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-2022-01

IN THE MATTER OF AN APPLICATION BY THE COMMUNICATIONS SECURITY ESTABLISHMENT TO THE MINISTER OF NATIONAL DEFENCE FOR A CYBERSECURITY AUTHORIZATION FOR ACTIVITIES TO HELP PROTECT FEDERAL INFRASTRUCTURES PURSUANT TO SUBSECTION 27(1) OF THE *COMMUNICATIONS SECURITY ESTABLISHMENT ACT*

INTELLIGENCE COMMISSIONER DECISION AND REASONS

June 27, 2022

Canada

TABLE OF CONTENTS

I. Overview

On June 1, 2022, pursuant to subsection 27(1) of the *Communications Security Establishment Act*[1] (CSE Act), the Minister of National Defence (the Minister) issued a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures. On June 2, 2022, the Office of the Intelligence Commissioner received the Minister's authorization for my review and approval under the *Intelligence Commissioner* Act[2] (IC Act). In addition, the record received contained a cover letter from the Minister indicating that the following listed materials were all the materials before her when issuing the authorization: (1) *Authorization* – Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures; (2) *Application* – Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures, (i) Annex I – Ongoing Cybersecurity Activities; (ii) Annex II – S.45 MO – Ministerial Order Designating Recipients of Information Related to a Canadian or Person in Canada Acquired, Used, or Analyzed Under the Cybersecurity and Information Assurance Aspect of the CSE Mandate; (iii) Annex III – Outcomes from the Last MA Period; (iv) Annex IV – MND Notification Memo – MAPLETAP Deployment; (v) Annex V – CSE's Mission Policy Suite Cybersecurity; (3) Briefing Note to the Minister of National Defence – Cybersecurity Activities – Federal; (4) Cybersecurity Authorization – Overview Placemat; (5) Summary – Cybersecurity Activities – Federal; and (6) Record of Discussion with CSE Officials.

Based on the written application provided by the Chief of the Communications Security Establishment (Chief of CSE) pursuant to subsection 33(1) of the CSE Act, the Minister concluded, pursuant to subsection 33(2) of the CSE Act, that she had reasonable grounds to believe the Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures was necessary, and that the conditions set out in section 34 of the CSE Act for issuing it were met. The Minister also concluded that she had reasonable grounds to believe that the proposed cybersecurity activities are reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities, pursuant to subsection 34(1) of the CSE Act. The Minister also considered and concluded that she had reasonable grounds to believe the conditions set out in subsection 34(3) of the CSE Act were met.

Based on my review of the information provided, I am satisfied that the conclusions at issue are reasonable, with the exception of the conclusions relating to the activity aimed at the [redacted] for which I am not satisfied that they are reasonable.

Consequently, I must approve the Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures pursuant to paragraph 20(l)(*a*) of the IC Act, save for one activity. I do not approve the part of the Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures relating to the activity aimed at the [redacted] pursuant to paragraph 20(1)(*b*) of the IC Act.

[1] S.C. 2019, c. 13, s. 76.
[2] S.C. 2019, c. 13, s. 50.

II. Legislation

A. Role of the Minister

The CSE Act describes the five aspects of CSE's mandate, one of them being the cybersecurity and information assurance aspect, set out in section 17 of the CSE Act.

The Minister may, pursuant to subsection 27(1) of the CSE Act, issue a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures to CSE authorizing it to access a federal institution's information infrastructure and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(*e*) of the *Criminal Code* from mischief, unauthorized use, or disruption. In order to do so, the Minister must first receive a written application from the Chief of CSE.

The Minister, pursuant to section 34 of the CSE Act, must be able to draw conclusions on the following:

Conditions for authorizations

34 (1) *The Minister may issue an authorization under subsection 26(1), 27(1) or (2), 29(1) or 30(1) only if he or she concludes 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. (emphasis added)*

[...]

Conditions for authorizations – cybersecurity

(3) *The Minister may issue an authorization under subsection 27(1) or (2) only if he or she concludes that there are reasonable grounds to believe – in addition to the matters referred to in subsection (1) – that*

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

(b) *the consent of all persons whose information may be acquired could not reasonably be obtained, in the case of an authorization to be issued under subsection 27(1);*

(c) *any information acquired under the authorization is necessary to identify, isolate, prevent or mitigate harm to*

(i) federal institutions' electronic information or information infrastructures, in the case of an authorization to be issued under subsection 27(1), or

(ii) electronic information or information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada, in the case of an authorization to be issued under subsection 27(2); and

(d) *the measures referred to in section 24 will ensure that information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to identify, isolate, prevent or mitigate harm to*

(i) federal institutions' electronic information or information infrastructures, in the case of an authorization to be issued under subsection 27(1), or
(ii) electronic information or information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada, in the case of an authorization to be issued under subsection 27(2).

