

TRÈS SECRET//SI//RÉSERVÉ AUX CANADIENS

Dossier : 2200-B-2021-01



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, Téléc. 613-992-4256

[TRADUCTION FRANÇAISE]

**AFFAIRE INTÉRESSANT UNE DEMANDE PRÉSENTÉE PAR LE CENTRE
DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS AU MINISTRE DE LA
DÉFENSE NATIONALE AU SUJET D'UNE AUTORISATION DE
CYBERSÉCURITÉ POUR DES ACTIVITÉS MENÉES DANS 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 13 juillet 2021

Canada

TABLE DES MATIÈRES

I. Aperçu.....	3
II. Dispositions législatives.....	4
A. Rôle du ministre	4
B. Rôle du commissaire au renseignement	6
i. Concept applicable du caractère raisonnable.....	6
III. Analyse.....	7
A. Caractère raisonnable des conclusions du ministre.....	7
B. Réponse aux remarques formulées dans la décision du commissaire au renseignement de 2020	9
IV. Remarques	11
A. Demande du CST	11
B. Autorisation ministérielle.....	12
V. Conclusion.....	13

I. Aperçu

Le 18 juin 2021, le ministre de la Défense nationale (le ministre) a délivré une autorisation de cybersécurité pour des activités menées dans des infrastructures fédérales en vertu du paragraphe 27(1) de la *Loi sur le Centre de la sécurité des télécommunications* (la Loi sur le CST)¹. Le 21 juin 2021, le ministre a soumis l'autorisation au Bureau du commissaire au renseignement aux fins de mon examen et approbation conformément à la *Loi sur le commissaire au renseignement* (la Loi sur le CR)². En outre, le dossier comprenait une lettre de présentation du ministre indiquant qu'il disposait des documents suivants lorsqu'il a délivré l'autorisation : 1) la *demande* d'autorisation de cybersécurité pour des activités menées dans des infrastructures fédérales; 2) l'autorisation de cybersécurité pour des activités menées dans des infrastructures fédérales; 3) l'annexe I — Activités de cybersécurité en cours; 4) l'annexe II — Ensemble des politiques du CST sur la mission en matière de cybersécurité; 5) le compte rendu de discussions avec des responsables du CST. Toutefois, parmi les documents qui m'ont été présentés, il y avait aussi un document, qui n'était pas énuméré dans la lettre de présentation, intitulé [TRADUCTION] « Aperçu de l'autorisation de cybersécurité pour le commissaire au renseignement — activités menées dans des infrastructures fédérales 2021-2022 ». Je traiterai de ce document plus loin dans la présente décision.

Compte tenu de la demande écrite présentée par le chef du Centre de la sécurité des télécommunications conformément au paragraphe 33(1) de la Loi sur le CST, le ministre a conclu, aux termes du paragraphe 33(2) de cette même loi, qu'il y avait des motifs raisonnables de croire que l'autorisation de cybersécurité pour des activités menées dans des infrastructures fédérales était nécessaire et que les conditions de sa délivrance, énoncées au paragraphe 34 de la Loi sur le CST, étaient remplies. Le ministre a conclu qu'il y 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. Le ministre a également examiné les conditions énoncées au paragraphe 34(3) de la Loi sur le CST et a conclu qu'il y avait des motifs raisonnables de croire que celles-ci étaient remplies.

À la lumière de mon examen des renseignements présentés, je suis convaincu que les conclusions en cause sont raisonnables. Par conséquent, je dois approuver l'autorisation de cybersécurité pour des activités menées dans des infrastructures fédérales conformément à l'alinéa 20(1)a) de la Loi sur le CR.

¹ LC 2019, c 13, art. 76.

² LC 2019, c 13, art. 50.

II. Dispositions législatives

A. Rôle du ministre

La Loi sur le CST décrit les cinq volets du mandat du CST, notamment le volet cybersécurité et assurance de l'information, qui est énoncé au paragraphe 17 de la Loi sur le CST.

