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

~~TRÈS SECRET//SI//RAC~~

DOSSIER : 2200-B-2022-01

AFFAIRE INTÉRESSANT UNE DEMANDE PRÉSENTÉE PAR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS À LA MINISTRE DE LA DÉFENSE NATIONALE AU SUJET D'UNE AUTORISATION DE CYBERSÉCURITÉ CONCERNANT DES ACTIVITÉS MENÉES AFIN D'AIDER À PROTÉGER DES INFRASTRUCTURES FÉDÉRALES EN VERTU DU PARAGRAPHE 27(1) DE LA *LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS*

COMMISSAIRE AU RENSEIGNEMENT
DÉCISION ET MOTIFS

Le 27 juin 2022

Canada

TABLE DES MATIÈRES

I. Aperçu

Le 1er juin 2022, la ministre de la Défense nationale (la ministre) a délivré une autorisation de cybersécurité en vertu du paragraphe 27(1) de la *Loi sur le Centre de la sécurité des télécommunications*[1] (la Loi sur le CST) concernant des activités menées afin d'aider à protéger des infrastructures fédérales. Le 2 juin 2022, la ministre a fourni l'autorisation au Bureau du commissaire au renseignement aux fins de mon examen et approbation conformément à la *Loi sur le commissaire au renseignement*[2] (la Loi sur le CR). En outre, le dossier comprenait une lettre de présentation de la ministre indiquant qu'elle disposait des documents suivants lorsqu'elle a délivré l'autorisation : 1) *Autorisation* – autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales; 2) *Demande* – demande d'autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales, (i) annexe I – Activités de cybersécurité en cours; (ii) annexe II – Article 45 – Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu d'une autorisation ministérielle de renseignement étranger; (iii) annexe III – Résultats obtenus lors de la dernière période d'AM; (iv) annexe IV – Avis du MDN concernant le déploiement de MapleTap; (v) annexe V – Ensemble des politiques du CST sur la mission en matière de cybersécurité; 3) Note de synthèse à l'intention de la ministre de la Défense nationale – Activités de cybersécurité dans des institutions fédérales; 4) Autorisation de cybersécurité – Napperon de l'aperçu; 5) Résumé – Activités de cybersécurité dans des institutions fédérales; 6) Compte rendu des discussions avec les responsables du CST.

Compte tenu de la demande écrite présentée par la chef du Centre de la sécurité des télécommunications (la chef du CST) conformément au paragraphe 33(1) de la Loi sur le CST, la ministre a conclu, aux termes du paragraphe 33(2) de cette même loi, qu'elle avait des motifs raisonnables de croire que l'autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales était nécessaire et que les conditions énoncées à l'article 34 de la Loi sur le CST étaient remplies. La ministre a conclu également qu'elle avait des motifs raisonnables de croire que les activités de cybersécurité proposées étaient raisonnables et proportionnelles compte tenu de la nature de l'objectif à atteindre et des activités, conformément au paragraphe 34(1) de la Loi sur le CST. La ministre a également examiné les conditions énoncées au paragraphe 34(3) de la Loi sur le CST et a conclu qu'elle avait des motifs raisonnables de croire que ces conditions étaient remplies.

À la lumière de mon examen des renseignements présentés, je suis convaincu que les conclusions en cause sont raisonnables, sauf celles qui concernent l'activité visant [redacted] pour lesquels je ne suis pas convaincu qu'elles soient raisonnables.

Par conséquent, je dois approuver l'autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales conformément à l'alinéa 20(1)*a*) de la Loi sur le CR, à l'exception d'une activité. Je n'approuve pas le volet de l'autorisation de

[1] LC 2019, c 13, art 76.
[2] LC 2019, c 13, art 50.

cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales qui a trait à l'activité visant [redacted], conformément à l'alinéa 20(1)*b*) de la Loi sur le CR.

II. Législation

A. Rôle de la ministre

La Loi sur le CST décrit les cinq volets du mandat du CST, notamment celui qui touche la cybersécurité et l'assurance de l'information, dont il est question à l'article 17 de la Loi sur le CST.

