~~SECRET//CEO~~

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-2021-05

IN THE MATTER OF AN APPLICATION BY THE COMMUNICATIONS SECURITY ESTABLISHMENT TO THE MINISTER OF NATIONAL DEFENCE FOR AN AUTHORIZATION FOR CYBERSECURITY ACTIVITIES ON NON-FEDERAL INFRASTRUCTURES – PURSUANT TO SUBSECTION 27(2) OF THE *COMMUNICATIONS SECURITY ESTABLISHMENT ACT*

INTELLIGENCE COMMISSIONER DECISION AND REASONS

November 18, 2021

Canada

TABLE OF CONTENTS

I. Overview 3
II. Legislation 4
A. Role of the Minister 4
B. Role of the Intelligence Commissioner 4
i. The Applicable Concept of Reasonableness 5
III. Analysis 5
A. The Reasonableness of the Minister's Conclusions 5
IV. Conclusion 8

I. Overview

On [redacted] pursuant to subsection 27(2) of the *Communications Security Establishment Act*[1] (CSE Act), the Minister of National Defence issued an authorization for Cybersecurity Activities on Non-Federal Infrastructures in relation to [redacted]. That same evening, 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 dated [redacted], indicating that pursuant to "section 23 of the *Intelligence Commissioner Act*, I confirm that the materials listed above were all the materials before me when issuing the Authorization."[3] The listed materials included the written application from the Chief of CSE dated [redacted], which included four annexes: (1) the Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada dated August 25, 2020; (2) 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 dated August 13, 2021; (3) the letter of request [redacted]; and, (4) CSE's Mission Policy Suite Cybersecurity approved on October 2, 2020. The material provided also included a deck presentation entitled "Cybersecurity Activities on Non-Federal Infrastructures – [redacted], and a written record of discussion between the Minister, her staff and CSE officials entitled "MND Briefing – [redacted]".

Based on the written application provided by the 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 authorization for Cybersecurity Activities on Non-Federal Infrastructures in relation to [redacted] was necessary, and that the conditions set out in section 34 of the CSE Act for issuing it were met. The Minister issued conclusions demonstrating she had reasonable grounds to believe that the proposed cybersecurity activities are reasonable and proportionate, having regard to the nature of the objective 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 that the conditions set out in subsection 34(3) of the CSE Act were met.

Based on a review of the information provided to me, I am satisfied that the conclusions at issue are reasonable. Consequently, I must approve the authorization for Cybersecurity Activities on Non-Federal Infrastructures in relation to [redacted] pursuant to paragraph 20(1)(*a*) of the IC Act.

---

[1] S.C. 2019, c. 13, s. 76.
[2] S.C. 2019, c. 13, s. 50.
[3] Cover letter from the Minister of National Defence to the Intelligence Commissioner dated [redacted], page 2.

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(2) of the CSE Act, issue an authorization for Cybersecurity Activities on Non-Federal Infrastructures authorizing CSE to access an information infrastructure designated under subsection 21(1) as being of importance to the Government of Canada 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 which must include a written request from the owner or operator of the information infrastructure.

In order to issue an authorization for Cybersecurity Activities on Non-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 also 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 arriving at the decision.

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 on Non-Federal Infrastructures was issued by the Minister under subsection 27(2) 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 they are justified in relation to the relevant factual and legal contexts.[4]

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.[5]