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

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

Conditions des autorisations

34 (1) *Le ministre ne peut délivrer l'autorisation visée aux paragraphes 26(1), 27(1) ou (2), 29(1) ou 30(1) que s'il 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) *Le ministre ne peut délivrer l'autorisation visée aux paragraphes 27(1) ou (2) que s'il 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 pour des activités menées dans des infrastructures fédérales, le ministre doit donc avoir des motifs raisonnables de croire, compte tenu des faits présentés dans la demande écrite du 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, le ministre doit conclure qu'il existe 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, et que les conditions énoncées au paragraphe 34(3) de la Loi sur le CST sont remplies. Ce faisant, le ministre doit expliquer les motifs qui l'ont amené à délivrer l'autorisation. C'est ce qu'il 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 pour des activités menées dans des infrastructures fédérales délivrée par le ministre 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 des renseignements ou du dossier dont disposait le 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 le ministre de la Défense nationale en l'espèce, fournisse au commissaire au renseignement tous les renseignements dont elle disposait au moment d'accorder l'autorisation.

Il convient de souligner que ce sont les conclusions du 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 du ministre, sur lesquelles repose l'autorisation 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 du ministre sont raisonnables. Je désignerai ce processus comme le concept du caractère raisonnable.

Le terme « raisonnable » n'est pas défini dans la Loi sur le CR ni la Loi sur le CST. Toutefois, il s'agit d'un terme qui 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 si ce dernier 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 ministre, qui agit à titre de décideur administratif.

J'estime toutefois que, lorsque le législateur a utilisé le terme « raisonnable » dans le contexte de l'examen quasi judiciaire de décisions administratives par un juge à la retraite d'une juridiction supérieure, son intention était d'accorder à ce terme la signification qui lui est prêtée dans la jurisprudence en droit administratif. À cet égard, le

commissaire au renseignement doit être convaincu que les conclusions du 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 pertinentes³.

En outre, 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 respect⁴.

III. Analyse

A. Caractère raisonnable des conclusions du ministre

Le chef du CST a présenté une demande écrite en vue d'obtenir une autorisation de cybersécurité pour des activités menées dans 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 sophistiquées, notamment des cybercriminels et des acteurs parrainés par l'État. En outre, 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 ainsi que le vaste éventail d'appareils utilisés sur ceux-ci⁵. Dans ce contexte, afin d'aider à protéger les systèmes fédéraux, le CST mène trois activités clés permettant d'accéder aux renseignements qui transitent par les systèmes, appareils et réseaux des institutions fédérales consentantes, et de les acquérir. Ces trois activités sont les solutions au niveau de l'hôte, les solutions axées sur les réseaux et les solutions infonuagiques⁶.

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. La demande décrit également la façon dont le CST analyse, utilise, conserve et divulgue l'information acquise au moyen des trois activités, ainsi que la manière dont ces activités satisfont à l'objectif d'aider à protéger l'information électronique et les infrastructures de l'information fédérales.

À la lumière des faits présentés dans la présente demande et le dossier en général, le ministre a tiré des conclusions sur le fondement desquelles il a délivré l'autorisation,

³ *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65, au paragraphe 99 [*Vavilov*] (citant *Dunsmuir c Nouveau-Brunswick*, [2008] 1 RCS 190 aux paragraphes 47 et 74; *Catalyst Paper Corp. c North Cowichan (District)*, [2012] 1 RCS 5 au paragraphe 13).

⁴ *Vavilov*, au paragraphe 14.

⁵ Demande présentée au ministre de la Défense nationale concernant une autorisation de cybersécurité pour des activités menées dans des infrastructures fédérales datée du 16 juin 2021, aux paragraphes 11 et 77, aux p 3 et 17.

⁶ *Ibid.*, au paragraphe 5, à la p 3.

assortie de conditions et restrictions, concernant des activités de cybersécurité dans des infrastructures fédérales.