La ministre peut, en vertu du paragraphe 27(1) de la Loi sur le CST, délivrer une autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales qui permet au CST d'accéder à l'infrastructure de l'information d'une institution fédérale et d'acquérir de l'information qui provient de cette infrastructure ou passe par elle, qui y est destinée ou y est stockée afin d'aider à protéger cette infrastructure, dans les cas visés à l'alinéa 184(2)*e*) du *Code criminel*, contre tout méfait, toute utilisation non autorisée ou toute perturbation de son fonctionnement. Pour ce faire, la ministre doit d'abord recevoir une demande écrite de la chef du CST.

Conformément à l'article 34 de la Loi sur le CST, la ministre doit être en mesure de tirer des conclusions sur les éléments suivants :

> ***Conditions des autorisations***
>
> ***34 (1)*** *[La] ministre ne peut délivrer l'autorisation visée aux paragraphes 26(1), 27(1) ou (2), 29(1) ou 30(1) que [si elle] conclut qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités. (Non souligné dans l'original.)*
>
> *[...]*
>
> ***Conditions : autorisation de cybersécurité***
>
> ***(3)*** *[La] ministre ne peut délivrer l'autorisation visée aux paragraphes 27(1) ou (2) que [si elle] conclut qu'il y a des motifs raisonnables de croire, outre ce qui est prévu au paragraphe (1) :*
>
> **a)** *que l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire;*

b) *dans le cas de l'autorisation visée au paragraphe 27(1), que le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu;*

c) *que l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages :*

(i) aux informations électroniques ou aux infrastructures de l'information des institutions fédérales, dans le cas de l'autorisation visée au paragraphe 27(1),

(ii) aux informations électroniques ou aux infrastructures de l'information désignées comme étant d'importance pour le gouvernement fédéral en vertu du paragraphe 21(1), dans le cas de l'autorisation visée au paragraphe 27(2);

d) *que les mesures visées à l'article 24 permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages :*

(i) aux informations électroniques ou aux infrastructures de l'information des institutions fédérales, dans le cas de l'autorisation visée au paragraphe 27(1),

(ii) aux informations électroniques ou aux infrastructures de l'information désignées comme étant d'importance pour le gouvernement fédéral en vertu du paragraphe 21(1), dans le cas de l'autorisation visée au paragraphe 27(2).

Pour délivrer une autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales, la ministre doit donc avoir des motifs raisonnables de croire, compte tenu des faits présentés dans la demande écrite de la chef du CST, que l'autorisation est nécessaire et que les conditions de sa délivrance sont remplies (paragraphe 33(2) de la Loi sur le CST).

Conformément au paragraphe 34(1) de la Loi sur le CST, la ministre doit également conclure qu'il existe des motifs raisonnables de croire que l'activité proposée en cause est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités, et que les conditions énoncées au paragraphe 34(3) de la Loi sur le CST sont remplies. Ce faisant, la ministre doit expliquer les motifs qui l'ont amené à délivrer l'autorisation. C'est ce qu'elle fait dans ses conclusions.

B. Rôle du commissaire au renseignement

Conformément à l'article 12 de la Loi sur le CR, le commissaire au renseignement est chargé, aux termes des articles 13 à 15, d'examiner les conclusions sur lesquelles reposent certaines autorisations accordées au titre de la Loi sur le CST et, s'il est convaincu que ces conclusions sont raisonnables, d'approuver ces autorisations. En l'espèce, conformément à l'article 14 de la Loi sur le CR, le commissaire au renseignement doit examiner si les conclusions formulées au titre des paragraphes 34(1) et 34(3) de la Loi sur le CST, et sur lesquelles repose l'autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales que la ministre a délivrée en vertu du paragraphe 27(1) de cette loi, sont raisonnables.

L'examen quasi judiciaire du commissaire au renseignement doit être effectué sur le fondement de tous les renseignements ou du dossier, dont disposait la ministre. Le paragraphe 23(1) de la Loi sur le CR requiert que la personne ayant formulé les conclusions qui font l'objet de l'examen, à savoir la ministre de la Défense nationale en l'espèce, fournisse au commissaire au renseignement tous les renseignements dont elle disposait au moment de délivrer l'autorisation.

