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

~~**PROTÉGÉ B**~~

Dossier : 2200-B-2023-02

[TRADUCTION FRANÇAISE]

COMMISSAIRE AU RENSEIGNEMENT

DÉCISION ET MOTIFS

AFFAIRE INTÉRESSANT UNE AUTORISATION DE CYBERSÉCURITÉ POUR DES ACTIVITÉS VISANT À AIDER À PROTÉGER DES INFRASTRUCTURES FÉDÉRALES EN VERTU DU PARAGRAPHE 27(1) DE LA *LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS* ET DE L'ARTICLE 14 DE LA *LOI SUR LE COMMISSAIRE AU RENSEIGNEMENT*

LE 13 JUIN 2023

TABLE DES MATIÈRES

APERÇU

1. Les cybermenaces qui ciblent les Canadiens et les institutions fédérales du Canada sont de plus en plus préoccupantes. Ces attaques, provenant de cybercriminels ou d'acteurs parrainés par des États étrangers, sont de plus en plus nombreuses et complexes. Le Centre de la sécurité des télécommunications (CST), l'organisme national du Canada en matière de cryptologie, a pour mandat d'assurer la sécurité des technologies de l'information du gouvernement du Canada face à cette menace croissante.

2. Dans le cadre de ses activités de cyberprotection, il peut être nécessaire pour le CST de contrevenir à certaines lois canadiennes. En outre, lorsqu'il obtient de l'information sur la cybersécurité liée à des activités malveillantes qui sont menées dans les infrastructures d'information fédérales, le CST peut incidemment acquérir des communications ou de l'information qui nuisent à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

3. Toutefois, le fait de mener des activités visant à protéger l'information électronique et les infrastructures des institutions fédérales contre les méfaits et les perturbations causés par des auteurs de cybermenace ne devrait pas donner au CST un passe-droit pour contrevenir aux lois canadiennes et porter atteinte aux droits des Canadiens et des personnes se trouvant au Canada en matière de protection de la vie privé. À cette fin, le législateur a créé un régime de mise en balance – l'autorisation de cybersécurité – qui vise à donner au CST la latitude nécessaire pour être efficace tout en assurant le respect de la primauté du droit et la protection des droits des Canadiens en matière de respect de la vie privée.

4. Plus précisément, ce régime d'autorisation de cybersécurité permet au CST de contrevenir à certaines lois fédérales ou de tout État étranger lorsqu'il mène des activités de cybersécurité dans le but de protéger l'information électronique et les infrastructures appartenant aux institutions fédérales. Le régime autorise également le CST, dans le cadre de ses activités de cybersécurité, à acquérir, à utiliser, à analyser, à conserver et à diffuser de l'information sur les Canadiens et les personnes se trouvant au Canada, mais seulement si un certain nombre de conditions sont remplies et des mesures précises sont prises. Il a été constaté, dans les autorisations de cybersécurité antérieures, que le recours à la conservation et à la diffusion d'une telle information est extrêmement minime, voire exceptionnel.

5. Le processus d'autorisation découle d'une demande écrite de la chef du CST (la chef) à la ministre de la Défense nationale (la ministre) pour obtenir une autorisation de cybersécurité qui énonce, entre autres, les motifs pour lesquels elle est nécessaire ainsi que les activités que le CST serait autorisé à entreprendre. La ministre peut délivrer l'autorisation de cybersécurité si, entre autres conditions, elle conclut que les activités proposées sont raisonnables et proportionnelles.

6. Une autorisation de cybersécurité ne devient valide qu'après que le commissaire au renseignement l'a approuvée; celui-ci doit déterminer si les conclusions de la ministre en vertu desquelles l'autorisation a été délivrée sont raisonnables.

7. Le 17 mai 2023, en vertu du paragraphe 27(1) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*), la ministre a délivré une autorisation de cybersécurité relativement à des activités visant à aider à protéger des infrastructures fédérales (l'autorisation).

8. Le 18 mai 2023, le Bureau du commissaire au renseignement a reçu l'autorisation à des fins d'examen et d'approbation, au titre de la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*).