Je suis convaincu que les conclusions du ministre démontrent qu'il 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 pour des activités menées dans des infrastructures fédérales était nécessaire et que les conditions relatives à sa délivrance étaient remplies. En particulier, je suis convaincu que les conclusions du ministre, selon lesquelles les activités en cause sont raisonnables et proportionnelles, sont raisonnables compte tenu de la nature de l'objectif du CST, qui est d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales, et de ces activités de cybersécurité. Les conclusions du ministre servent de fondement à l'autorisation qu'il a délivrée. De plus, ces conclusions appuient la délivrance de l'autorisation, 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 « raisonnabilité » suppose une activité qui est équitable, solide, logique et bien fondée au regard de l'objectif. La notion de « proportionnalité » requiert que l'activité soit rationnellement liée à 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, cette notion suppose que l'acquisition de l'information ne l'emporte pas sur l'objectif d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales. 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 du ministre que ce dernier comprenait ces notions et qu'il les a bien appliquées. En outre, il a fondé ses conclusions sur les faits de la demande et du dossier en général, lesquels étaient également clairs. Dans ses conclusions, le ministre montre en quoi l'acquisition de l'information obtenue au moyen des trois activités de cybersécurité est raisonnable et proportionnelle⁷. Par conséquent, il a été démontré à ma satisfaction que les conclusions du ministre sont raisonnables en ce qui concerne l'accès aux systèmes fédéraux et l'acquisition de l'information issue des trois activités de cybersécurité proposées compte tenu de la nature de l'objectif à atteindre et des activités.

⁷ Autorisation de cybersécurité présentée au Centre de la sécurité des télécommunications concernant des activités menées dans des infrastructures fédérales datée du 18 juin 2021, aux paragraphes 1 à 27, aux p 1 à 8.

B. Réponse aux remarques formulées dans la décision du commissaire au renseignement de 2020

Dans ma décision rendue le 30 juillet 2020, j'ai formulé des remarques concernant le dossier reçu⁸. Je souligne que le dossier de l'année en cours répond de manière satisfaisante à la majorité de ces remarques.

À la page 9 de ma décision de 2020, j'ai signalé que l'annexe I de la demande mentionnait les institutions fédérales avec lesquelles le CST menait des activités de cybersécurité qui risquaient de porter atteinte aux attentes raisonnables en matière de vie privée d'un Canadien ou d'une personne au Canada. J'ai également mentionné que ni la demande ni l'annexe ne précisaient la nature des cybersolutions dont profitait chacune des institutions. Je souligne que l'annexe de l'année en cours comprend une liste des institutions fédérales et des cybersolutions (solutions au niveau de l'hôte, solutions axées sur les réseaux et/ou solutions infonuagiques) qui leur sont offertes par le CST⁹.

Aux pages 9 et 10 de ma décision de 2020, j'ai souligné que le CST avait mis en œuvre des activités de solutions infonuagiques, mais que ses capacités d'atténuation connexes étaient toujours en cours d'élaboration. Le ministre avait autorisé le CST à mettre en place des mesures d'atténuation. Cependant, il n'avait imposé aucune condition voulant qu'il soit avisé du moment où ces mesures seraient déployées. J'ai indiqué que le ministre devait être informé du moment où ces mesures d'atténuation seraient déployées au cours de la période d'autorisation, puisque cela lui donnerait l'occasion de déterminer si celles-ci sont conformes aux activités précisées dans la demande. Je signale que le ministre a imposé une condition au chef du CST, à savoir l'informer du déploiement des nouvelles capacités de solutions infonuagiques en cours d'élaboration ainsi que des institutions fédérales auxquelles elles s'appliquent¹⁰.

À la page 10 de ma décision de 2020, j'ai souligné que l'autorisation du ministre ne prévoyait aucune condition voulant qu'il soit avisé en cas de contravention à une loi fédérale. J'ai indiqué que les autorisations ministérielles jouent un rôle important, soit de prévenir les poursuites civiles ou pénales découlant d'activités autorisées et d'aviser le ministre dans le cas où le CST contreviendrait à d'autres lois fédérales qui ne figurent pas dans la demande du chef. Dans l'autorisation pour l'année en cours, le ministre a imposé une condition voulant que le chef l'avise aussitôt que possible dans le cas où le

⁸ Décision et motifs du commissaire au renseignement « Affaire intéressant une demande présentée par le Centre de la sécurité des télécommunications au ministre de la Défense nationale au sujet d'une autorisation de cybersécurité concernant des activités menées dans les infrastructures fédérales en vertu du paragraphe 27(1) de la *Loi sur le centre de la sécurité des télécommunications* » (décision de 2020), 30 juillet 2020. Dossier : 2200-B-2020-01, aux p 8 à 10.

⁹ Annexe I de la demande — [TRADUCTION] « Services de cybersécurité en cours ».

