of analysis or if they reveal that the decision was based on an irrational chain of analysis: see *Wright v. Nova Scotia (Human Rights Commission)*, 2017 NSSC 11, 23 Admin. L.R. (6th) 110; *Southam*, at para. 56. A decision will also be unreasonable where the conclusion reached cannot follow from the analysis undertaken (see *Sangmo v. Canada (Minister of Citizenship and Immigration)*, 2016 FC 17, at para. 21 (CanLII) or if the reasons read in conjunction with the record do not make it possible to understand the decision maker's reasoning on a critical point (see *Blas v. Canada (Minister of Citizenship and Immigration)*, 2014 FC 629, 26 Imm. L.R. (4th) 92, at paras, 54-66; *Reid v. Criminal Injuries Compensation Board*, 2015 ONSC 6578; *Lloyd v. Canada (Attorney General)*, 2016 FCA 115, 2016 D.T.C. 5051; *Taman v. Canada (Attorney General)*, 2017 FCA 1, [2017] 3 F.C.R. 520, at para. 47).
>
> …

> *(2) A Reasonable Decision Is Justified in Light of the Legal and Factual Constraints That Bear on the Decision*
>
> [105] In addition to the need for internally coherent reasoning, a decision, to be reasonable, must be justified in relation to the constellation of law and facts that are relevant to the decision: *Dunsmuir*, at para. 47; *Catalyst*, at para. 13; *Nor-Man Regional Health Authority*, at para. 6. Elements of the legal and factual contexts of a decision operate as constraints on the decision maker in the exercise of its delegated powers.

41. 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.

42. 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;

43. 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 Intelligence Commissioner as a gatekeeper and as an overseer of Ministerial Authorizations as they relate to cybersecurity in this matter.

44. 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.

45. 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.

46. 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.

47. Let us now review the ministerial conclusions keeping in mind what is said above. In doing this, I have carefully read [redacted] the decision of the former Intelligence Commissioner.

V. ANALYSIS

A. Are the Minister's conclusions reasonable?

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

49. 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. The record indicates that the facts set out in the *Application* allowed the Minister to reach such conclusions.

50. The Minister also recognized that the authorized activities referred to in paragraph 54 of the *Authorization* 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.

51. As a result, the Minister issued [redacted] *Authorization*, which includes terms, conditions and restrictions.

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

52. As indicated previously, in accordance with subsection 34(1) of the *CSE Act*, 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.

53. When assessing whether the activities are reasonable and proportionate, the former Intelligence Commissioner, defined the notion of "reasonable and proportionate" in the context of the Cybersecurity Authorization for Activities on Non-Federal Infrastructures in relation to [redacted] as follows:

> [T]he notion of "reasonable" includes an activity that is fair, sound, logical, well-founded and well-grounded having regard to the objective. The notion of "proportionate" 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. In other words, it is a proper balance of the activities having regard to the "proportionate" aspects described in this paragraph.

54. I agree with this interpretation of reasonable and proportionate which aligns with the proportionality test developed by the Supreme Court of Canada in *R. v. Oakes*, [1986] 1 SCR 103. The three components of the test found at paragraph 70 are as follows;

> First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right or freedom in question: *R. v. Big M Drug Mart Ltd.*, supra, at p. 352. Third, there must be proportionality between the effects of the measures

> which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of "sufficient importance".

55. In the *Authorization*, the Minister indicated, at paragraph 23, 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.

56. 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.

57. 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] requested CSE's [redacted] assistance;
iv. CSE is not seeking to [redacted] as it remains necessary while [redacted] its cybersecurity posture;
v. CSE recommends actions for implementation [redacted] and CSE may only apply those measures with the consent of [redacted]
vi. The [redacted] has been demonstrated as the most effective and precise way to find indications of compromise and mitigate the compromise; and

vii. Important safeguards are in place to ensure that should information acquired present a risk that CSE will interfere with the reasonable expectation of privacy of a Canadian or a person in Canada.

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

58. Subsection 34(3) of the *CSE Act*, specifies that 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.

59. In the *Authorization*, the Minister described in detail how any information acquired under the *Authorization* will be retained for no longer than is reasonably necessary; any information acquired under the *Authorization* is necessary to identify, isolate, prevent or mitigate harm to [redacted] electronic information and information infrastructures; and 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.

iii. Am I satisfied that the Minister's conclusions are reasonable?

60. My quasi-judicial review of the record leads me to find that the Minister's conclusions, as per the guidance provided by the Supreme Court of Canada in *Vavilov*, are justified, transparent and intelligible in relation to the relevant factual and legal constraints that bear on the decision.