Il convient de souligner que ce sont les conclusions de la ministre, et non son autorisation, que le commissaire au renseignement doit examiner. Le régime d'examen quasi judiciaire prévu par la Loi sur le CR vise à garantir que le commissaire au renseignement est convaincu que les conclusions de la ministre, sur lesquelles repose l'autorisation qui a été délivrée, sont raisonnables.

i. Concept applicable du caractère raisonnable

Conformément aux articles 12 et 14 de la Loi sur le CR, le commissaire au renseignement doit examiner si les conclusions de la ministre sont raisonnables. Je rattacherai ce processus au concept du caractère raisonnable.

Le terme « raisonnable » n'est pas défini dans la Loi sur le CR ni dans la Loi sur le CST. Toutefois, il est associé, dans la jurisprudence, au processus de contrôle judiciaire des décisions administratives. L'examen mené par le commissaire au renseignement ne constitue pas un contrôle judiciaire en tant que tel, puisque le commissaire n'est pas une cour de justice, même s'il doit être un « juge à la retraite d'une juridiction supérieure » (paragraphe 4(1) de la Loi sur le CR). Le commissaire au renseignement est plutôt chargé d'effectuer un examen quasi judiciaire des conclusions du décideur administratif, qui est la ministre.

Je suis cependant d'avis que, lorsque le législateur a employé le terme « raisonnable » dans le contexte de l'examen quasi judiciaire de décisions administratives par un juge à la retraite d'une juridiction supérieure, il entendait lui donner le même sens que dans la jurisprudence en droit administratif. À cet égard, le commissaire au renseignement doit être convaincu que les conclusions de la ministre possèdent les caractéristiques essentielles d'une décision raisonnable,

soit la justification, la transparence et l'intelligibilité, et qu'elles sont justifiées au regard des contraintes factuelles et juridiques pertinentes[3].

De plus, il faut tenir compte du principe de la déférence envers le décideur. À cet égard, il convient de reconnaître la légitimité et la compétence des décideurs administratifs et d'adopter une attitude de respect[4].

III. Analysis

A. Caractère raisonnable des conclusions de la ministre

La chef du CST a présenté une demande écrite en vue d'obtenir une autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales. Selon le CST, l'information électronique et les infrastructures de l'information des institutions fédérales (les systèmes fédéraux) sont ciblées par divers auteurs de cybermenaces sophistiqués, notamment des cybercriminels et des acteurs parrainés par l'État. Par ailleurs, les atteintes à la cybersécurité sont de plus en plus difficiles à détecter, puisque les auteurs de menaces disposent de multiples points d'entrée pour infiltrer les réseaux et le vaste éventail d'appareils que ceux-ci utilisent aux niveaux de l'hôte, des réseaux ou du nuage[5]. Dans ce contexte, afin d'aider à protéger les systèmes fédéraux, le CST mène les trois activités clés suivantes, qui lui permettent d'accéder aux renseignements qui transitent par les systèmes, appareils et réseaux des institutions fédérales consentantes, et de les acquérir : ce sont les solutions au niveau de l'hôte, les solutions axées sur les réseaux et les solutions infonuagiques[6].

Il est précisé dans la demande que, à l'appui de ces trois solutions de cybersécurité, le CST doit également [redacted] et, selon le CST, il est donc nécessaire d'obtenir une autorisation conformément aux exigences de [redacted] de la Loi sur le CST[7].

La demande décrit les trois activités ainsi que les activités d'accès, d'acquisition, d'analyse et d'atténuation entreprises par le CST pour mettre en œuvre les solutions au niveau de l'hôte, les solutions axées sur les réseaux et les solutions infonuagiques. Elle décrit également la façon dont le CST analyse, utilise, conserve et divulgue l'information acquise au moyen des trois solutions, ainsi que la manière dont ces activités satisfont à l'objectif d'aider à protéger les systèmes fédéraux.

---

[3] *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65 au para 99 [*Vavilov*] (citant *Dunsmuir c Nouveau-Brunswick*, [2008] 1 RCS 190 aux para 47 et 74; *Catalyst Paper Corp c North Cowichan (District)*, [2012] 1 RCS 5 au para 13).
[4] *Vavilov* au para 14.
[5] *Demande présentée à la ministre de la Défense nationale concernant une autorisation de cybersécurité pour des activités menées afin d'aider à protéger des infrastructures fédérales* datée du 26 mai 2022, au para 13 à la p 4.
[6] *Ibid* para 5 à la p 3.
[7] *Ibid* para 2 aux pp 1–2.