¹⁰ *Précitée*, note 7, au paragraphe 67, à la p 11.

CST contreviendrait à une loi fédérale qui ne figure pas dans la demande¹¹. De plus, il convient de signaler que la demande comprend aussi une autre disposition d'une loi fédérale susceptible d'être enfreinte – [REDACTED]

[REDACTED]¹².

Aux pages 8 et 9 de ma décision de 2020, j'ai souligné que la demande de 2019 comprenait une annexe dans laquelle étaient décrits les résultats obtenus au cours de la période d'autorisation ministérielle de l'année précédente, qui était antérieure à l'entrée en vigueur de la Loi sur le CST. Cette annexe permettait au ministre de tenir compte de ces résultats au moment de déterminer si les activités de cybersécurité étaient nécessaires, puis de décider de les autoriser ou non. J'ai indiqué que la demande de 2020 ne comprenait aucune annexe du genre et que certains exemples relatifs à l'utilisation des solutions au niveau de l'hôte, des solutions axées sur les réseaux et des solutions infonuagiques étaient désuets et répétitifs par rapport à la demande de 2019. La demande pour l'année en cours ne comprenait aucune annexe précisant les résultats, malgré qu'elle présentait des exemples de résultats obtenus pour chacune des activités : – [REDACTED] pour les solutions au niveau de l'hôte, [REDACTED] pour les solutions axées sur les réseaux et [REDACTED] pour les solutions infonuagiques.

Finalement, l'an dernier, j'ai ajouté les remarques suivantes à la page 9 de ma décision :

[TRADUCTION]

Le paragraphe 33(2) de la Loi sur le CST requiert que la demande du chef du CST établisse « les faits qui permettraient au ministre de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire » [non souligné dans l'original]. Il est sans doute possible de démontrer la nécessité d'une activité donnée pour laquelle une autorisation est demandée en expliquant ce que l'activité proposée permettrait d'accomplir, en théorie, au regard de l'objectif ultime de l'initiative.

Cependant, j'estime que le fait de fonder des demandes uniquement ou principalement sur la théorie sous-jacente à l'activité proposée, sans reconnaître précisément l'endroit où l'activité est déployée en pratique, pourrait ne pas satisfaire à la norme juridique que j'ai mentionnée. Les résultats obtenus et les exemples contribuent à établir la nécessité des activités à autoriser, à favoriser la transparence ainsi qu'à appuyer le ministre dans son processus décisionnel. [soulignement ajouté]

¹¹ Précitée, note 7, au paragraphe 65, à la p 11.

¹² Précitée, note 5, au paragraphe 74, à la p 16.

Bien que la demande pour l'année en cours comprenne certains résultats obtenus et des exemples précis relatifs aux solutions au niveau de l'hôte, aux solutions axées sur les réseaux et aux solutions infonuagiques, j'aborderai également cette question dans mes remarques.

IV. Remarques

Je suis convaincu que les conclusions du ministre sont raisonnables. Cependant, j'aimerais me prononcer sur certains aspects de la demande du CST et de l'autorisation dans le but d'améliorer les demandes et les autorisations à venir.

A. Demande du CST

En ce qui concerne les résultats obtenus, y compris les chiffres et données empiriques, je souligne que des résultats supplémentaires auraient pu être présentés au ministre dans la demande pour l'année en cours afin d'étayer la demande en vue d'autoriser le déploiement des solutions au niveau de l'hôte, des solutions axées sur les réseaux et des solutions infonuagiques visant à protéger les systèmes fédéraux. Je suis d'avis que de tels renseignements supplémentaires permettraient de renforcer les conclusions du ministre en ce qui concerne la norme juridique relative à la nécessité de l'autorisation et la question de savoir si les activités proposées sont raisonnables et proportionnelles.

La présente demande comprend les données et exemples suivants :

- Plus de [REDACTED] déployés dans divers points de terminaison (paragraphe 20);
- Solutions au niveau de l'hôte – exemple de [REDACTED] (paragraphe 31), [REDACTED] (paragraphe 32);
- Solutions axées sur les réseaux – exemple de [REDACTED] (paragraphe 42); cueillette de [REDACTED] [REDACTED] (paragraphe 44);
- Solutions infonuagiques – exemple de [REDACTED] (26 mars 2021) (paragraphe 56).