61. I am therefore satisfied that the Minister's conclusions are reasonable. She 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 the conditions for issuing the *Authorization* were met.

VI. REMARKS

62. Although I am satisfied that the Minister's conclusions are reasonable, I would nonetheless wish to make the following four selected remarks to assist in informing future applications and authorizations.

63. My first remark is in regards to the statement made in the *Authorization* and the *Application* regarding the additional use of information acquired under a cybersecurity authorization under the other aspects of CSE's mandate. My second remark is in relation to the [redacted] retention periods of acquired information. My third and fourth remarks are 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 other Acts of Parliament.

i. Use of Information Acquired Under a Cybersecurity Authorization for Other Aspects of CSE's Mandate

64. I note that the *Authorization* contains [redacted] information in paragraph 22, [redacted] stating the following:

> CSE may also use the cyber threat information acquired under this authorization to enable activities under the foreign intelligence or active and defensive cyber operations aspects of the mandate in line with the authorizations, conditions and prohibitions for each.

65. I have also taken note that a variant of this paragraph is also found in the *Application* at paragraph 43, which was included in [redacted] at paragraph 42.

66. I note that these paragraphs neither provide any explanation nor include the legal authority for CSE allowing for this use. In the future, I would expect that such information be provided to the Minister. Such information would also be of assistance to me in my review of record.

ii. Retention of Acquired Information

a. [redacted] *retention period*

67. The *Authorization*, at paragraph 59 indicates that CSE may acquire information and hold this information for [redacted] from the date of its acquisition.

68. It is stated that within these [redacted] CSE must assess the information for necessity or essentiality.

69. I understand from my review of the record and the relevant sections of the *CSE Act* that the "necessity test" applies to acquired information and the "essentiality test" applies to acquired information for which a Canadian or a person in Canada may have a reasonable expectation of privacy. I also note that if information is not identified as necessary or essential, the information will be automatically deleted after [redacted] of its acquisition date.

70. The *Application*, at paragraph 75, provides the following explanation as to why CSE deems this [redacted] period as reasonable:

> It is reasonable to retain unassessed information for a period of [redacted] from the date of its acquisition to allow for retrospective analysis and to provide valuable context for newly discovered malicious cyber activities. The retention period provides a reasonable analysis period to reach back to origins of an event and/or examine its evolution over time if it is identified as a compromise some time after malicious activity first began.

71. Although I have read and understand the rationale provided, in the future, I would suggest that more specific information be given, as well as concrete examples, to support CSE's explanation for the [redacted] retention requirement of unassessed information.

b. [redacted] *retention period*

72. My second remark has to do with the retention period of acquired information deemed to meet either the "necessity test" or the "essentiality test".

73. At paragraph 60 of the *Authorization*, the Minister states the following:

> Upon acquisition, if information is assessed to be necessary or essential, CSE may retain that information for a maximum of [redacted] from the date of assessment for the purpose of identifying, isolating, preventing, or mitigating harm to [redacted] electronic information or information infrastructure, federal systems or those of systems of importance to the GC. (emphasis added)

74. This [redacted] retention period can be found in the *Authorization*, in the *Application* and in CSE's *Mission Policy Suite - Cybersecurity*.

75. I have noted that the explanation provided for this [redacted] retention period is that this is done in accordance with the *Library and Archives of Canada Act*, SC 2004, c 11, and the *Privacy Act*, RSC, 1985, c P-21, requirements.

76. In the future, I would appreciate that specific details relating to these identified requirements be included. We must not forget that some of the information which will be held for [redacted] includes information for which a Canadian or a person in Canada may have a reasonable expectation of privacy.

iii. Solicitor-Client Communications

77. With regard to solicitor-client communications, CSE explains that upon recognition by an analyst, the information collected will be destroyed unless the Chief of CSE has reasonable ground to believe that the communication is essential to identify, isolate, prevent or mitigate harm to [redacted] electronic information or information infrastructure.

78. Before using, analysing, retaining or disclosing a solicitor-client communication, the Chief of CSE will advise the Minister and seek direction. Should the Chief determine that the solicitor-client communication meets this "essentiality test", the Chief will advise the Minister and seek her direction regarding its use, analysis, retention, and disclosure.

79. Furthermore, in cases where the Chief has reasonable grounds to believe that the failure to immediately use, analyse, retain, or disclose the solicitor-client communication will compromise the ability of CSE to mitigate an imminent threat to [redacted] electronic information or information infrastructures, the Chief is permitted to use, analyse, retain, or disclose the communication to the extent necessary to address the imminent threat. If such a situation arises, the Chief will advise the Minister, no later than 48 hours after such a determination is made.

