~~TOP SECRET//SI//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-2021-01

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*

INTELLIGENCE COMMISSIONER DECISION AND REASONS

July 13, 2021

Canada

TABLE OF CONTENTS

I. Overview

On June 18, 2021, 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 on Federal Infrastructures. On June 21, 2021, 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 him when issuing the authorization: (1) Cybersecurity Authorization for Activities for [*sic*] Federal Infrastructure *Application*; (2) Cybersecurity Authorization for Activities of Federal Infrastructure, (3) Annex I – Ongoing Cybersecurity Activities; (4) Annex II – CSE's Mission Policy Suite Cybersecurity; and (5) Record of Discussion with CSE officials. However, the materials provided to me also included a document, which was not listed in the cover letter, entitled "Cybersecurity Authorization Overview for the Intelligence Commissioner – Activities on Federal Infrastructures 2021-2022". I will discuss that document later.

Based on the written application provided by the Chief of the Communications Security Establishment (CSE) pursuant to subsection 33(1) of the CSE Act, the Minister concluded, pursuant to subsection 33(2) of the CSE Act, that he had reasonable grounds to believe the Cybersecurity Authorization for Activities on Federal Infrastructures 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 he 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 he 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. Consequently, I must approve the Cybersecurity Authorization for Activities on Federal Infrastructures pursuant to paragraph 20(1)(*a*) of the IC Act.

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 on 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

---

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

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

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 on 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 his reasons for issuing the authorization. This is done in his 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 on 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 him 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.[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]

III. Analysis

A. The Reasonableness of the Minister's Conclusions

The Chief of CSE submitted a written application for a Cybersecurity Authorization for Activities on Federal Infrastructures. According to CSE, federal institutions' electronic information and information infrastructures ("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 on those networks.[5] In order to help protect federal systems in this environment, CSE conducts three key activities to access and acquire information passing through the systems, devices and networks of the consenting federal institutions. These three activities are host-based solutions (HBS), network-based solutions (NBS) and cloud-based solutions (CBS).[6]

---

[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.

[5] Application to the Minister of National Defence for Cybersecurity Authorization for Activities on Federal Infrastructures dated June 16, 2021, at paragraphs 11 and 77, pp. 3 and 17.

[6] *Ibid*, paragraph 5, p. 3.

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 electronic information and information infrastructures.

Based on the facts presented in this application and generally in the record, the Minister reached conclusions on the basis of which he issued an authorization, as well as terms, conditions and restrictions, for cybersecurity activities on federal infrastructures.

I am satisfied that the Minister's conclusions demonstrate that he 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 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 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 he issued. In addition, those conclusions 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 electronic information and information infrastructures. 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 his conclusions on the facts of the application and generally of the record, which were also clear. In his conclusions, the Minister demonstrates how the acquisition of information obtained from the three cybersecurity activities is reasonable and proportionate.[7] It has therefore been established to my satisfaction that the conclusions of the Minister are reasonable with respect to accessing the federal systems and the acquisition of information obtained from the three proposed cybersecurity activities considering the nature of the objective to be achieved and the nature of the activities.

[7] Cybersecurity Authorization to the Communications Security Establishment for Activities on Federal Infrastructures dated June 18, 2021, paragraphs 1 to 47, pp. 1 to 8.

B. Response to Remarks Made in the 2020 Intelligence Commissioner Decision

In my decision of last year dated July 30, 2020, I made remarks with respect to the record received.[8] I note that this year's record satisfactorily responds to most of those remarks.

At page 9 of my 2020 decision, I noted that annex 1 of the application listed the federal institutions with which CSE was engaged in ongoing cybersecurity activities that risked interfering with the reasonable expectation of privacy of a Canadian or person in Canada. I also indicated that neither the application nor the annex specified which cyber solutions each institution was receiving. I note that this year's annex does include a list of the federal institutions, as well as which of the cyber solutions (HBS, NBS and/or CBS) they are receiving from CSE.[9]

At pages 9 and 10 of my 2020 decision, I noted that while CSE undertook CBS activities, it was still developing its related mitigation capabilities. The Minister had authorized CSE to conduct mitigation actions; however, he had not imposed any condition that he be advised when such new activities would be deployed. I indicated that the Minister should be informed when those mitigation activities are deployed during the authorization period, as this would provide the Minister with the opportunity to determine if the deployed activities conformed to the activities described in the application. I note that the Minister imposed a condition on the Chief of CSE to advise him when the new CBS capabilities under development have been deployed, and to which federal institution they apply.[10]

I noted at page 10 of my 2020 decision that there was no condition in the Minister's authorization to be advised if there was a contravention of any other Acts of Parliament. I indicated that ministerial authorizations serve an important purpose, which is to preclude civil or criminal liability from authorized activities, and that if CSE contravened other Acts of Parliament not listed in the Chief's application, the Minister should be informed. In this year's authorization, the Minister imposed a condition to be advised at the earliest opportunity by the Chief if CSE contravenes an Act of Parliament not listed in the application.[11] It should also be noted that the application also includes an additional provision of an Act of Parliament which could be contravened – [redacted][12]

At pages 8 and 9 of my 2020 decision, I noted that the 2019 application included an annex describing the outcomes achieved under the previous year's ministerial authorization period, prior to the coming into force of the CSE Act. This annex enabled the Minister to consider these outcomes when determining whether the cybersecurity activities were necessary and ultimately

---

[8] 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*" ("2020 decision"), July 30, 2020, File: 2200-B-2020-01, pp. 8 to 10.