III. Analysis

A. The Reasonableness of the Minister's Conclusions

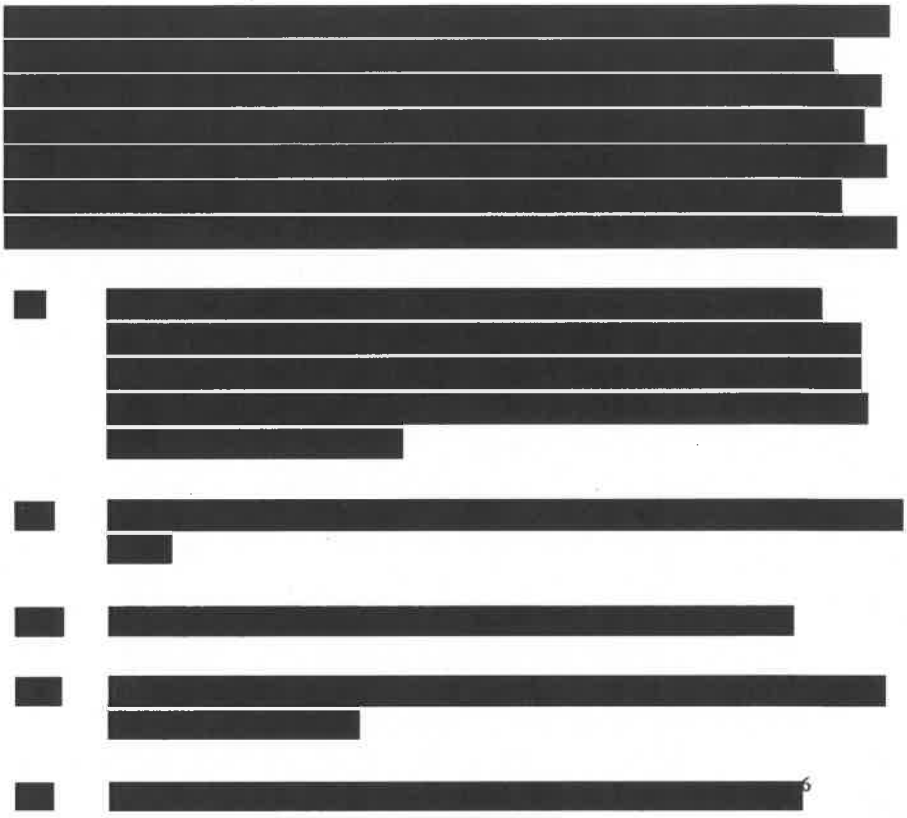
The Chief of CSE submitted a written application for an authorization for Cybersecurity Activities on Non-Federal Infrastructures in relation to [redacted]. The CSE application describes

---

[4] *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).

[5] *Vavilov* at paragraph 14.

[redacted] as follows:



The CSE application indicates that "[s]ince [redacted]"[7]

The application states that CSE was first notified [redacted] that they had been a [redacted]. During direct engagements with [redacted], CSE indicates that it was provided the identity of the threat actor as the [redacted][8] [redacted]"[9]

---

[6] *CSE Application to the Minister of National Defence for Cybersecurity Activities on Non-Federal Infrastructure* – [redacted] dated [redacted] at paragraph 13, page 4.
[7] *Ibid* at paragraph 14, page 4.
[8] *Ibid* at paragraph 16, page 5.
[9] *Ibid* at paragraph 17, page 5.

CSE has determined that [redacted][10]

In accordance with subsection 33(3) of the CSE Act, [redacted], by letter dated [redacted], requested that CSE conduct cyber defence activities to assist in the protection of the electronic information and information infrastructures under the control and supervision of [redacted], including mitigating the cyber threat.[11]

The application explains the rationale for the [redacted], the objectives to be achieved, the supporting activities (analysis and retention of information) and 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.

In her authorization, the Minister determined that [redacted] is a non-federal infrastructure that falls under the [redacted] pursuant to the Ministerial Order Designating Electronic Information and Information Infrastructure of Importance to the Government of Canada issued on August 25, 2020.[12]

Based on the facts presented in the CSE application, the Minister reached conclusions on the basis of which she issued an authorization, as well as terms, conditions and restrictions, for Cybersecurity Activities on Non-Federal Infrastructures in relation to [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 on Non-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, 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. The conclusions of the Minister serve as a basis for the authorization that she issued. In addition, those conclusions substantiate the issuance of the authorization, and they are justified, transparent and intelligible. [13]

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

---

[10] *Ibid* at paragraphs 20-21, page 5.
[11] Annex III of the application: letter of request from [redacted] to CSE (Canadian Centre for Cyber Security) dated [redacted], page 1.
[12] *CSE Cybersecurity Authorization for Activities on Non-Federal Infrastructures* – [redacted] dated [redacted], paragraph 6, page 2 and annex I to the application.
[13] *Ibid* at paragraphs 1 to 43, pages 1 to 8.

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.

The Minister's conclusions show that the Minister understood these notions, and applied them properly. Furthermore, the Minister based her conclusions on the facts of the application and generally of the record, which were also clear. In her conclusions, the Minister demonstrates how the acquisition of information obtained from the cybersecurity activities is reasonable and proportionate. It has therefore been established to my satisfaction that the conclusions of the Minister are reasonable with respect to accessing [redacted] systems and the acquisition of information obtained from the [redacted] considering the nature of the objective to be achieved and the nature of the activities.

IV. Conclusion

Based on my review of the record submitted, I am satisfied that the conclusions of the Minister are reasonable. I therefore must approve the Minister's authorization for Cybersecurity Activities on Non-Federal Infrastructures in relation to [redacted], dated [redacted], pursuant to paragraph 20(1)(*a*) of the *Intelligence Commissioner Act*.

The Honourable Jean-Pierre Plouffe, CD
Intelligence Commissioner

November 18, 2021.
Date