In order to issue a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures, the Minister must therefore have reasonable grounds to believe, based on the facts presented in the written application of the Chief of CSE, that the authorization is necessary and that the conditions for issuing it are met (subsection 33(2) of the CSE Act).

The Minister must conclude, in accordance with subsection 34(1) of the CSE Act, 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, and that the conditions of subsection 34(3) of the CSE Act have been met. In doing so, the Minister must explain her reasons for issuing the authorization. This is done in her conclusions.

B. Role of the Intelligence Commissioner

Pursuant to section 12 of the IC Act, the Intelligence Commissioner is responsible, as set out in sections 13 to 15, for reviewing the conclusions on the basis of which certain authorizations are issued under the CSE Act and, if satisfied that those conclusions are reasonable, approving those authorizations. In this instance, pursuant to section 14 of the IC Act, the Intelligence Commissioner must review whether the conclusions — made under subsections 34(1) and 34(3) of the CSE Act and on the basis of which a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures was issued by the Minister under subsection 27(1) of that Act — are reasonable.

This quasi-judicial review of the Intelligence Commissioner must be performed on the basis of all the information, or record, which was before the Minister. Subsection 23(1) of the IC Act requires that the person whose conclusions are being reviewed, the Minister of National Defence in this instance, must provide to the Intelligence Commissioner all the information that was before her when issuing the authorization.

It is noteworthy that it is the conclusions of the Minister that must be reviewed by the Intelligence Commissioner, as opposed to the authorization of the Minister. The quasi-judicial review regime of the IC Act aims to ensure that the Intelligence Commissioner is satisfied that the conclusions of the Minister, on the basis of which the authorization was issued, are reasonable.

i. The Applicable Concept of Reasonableness

Pursuant to sections 12 and 14 of the IC Act, the Intelligence Commissioner must review whether the Minister's conclusions are reasonable. I will refer to this as the concept of reasonableness.

The term "reasonable" is not defined in either the IC Act or the CSE Act. It is a term, however, that has been associated in jurisprudence with the process of judicial review of administrative decisions. 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" (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.

However, I accept 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. In that regard, the Intelligence Commissioner must be satisfied that the Minister's conclusions bear the essential elements of reasonableness: justification, transparency, intelligibility, and whether the are justified in relation to the relevant factual and legal contexts.[3]

Moreover, the concept of deference towards the decision-maker must be taken into account. In that regard, the legitimacy and authority of administrative decision-makers must be recognized and an appropriate posture of respect is to be adopted.[4]

[3] *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, at paragraph 99 [*Vavilov*] (citing *Dunsmuir v New Brunswick*, [2008] 1 SCR 190 at paragraphs 47 and 74; *Catalyst Paper Corp. v North Cowichan (District)*, [2012] 1 SCR 5 at paragraph 13).
[4] *Vavilov* at paragraph 14.

III. Analysis

A. The Reasonableness of the Minister's Conclusions

The Chief of CSE submitted a written application for a Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures. According to CSE, federal institutions' electronic information and information infrastructures referred to as "federal systems" are targeted by a range of sophisticated cyber threat actors, which may include cyber criminals and state-sponsored actors. Furthermore, cyber-related compromises are becoming increasingly difficult to detect, as threat actors have a multitude of entry points to infiltrate networks and the wide variety of devices used at the host, network or cloud level.[5] In order to help protect federal systems in this environment, CSE conducts the following three key activities to access and acquire information passing through the systems, devices and networks of the consenting federal institutions: host-based solutions (HBS), network-based solutions (NBS) and cloud-based solutions (CBS).[6]

The application indicates that in support of these three cybersecurity solutions, CSE also [redacted] and, according to CSE, would therefore require an authorization as per the requirements [redacted] of the CSE Act.[7]

The application describes the three activities as well as the access, acquisition, analysis and mitigation activities CSE undertakes when carrying out HBS, NBS and CBS. The application also describes how CSE analyses, uses, retains and discloses the information acquired by HBS, NBS and CBS and how these activities fulfill the objective of helping to protect federal systems.