À la lumière des faits exposés dans la demande en l'espèce et le dossier en général, la ministre a tiré des conclusions sur le fondement desquelles elle a délivré une autorisation de cybersécurité, assortie de conditions et restrictions, concernant les activités menées afin d'aider à protéger les systèmes fédéraux.

Sauf pour ce qui est des conclusions qui ont servi de fondement à la délivrance d'une autorisation relative à l'activité visant [redacted], je suis convaincu que les conclusions de la ministre démontrent qu'elle avait des motifs raisonnables de croire, compte tenu des renseignements dignes de foi et concluants qui se trouvaient dans la demande et le dossier en général, que l'autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales était nécessaire et que les conditions de délivrance étaient satisfaites. En particulier, je suis convaincu du caractère raisonnable des conclusions de la ministre selon lesquelles les activités en cause sont raisonnables et proportionnelles, à l'exception des conclusions qui ont servi de fondement à la délivrance d'une autorisation concernant [redacted], compte tenu de l'objectif du CST, qui est d'aider à protéger les systèmes fédéraux, et de la nature de ces activités de cybersécurité. Les autres conclusions de la ministre servent de fondement à l'autorisation qu'elle a délivrée. En outre, ces conclusions appuient la délivrance de l'autorisation, sauf pour celles qui concernent l'exception mentionné précédemment, et elles sont justifiées, transparentes et intelligibles.

Lorsqu'il s'agit d'évaluer si les activités sont raisonnables et proportionnelles, je suis d'avis que la notion de « caractère raisonnable » suppose une activité qui est équitable, solide, logique et bien fondée au regard de l'objectif. La notion de « proportionnalité » nécessite que l'activité ait un lien rationnel avec l'objectif, qu'elle porte le moins possible atteinte aux droits et libertés de tierces parties et qu'elle endommage le moins possible leurs équipements et infrastructures. Qui plus est, elle suppose que l'acquisition de l'information ne l'emporte pas sur l'objectif d'aider à protéger les systèmes fédéraux. De plus, des mesures visant à restreindre l'acquisition et la conservation de l'information devraient être mises en place si cela s'avère nécessaire pour atteindre l'objectif. En d'autres termes, la notion de « proportionnalité » décrite dans le présent paragraphe vise à établir un juste équilibre entre les activités et l'objectif à atteindre.

Il ressort des conclusions de la ministre qu'elle comprenait ces notions et qu'elle les a bien appliquées en ce qui concerne les solutions au niveau de l'hôte, les solutions axées sur les réseaux et les solutions infonuagiques. En outre, elle a fondé ses conclusions à cet égard sur les faits de la demande et le dossier en général, lesquels étaient également clairs. Dans ses conclusions, la ministre montre en quoi les activités d'acquisition de l'information au moyen des trois solutions de cybersécurité sont raisonnables et proportionnelles compte tenu de la nature de l'objectif à atteindre et des activités[8]. Par conséquent, il a été démontré à ma satisfaction que les conclusions de la ministre sont raisonnables en ce qui concerne l'accès aux systèmes fédéraux et l'acquisition de l'information au moyen des trois solutions de cybersécurité proposées.

[8] *Autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales* datée du 1er juin 2022 aux paragraphes 1–46, 44 aux pp 1–9.

Je vais maintenant me pencher sur les conclusions de la ministre relatives à [redacted]

i. [redacted]

Au paragraphe 47c) de l'autorisation, la ministre a autorisé l'activité visant [redacted][9]. Je dois donc examiner les conclusions tirées par la ministre qui ont mené à l'autorisation de cette activité et décider si ces conclusions possèdent les caractéristiques d'une décision raisonnable, soit la justification, la transparence et l'intelligibilité, et si elles sont justifiées au regard des contraintes factuelles et juridiques pertinentes.