[9] Annex I to the application – "Ongoing Cybersecurity Services".

[10] *Supra*, note 7, paragraph 67, p. 11.

[11] *Supra*, note 7, paragraph 65, p. 11.

[12] *Supra*, note 5, paragraph 74, p. 16.

decide whether or not to authorize them. I indicated that the 2020 application did not include such an annex and that some examples regarding the use of HBS, NBS and CBS were outdated and repetitive from the 2019 application. In this year's application, no annex indicating the outcomes was included, although examples of outcomes achieved for each activity – [redacted] for HBS, [redacted] for NBS and [redacted] for CBS – were specified.

Finally, last year I added the following remarks at page 9 of my decision:

> *Subsection 33(2) of the CSE Act requires that the Chief of CSE's application set out "the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary [...]." [emphasis added] Arguably, establishing the necessity of a particular activity to be authorized can be based on explaining, in theory, what the proposed activity can achieve with respect to the ultimate goal or purpose of the initiative.*
>
> *However, I am of the view that basing applications solely or primarily on the theory behind a proposed activity, without specifically recognizing where the activity is deployed in practice, may not meet the above noted legal standard. Achieved outcomes and examples contribute to establishing the necessity of the activities to be authorized, fosters transparency, and supports the Minister in his decision making."*
> (emphasis added)

Although this year's application contains some achieved outcomes and specific examples relating to HBS, NBS and CBS, I will further address this matter in my remarks below.

IV. Remarks

I am satisfied that the Minister's conclusions are reasonable. However, I would like to express my opinion on some aspects of CSE's application and the Minister's authorization to inform future applications and authorizations.

A. CSE Application

In terms of providing achieved outcomes, including figures and empirical data, I note that this year's application could have provided additional outcomes to the Minister in support of the request to authorize the deployment of HBS, NBS and CBS to protect federal systems. I am of the view that such additional information would assist in bolstering the Minister's conclusions with respect to the legal standard of the necessity of the authorization and whether the proposed activities are reasonable and proportional.

The current application does include the following data and examples:

- Over [redacted] deployed to various endpoints (paragraph 20);

- HBS – example of the [redacted] (paragraph 31), [redacted] (paragraph 32);
- NBS – example of [redacted] (paragraph 42); collection of [redacted] (paragraph 44); and
- CBS – example of [redacted] (March 26, 2021) (paragraph 56).

Notwithstanding the information provided, I reiterate that the inclusion of updated achieved outcomes, including figures and empirical data, in an annex to the application – as was done in the 2019 record – would better support the facts and statements made in the application, which in turn would bolster the Minister's conclusions that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it, as set out in subsections 34(1) and (3) of the CSE Act, are met.[13]

B. Ministerial Authorization

Subsection 23(1) of the IC Act states that "the person whose conclusions are being reviewed by the Commissioner under any of sections 13 to 19 must, for the purposes of the Commissioner's review, provide the Commissioner with all information that was before the person in issuing … the authorization …".

I note that the cover letter accompanying the record that was provided to me by the Minister listed five documents that were before him, but did not list the document or deck entitled "Cybersecurity Authorization Overview for the Intelligence Commissioner – Activities on Federal Infrastructures 2021-2022". Based on the cover letter received, it would appear that the deck was not provided to the Minister and as such could not be considered as part of the information before the Minister. That being said, in reviewing the document entitled "Record of Discussion with CSE Officials", listed as item 5 of the record, I note that it indicates the following:

> *DC SIGINT provided an update to the Minister on this year's application in line with the provided deck, specifically noting the similarity to the previous year's application, outlining CSE's changes relating to comments raised by the Intelligence Commissioner, noting the relevant examples of success, and noting the rational [sic] for delayed CBS capabilities. The Minister was assured that Chief, CSE would advise the Minister when new CBS capabilities were deployed. The Minister was satisfied with the briefing, reviewed the associated documents, and approved the authorization.* (emphasis added)

Although the deck was not specifically listed in the Minister's cover letter, I have concluded that it was part of the materials before him as there is a reference to it in the above-noted "Record of Discussion with CSE Officials". The words "provided deck" and the contents of that document

[13] File: 2200-B-2019-002, Annex I – Outcomes from last MA period.

refer to the contents of the deck. To avoid any confusion in the future and to fulfil his statutory obligation under subsection 23(1) of the IC Act, it is imperative for the Minister to list in his cover letter all the materials that were before him.

Furthermore, I note that the authorization refers to a Ministerial Order (MO) issued on August 25, 2020.[14] This MO was not included in the present record submitted to the Intelligence Commissioner as it should have been. However, I note that this MO was included in the record received on July 21, 2021, regarding the Foreign Intelligence Authorization for Passive Access Activities issues by the Minister of June 18, 2021.

V. Conclusion

Based on my review of the record submitted, I am satisfied that the ministerial conclusions are reasonable. I therefore must approve the Minister's Cybersecurity Authorization for Activities on Federal Infrastructures, dated June 18, 2021, pursuant to paragraph 20(1)(*a*) of the *Intelligence Commissioner Act*.

The Honourable Jean-Pierre Plouffe, C.D.
Intelligence Commissioner

July 13th, 2021.
Date

[14] *Supra*, note 7, paragraph 56, p. 9.