Based on the facts presented in this application and generally in the record, the Minister reached conclusions on the basis of which she issued a cybersecurity authorization, as well as terms, conditions and restrictions, for activities to help protect federal systems.

With the exception of her conclusions on the basis of which she issued an authorization for the activity aimed at the [redacted] I am satisfied that the Minister's conclusions demonstrate 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 Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures was necessary, and that the conditions for issuing it were met. Particularly, I am satisfied that the Minister's conclusions are reasonable in determining that the described activities are reasonable and proportionate, with the exception of her conclusions

[5] *Application to the Minister of National Defence for Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures* dated May 26, 2022, at paragraph 13, p. 4.
[6] *Ibid* at paragraph 5, p. 3.
[7] *Ibid* at paragraph 2, pp. 1–2.

on the basis of which she issued an authorization for the [redacted] having regard to the nature of CSE's objective of helping to protect federal systems, and the nature of those cybersecurity activities. The remaining conclusions of the Minister serve as a basis for the authorization that she issued. In addition, those conclusions, save for those related to the exception, substantiate the issuance of the authorization, and they are justified, transparent and intelligible.

When assessing whether the activities are reasonable and proportionate, I am of the view that the 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 federal systems. 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.

The Minister's conclusions show that the Minister understood these notions, and applied them properly as it relates to the HBS, NBS and CBS. Furthermore, the Minister based her conclusions in this regard on the facts of the application and generally of the record, which were also clear. In her conclusions, the Minister demonstrates how the activities of acquiring information using the three cybersecurity solutions are reasonable and proportionate considering the nature of the objective to be achieved and the nature of the activities.[8] It has therefore been established to my satisfaction that the conclusions of the Minister are reasonable with respect to the activities of accessing the federal systems and of acquiring information using the three proposed cybersecurity solutions.

I will now be addressing below the Minister's conclusions as they relate to the [redacted]

i. [redacted]

At paragraph 47(c) of the authorization, the Minister authorized the activity aimed at the [redacted][9] I must therefore review the conclusions of the Minister that led to the issuance of that authorized activity and determine whether these conclusions contain the following elements of reasonableness: justification, transparency, intelligibility, and whether they are justified in relation to the relevant factual and legal contexts.

[8] *Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures* dated June 1, 2022, paragraphs 1–46, pp. 1–9.
[9] *Ibid* at paragraph 47(c), p. 9.

Paragraph 3 of the Chief of CSE's application provides:

> *By deploying its cybersecurity solutions on federal infrastructures, there is a risk that CSE may contravene other Acts of Parliament. Through its cybersecurity solutions* [redacted] *In accordance with* [redacted] *and subsection 27(1) of the CSE Act, you, as Minister of National Defence, may issue an Authorization that authorizes CSE, despite any other Act of Parliament, to access a federal system and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure* ...[10] (emphasis added)

While the Chief of CSE requires an authorization pursuant to subsection 27(1) of the CSE Act for the [redacted] she only refers, in the above passage, to accessing a federal system and acquiring information originating from, directed to, stored on or being transmitted on or through that infrastructure. There is no supporting information, or specific rationale, establishing how the activity of [redacted] falls under the subsection 27(1) regime.

When questioned by the Minister during a briefing that was held on May 31, 2022,[11] the Chief of CSE reiterated that some of [redacted] Again, the Chief of CSE offered no supporting information, nor provided a specific rationale to the Minister in the course of that briefing with respect to the use of subsection 27(1) in that regard.

The application discusses the importance of [redacted] including at paragraphs 101, 108, 110(c), 110(d), 112 and 117.[12] The Minister also discusses at length the importance of [redacted] in her conclusions, including at paragraphs 5, 12, 16, 17, 20(j), and 28 of the authorization.[13]

The Minister also discusses the fact that [redacted] but falls short, in her conclusions, of referring to [redacted] of the CSE Act and of discussing the need for an authorization under subsection 27(1) of the CSE Act.

There are three different sections of the CSE Act that are relevant for my review.

1) Section 17 of the CSE Act provides for the cybersecurity and information assurance mandate of the CSE. Paragraph (b) states the following: acquire, use and analyze information from the GII or from other sources in order to provide

[10] *Supra* note 5, paragraph 3, p. 2.
[11] *Record of Discussion with CSE officials, MND Briefing – May 31, 2022: Application for Cybersecurity Authorization for Activities on Federal Infrastructures (2022-23)*, p. l.
[12] *Supra* note 5, pp. 20–24.
[13] *Supra* note 8, pp. 1–6.

such advice, guidance and services.