Le paragraphe 3 de la demande présentée par la chef du CST est libellé ainsi :

> *[TRADUCTION]*
> *En déployant ses solutions de cybersécurité dans des infrastructures fédérales, le CST risque de contrevenir à d'autres lois fédérales. Au moyen de ses solutions de cybersécurité de* [redacted] *Conformément à* [redacted] *et au paragraphe 27(1) de la Loi sur le CST, en votre qualité de ministre de la Défense nationale, vous pouvez délivrer une autorisation habilitant le CST, malgré toute autre loi fédérale, à accéder à un système fédéral et à acquérir de l'information qui provient de cette infrastructure, qui passe par elle, qui y est stockée ou destinée […][10] (Non souligné dans l'original.)*

Bien que la chef du CST ait besoin d'une autorisation aux termes du paragraphe 27(1) de la Loi sur le CST pour [redacted], elle ne mentionne dans l'extrait précité que l'accès à un système fédéral et l'acquisition de l'information qui provient de cette infrastructure, qui passe par elle, qui y est stockée ou destinée. Il n'y a aucune information à l'appui ni de raisonnement précis établissant de quelle manière l'activité de [redacted] est permise sous le régime du paragraphe 27(1).

Interrogée par la ministre durant le compte rendu qui s'est déroulé le 31 mai 2022 [11], la chef du CST a réitéré que certains [redacted]. Là encore, la chef du CST n'a fourni aucune information à l'appui ni de raisonnement précis à la ministre justifiant le recours au paragraphe 27(1) à cet égard.

---

[9] *Ibid* au para 47(c) à la p 9.
[10] *Supra* note 5 au para 3 à la p 2.
[11] *Compte rendu des discussions avec les responsables du CST, compte rendu du MDN – 31 mai 2022* : *Demande d'autorisation de cybersécurité pour des activités menées dans des activités menées dans des infrastructures fédérales (2022-2023)* à la p l.

La demande souligne l'importance de [redacted], notamment aux paragraphes 101, 108, 110c), 110d), 112 et 117[12]. La ministre décrit en détails également l'importance de [redacted] dans ses conclusions, notamment aux paragraphes 5, 12, 16, 17, 20j) et 28 de l'autorisation[13].

La ministre signale par ailleurs que [redacted], mais elle omet de se reporter, dans ses conclusions, à [redacted] de la Loi sur le CST et de mentionner la nécessité d'obtenir une autorisation visée au paragraphe 27(1) de la Loi sur le CST.

Trois dispositions différentes de la Loi sur le CST sont pertinentes pour les besoins de mon examen.

1) L'article 17, qui a trait au volet du mandat du CST touchant la cybersécurité et l'assurance de l'information. L'alinéa b) dispose que le CST acquiert, utilise et analyse l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir de tels avis, conseils et services.

2) [redacted]

3) Le paragraphe 27(1) mentionne une autorisation en vue d'accéder à l'infrastructure de l'information d'une institution fédérale et d'acquérir de l'information qui provient de cette infrastructure, qui passe par elle, qui y est stockée ou destinée.

Le libellé du paragraphe 27(1) n'invoque pas ni ne permet, à première vue, la délivrance d'une autorisation qui va au-delà de l'accès à l'infrastructure de l'information d'une institution fédérale et de l'acquisition d'information qui provient de cette infrastructure, qui passe par elle, qui y est stockée ou destinée. Cependant, la chef du CST invoque ce paragraphe dans la demande, et la ministre est d'accord, à titre de fondement législatif de l'activité autorisée, soit [redacted]

Au fond, il manque des informations dans les conclusions de la ministre et le dossier sur la façon dont le paragraphe 27(1) s'applique à l'activité autorisée visant [redacted] De fait, cette notion de [redacted] possède une portée beaucoup plus large que l'infrastructure de l'information d'une institution fédérale qui est l'objet de la disposition précitée.

À la lumière de ce qui précède, je suis d'avis que les conclusions de la ministre ne possèdent pas les caractéristiques essentielles d'une décision raisonnable, soit la justification, la transparence,

[12] *Supra* note 5 aux pp 20–24.
[13] *Supra* note 8 aux pp 1–6.

l'intelligibilité, et que l'activité autorisée n'est pas justifiée au regard des contraintes factuelles et juridiques pertinentes[14].

Comme je ne suis pas convaincu que les conclusions de la ministre en ce qui concerne l'activité visant [redacted] sont raisonnables, l'alinéa 20(1)*b*) de la Loi sur le CR exige que je n'approuve pas l'autorisation et que je motive ma décision. J'ai déjà exposé mes motifs ci-dessus.