En dépit des renseignements présentés, je réitère que le fait d'inclure, dans une annexe à la demande, des résultats obtenus à jour, y compris des chiffres et données empiriques (comme cela a été fait dans le dossier de 2019) étayerait davantage les faits et déclarations figurant dans la demande, ce qui renforcerait les conclusions du ministre selon lesquelles il y a des motifs raisonnables de croire que l'autorisation est nécessaire et

que les conditions de sa délivrance telles qu'elles sont établies aux paragraphes 34(1) et 34(3) de la Loi sur le CST sont remplies¹³.

B. Autorisation ministérielle

Le paragraphe 23(1) de la Loi sur le CR prévoit que « la personne ayant formulé les conclusions examinées par le commissaire au titre des articles 13 à 19 lui fournit, aux fins de son examen, les renseignements dont elle disposait pour accorder [...] l'autorisation ».

Je signale que dans la lettre de présentation jointe au dossier qu'il m'a soumis, le ministre a mentionné cinq documents dont il disposait au moment de tirer ses conclusions, mais pas la présentation intitulée [TRADUCTION] « Aperçu de l'autorisation de cybersécurité pour le commissaire au renseignement — activités menées dans les infrastructures fédérales 2021-2022 ». D'après la lettre de présentation reçue, il semblerait que la présentation n'a pas été transmise au ministre et qu'elle ne pourrait donc pas être considérée comme faisant partie des renseignements dont il disposait. Cela dit, je signale que le document que j'ai examiné et qui s'intitule [TRADUCTION] « Compte rendu de discussions avec des responsables du CST », qui constituait la pièce n° 5 au dossier, mentionne ce qui suit :

[TRADUCTION]

Le chef adjoint SIGINT a informé le ministre que la demande pour l'année en cours avait été mise à jour en conformité avec la présentation fournie. En particulier, il a souligné les similitudes avec la demande de l'année précédente, a énoncé les changements apportés par le CST à la lumière des commentaires soulevés par le commissaire au renseignement, a souligné les exemples pertinents de bons coups et a expliqué pourquoi le déploiement des capacités en matière de solutions infonuagiques avait été retardé. On a assuré au ministre que le chef du CST l'aviserait lors du déploiement des nouvelles capacités en matière de solutions infonuagiques. Le ministre s'est dit satisfait du compte rendu, a examiné les documents connexes et a approuvé l'autorisation.

[soulignement ajouté]

Malgré que la présentation n'était pas explicitement mentionnée dans la lettre du ministre, j'ai conclu qu'elle faisait partie des documents dont ce dernier disposait, puisque le document [TRADUCTION] « Compte rendu de discussions avec des responsables du CST » y faisait référence. Les mots « présentation fournie » ainsi que le contenu de ce document font référence au contenu de la présentation. Pour éviter toute confusion à l'avenir, et afin de remplir l'obligation que lui impose le paragraphe 23(1) de la Loi sur le CR, le ministre

¹³ Dossier : 2200-B-2019-002. Annexe I – Résultats obtenus lors de la dernière période d'AM.

doit absolument mentionner l'ensemble des documents dont il disposait dans sa lettre de présentation.

En outre, je signale que l'autorisation renvoie à un arrêté ministériel pris le 25 août 2020¹⁴. Cet arrêté n'était pas compris dans le présent dossier présenté au commissaire au renseignement comme il aurait dû l'être. Toutefois, je fais remarquer qu'il figurait au dossier reçu le 21 juillet 2021 concernant l'autorisation de renseignement étranger en vue de mener des activités passives en matière d'accès présentée par le ministre le 18 juin 2021.

V. Conclusion

À la lumière de mon examen du dossier présenté, je suis convaincu que les conclusions ministérielles sont raisonnables. Par conséquent, je dois approuver l'autorisation de cybersécurité pour des activités menées dans les infrastructures fédérales du 18 juin 2021 présentée par le ministre, conformément à l'alinéa 20(1)a) de la *Loi sur le commissaire au renseignement*.

(Signature manuscrite)

L'honorable Jean-Pierre Plouffe, C.D.
Commissaire au renseignement

13 juillet 2021

Date

¹⁴ *Précitée*, note 7, au paragraphe 56, à la p 9.