2) [redacted]

3) Subsection 27(1) refers to an authorization to access a federal institution's information infrastructure and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure.

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

In fact, there is a lack of information in the Minister's conclusions and in the record on how the authorized activity aimed at the [redacted] is covered by subsection 27(1). Indeed, the latter notion of [redacted] covers a much wider ambit than the notion of federal institution's information infrastructures found in the above provision.

In light of the above, I am of the view that the Minister's conclusions do not bear the essential elements of reasonableness: justification, transparency, intelligibility, and whether the authorized activity is justified in relation to the relevant factual and legal contexts.[14]

Having determined that I am not satisfied that the Minister's conclusions in respect of the activity aimed at the [redacted] are reasonable, paragraph 20(1)(*b*) of the IC Act provides that I must not approve the authorization and set out my reasons for doing so. I have already provided my reasons above.

I must now determine whether my decision affects the authorization as a whole, or solely the portion of the ministerial authorization with respect to the activity aimed at the [redacted] I am of the opinion that the latter applies.

The authorization can be comprised of more than one activity, and it is usually the case. Section 35 of the CSE Act does provide that an authorization issued under subsection 27(1) must specify (a) the activities or classes of activities that it authorizes CSE to carry out.

[14] *Supra* note 3.

Subsection 34(1) of the CSE Act provides that the Minister may issue an authorization if she concludes that there are reasonable grounds to believe that any activity that would be authorized by it is reasonable and proportionate. The French version indicates "s'il conclut qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle." (emphasis added)

Therefore, the test that must be exercised by the Minister under subsection 34(1) must apply to each activity to be authorized.

Paragraph 20(1)(*a*) of the IC Act provides that after his review, the Intelligence Commissioner must approve the authorization if he is satisfied that the conclusions at issue are reasonable. The French version states "s'il est convaincu que les conclusions en cause sont raisonnables." Paragraph 20(1)(*b*) covers those situations where the Intelligence Commissioner is not so satisfied. (emphasis added)

The analysis of the above provisions from both the IC Act and the CSE Act leads me to conclude that the Intelligence Commissioner must determine whether the conclusions at issue for each and every activity that is being requested by the applicant are reasonable, in the same manner that the Minister must determine whether she can conclude that each and every activity is reasonable and proportionate.

I am also of the view that Parliament could not have intended, for the legislative scheme in question, to support the untenable position that the authorization as a whole, covering a number of activities, should not be approved when the conclusions concerning a particular activity are found to not be reasonable.

Based on my analysis, I am of the view that in my role of having to ultimately determine whether to approve or not approve the authorization, I am legally entitled to determine that I am not satisfied that the ministerial conclusions at issue, on the basis of which the activity aimed at the [redacted] are reasonable.[15] Consequently, I do not approve the authorization regarding this activity.

B. Response to Remarks Made in the 2021 Intelligence Commissioner Decision

In my decision of last year dated July 13, 2021, I made remarks with respect to the record received.[16] I note that this year's record responds to those remarks.

[15] *Supra* note 3.

[16] *Intelligence Commissioner Decision and Reasons*, "In the Matter of an Application by the Communications Security Establishment to the Minister of National Defence for a Cybersecurity Authorization for Activities on Federal Infrastructures Pursuant to Subsection 27(1) of the *Communications Security Establishment Act*," dated July 13, 2021, File: 2200-B-2021-01, pp. 9–11.

IV. Conclusion

Based on my review of the record submitted, I am satisfied that the ministerial conclusions are reasonable, with the exception of those with respect to the activity aimed at the [redacted] Consequently, I must approve the Minister's Cybersecurity Authorization for Activities to Help Protect Federal Infrastructures, dated June 1, 2022, pursuant to paragraph 20(1)(*a*) of the *Intelligence Commissioner Act*, save for one activity. I do not approve the part of the Cybersecurity Authorization for Activities to Help Protect on Federal Infrastructures relating to the activity aimed at the [redacted] pursuant to paragraph 20(1)(*b*) of the *Intelligence Commissioner Act*.

(Original signed)
The Honourable Jean-Pierre Plouffe, C.D.
Intelligence Commissioner

June 27, 2022
Date