Je dois maintenant me demander si ma décision a une incidence sur l'autorisation ministérielle dans son ensemble ou seulement sur la partie qui concerne l'activité visant [redacted]. J'estime que c'est ce dernier cas qui s'applique.

L'autorisation peut concerner plus d'une activité, et tel est généralement le cas. L'article 35 de la Loi sur le CST énonce clairement qu'une autorisation délivrée en vertu du paragraphe 27(1) doit préciser a) les activités ou catégories d'activités qu'elle autorise le CST à mener.

Le paragraphe 34(1) de la Loi sur le CST permet à la ministre de délivrer une autorisation si elle conclut qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle. Le libellé de la version anglaise est « *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* ». (Non souligné dans l'original.)

Par conséquent, la ministre doit appliquer le critère prévu au paragraphe 34(1) à chaque activité devant être autorisée.

Selon l'alinéa 20(1)*a*) de la Loi sur le CR, après son examen, le commissaire au renseignement approuve l'autorisation s'il est convaincu que les conclusions en cause sont raisonnables. Le libellé de la version anglaise est « *if he or she is satisfied that the conclusions at issue are reasonable* ». L'alinéa 20(1)*b*) vise les situations où, au contraire, le commissaire au renseignement n'est pas convaincu du caractère raisonnable des conclusions en cause. (Non souligné dans l'original.)

L'analyse des dispositions ci-dessus de la Loi sur le CR et de la Loi sur le CST m'amène à conclure que le commissaire au renseignement doit décider si, pour chaque activité visée par la demande d'autorisation présentée par le demandeur, les conclusions en cause sont raisonnables, tout comme la ministre doit décider si elle peut conclure que chacune de ces activités est raisonnable et proportionnelle.

Je suis également d'avis que le législateur ne peut avoir voulu que le régime législatif en question appuie la position intenable selon laquelle il n'y a pas lieu d'approuver l'autorisation dans son ensemble, portant sur plusieurs activités, dès que les conclusions concernant une activité en particulier sont jugées déraisonnables.

[14] *Supra* note 3.

Compte tenu de mon analyse, je suis d'avis que, dans mon rôle qui consiste à décider si, tout bien considéré, il faut approuver ou non l'autorisation, la loi m'autorise à ne pas me dire convaincu que les conclusions ministérielles en cause, sur lesquelles repose l'autorisation de l'activité visant [redacted], sont raisonnables[15]. Par conséquent, je n'approuve pas l'autorisation concernant cette activité.

B. La réponse aux remarques formulées dans la décision du commissaire au renseignement de 2021

Dans ma décision de l'an passé, datée du 13 juillet 2021, j'ai formulé des remarques relativement au dossier reçu[16]. Je constate que le dossier de cette année a été constitué compte tenu de ces remarques.

IV. Conclusion

À la lumière de mon examen du dossier présenté, je suis convaincu que les conclusions ministérielles sont raisonnables, sauf en ce qui concerne l'activité visant [redacted] Par conséquent, j'approuve l'autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales datée du 1er juin 2022, conformément à l'alinéa 20(1)*a*) de la *Loi sur le commissaire au renseignement*, sauf pour une activité. Je n'approuve pas la partie de l'autorisation de cybersécurité concernant des activités menées afin d'aider à protéger des infrastructures fédérales en ce qui a trait à l'activité visant [redacted], conformément à l'alinéa 20(1)*b*) de la *Loi sur le commissaire au renseignement*.

(Original signé)
L'honorable Jean-Pierre Plouffe, C.D.
Commissaire au renseignement

27 juin 2022
Date

[15] *Supra* note 3.
[16] *Décision et motifs du commissaire au renseignement, Affaire intéressant une demande présentée par le Centre de la sécurité des télécommunications Canada à la ministre de la Défense nationale au sujet d'une autorisation de cybersécurité concernant des activités menées dans des infrastructures fédérales en vertu du paragraphe 27(1) de la* Loi sur le centre de la sécurité des télécommunications, datée du 13 juillet 2021, dossier : 2200-B-2021-01 aux pp 9–11.