80. In accordance with subsection 52(1) of the *CSE Act*, within 90 days after the last day of the period of validity of the *Authorization*, the Chief must provide the Minister with a written report on the outcomes of the activities carried out under the Authorization, including the number of recognized solicitor-client communications used, analysed, retained or disclosed. The Minister must provide the Intelligence Commissioner, and the National Security and Intelligence Review Agency, with a copy of the report.

81. I acknowledge that the Minister's office has been very diligent in providing my office with a copy of the report as soon as feasible when produced.

82. Notwithstanding this legislative requirement, we must not forget the privilege offered to solicitor-client communications, as highlighted by the Supreme Court of Canada in *Canada (National Revenue) v. Thompson*, 2016 SCC 21, at paragraph 17:

> [17] Solicitor-client privilege has evolved from being treated as a mere evidentiary rule to being considered a rule of substance and, now, a principle of fundamental justice (*Foster Wheeler Power Co. v. Société intermunicipale de gestion et d'élimination des déchets (SIGED) inc.*, 2004 SCC 18, [2004] 1 S.C.R. 456, at para. 34; Lavallée, Rackel & *Heintz v. Canada (Attorney General)*, 2002 SCC 61, [2002] 3 S.C.R.

> 209, at para. 49; *Maranda v. Richer*, 2003 SCC 67, [2003] 3 S.C.R. 193, at para. 11; *Solosky v. The Queen*, [1980] 1 S.C.R. 821, at p. 839; *Descoteaux v. Mierzwinski*, [1982] 1 S.C.R. 860, at p. 875; *Canada (Attorney General) v. Federation of Law Societies of Canada*, 2015 SCC 7, [2015] 1 S.C.R. 401, at paras. 8 and 84). The obligation of confidentiality that springs from the right to solicitor-client privilege is necessary for the preservation of a lawyer-client relationship that is based on trust, which in turn is
>
> > indispensable to the continued existence and effective operation of Canada's legal system. It ensures that clients are represented effectively and that the legal information required for that purpose can be communicated in a full and frank manner (*R. v. Gruenke*, [1991] 3 S.C.R. 263, at p. 289 ...).
>
> (*Foster Wheeler*, at para. 34)

83. Given the importance of solicitor-client communications, I would suggest that when CSE applies for the renewal of an existing Authorization, [redacted] that the number of recognized solicitor-client communications used, analysed, retained and disclosed, if any, be included in the Application to the Minister. This includes the number of solicitor-client communications which were collected and destroyed. If no solicitor-client communications were collected, I would expect to be advised of that as well.

84. I am sure that the inclusion of such information in the *Application* would be of interest to the Minister – who would have been consulted on the matter at the relevant time – as a reminder of the number of instances where solicitor-client communication was acquired and what became of such information.

85. Furthermore, its inclusion on the record would also assist me in answering any questions or concerns I may have with the potential acquisition and use of solicitor-client communication.

86. I am of the view that waiting up to 90 days after the expiration of the previous Authorization is simply not adequate keeping in mind that the solicitor-client privilege is of utmost importance being in itself a principle of fundamental justice.

iv. Other Acts of Parliament

87. My fourth remark relates to the conditions regarding the possibility that CSE may contravene other Acts of Parliament not listed in the *Application*.

88. In the *Authorization*, the Minister imposed a condition that if CSE knows beforehand that an activity – which must be within the scope of the activities outlined in the *Authorization* and described in the *Application* – may contravene other Acts of Parliament not listed in the *Application*, the Chief of CSE will notify the Minister, prior to the conduct of said activity and seek her approval before proceeding. Furthermore, should CSE learn that activities described in the *Application* inadvertently resulted in a contravention of an Act of Parliament not listed in the *Application*, the Chief of CSE will notify the Minister at the earliest opportunity.

89. Should such a situation occur, I would expect to be advised of any contravention of other Acts of Parliament not listed in a previous application, prior to issuing my reasons with respect to the renewal of an authorization. This would therefore require that any such contravention be in the materials before the Minister and on the record before me.

90. I have included the selected remarks to indicate the importance of including substantive information as part of the documentation submitted in support of the ministerial authorization. As said above, my role as Intelligence Commissioner is to assess whether or not the ministerial authorization is reasonable. In order to assume such a role, I need substantive information.

VII. CONCLUSIONS

91. 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 54 of the *Authorization*.

92. 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*.

93. 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.

94. 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.

November 14, 2022

(Original signed)

The Honourable Simon Noël, K.C.
Intelligence Commissioner