9. D'après mon examen et pour les motifs ci-après, je suis convaincu que les conclusions que la ministre a tirées en application des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités et aux catégories d'activités énumérées au paragraphe 36 de l'autorisation sont raisonnables.

10. Par conséquent, conformément à l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation ministérielle relativement à des activités de cybersécurité visant à aider à protéger des infrastructures fédérales.

I. CONTEXTE LÉGISLATIF

A. *Loi sur le Centre de la sécurité des télécommunications*

11. En juin 2019, la *Loi concernant des questions de sécurité nationale (*appelée *Loi de 2017 sur la sécurité nationale*, LC 2019, c 13) est entrée en vigueur et a créé le poste de commissaire au renseignement. Les pouvoirs et les devoirs du CST ont également été élargis par la création de la *Loi sur le CST*, laquelle est entrée en vigueur en août 2019.

12. Le CST est l'organisme canadien du renseignement électromagnétique en matière de renseignement étranger et l'expert technique de la cybersécurité et de l'assurance de l'information. En ce qui a trait au volet de son mandat touchant la cybersécurité et l'assurance de l'information, le CST fournit, comme le décrit l'article 17 de la *Loi sur le CST*, des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales – c'est-à-dire les systèmes fédéraux – contre les cybermenaces. Essentiellement, le CST peut défendre les systèmes, les appareils et les réseaux des institutions fédérales contre les menaces ainsi que fournir des conseils et une orientation qui renforceront leur approche en matière de cybersécurité.

13. Comme le définit le CST, les « systèmes fédéraux » consistent en des réseaux et des systèmes, ainsi que les appareils connectés à ces réseaux et à ces systèmes, qui comprennent aussi diverses combinaisons de matériel informatique et de logiciels. Les « institutions fédérales » comprennent les ministères, les organismes gouvernementaux et les sociétés d'État.

14. Bien que les institutions fédérales aient recours à des mesures disponibles sur le marché (p. ex. antivirus, logiciel pare-feu) pour protéger leurs réseaux contre toute une gamme d'auteurs de cybermenaces de pointe, elles pourraient aussi avoir besoin du soutien du CST pour détecter les activités malveillantes visant ces réseaux et les protéger. Pour comprendre les points d'entrée vulnérables et les atteintes à l'intégrité des systèmes fédéraux, le CST pourrait devoir accéder aux systèmes et acquérir de l'information de ceux-ci. Le CST accède aux systèmes et acquiert cette information afin d'aider les institutions fédérales sur demande seulement et doit obtenir le consentement des institutions fédérales pour ce faire. L'information sur la cybersécurité acquise par le CST ne concerne pas une personne en particulier. Elle porte plutôt sur le fonctionnement des infrastructures de l'information et les menaces à leur intégrité.

15. Conformément au paragraphe 27(1) de la *Loi sur le CST*, le CST peut accéder à une infrastructure de l'information d'une institution fédérale et 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*, LRC 1985, c C-46 (*Code criminel*), cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement. L'alinéa 184(2)e) du *Code criminel* rend inapplicable l'infraction consistant à intercepter sciemment une communication privée si cette communication est interceptée dans un système informatique et est raisonnablement nécessaire pour gérer la qualité du service de ce système informatique ou pour le protéger.

16. Pour acquérir l'information passant par les systèmes fédéraux ou y accéder, le CST mène des activités de cybersécurité techniques à l'aide de trois types de capteurs. Les solutions de cybersécurité sont appliquées à différents niveaux de l'infrastructure de l'information fédérale pour détecter et contrer les cyberactivités malveillantes. Elles incluent : 1) les solutions au niveau de l'hôte — des capteurs sont installés sur des dispositifs de points terminaux physiques ou virtuels (p. ex. postes de travail, appareils mobiles et serveurs); 2) les solutions axées sur les réseaux — les capteurs sont installés sur le périmètre du réseau donnant ainsi au CST accès à tout le trafic du réseau et entraînant automatiquement la prise de mesures d'atténuation; 3) les solutions infonuagiques — offre des capacités semblables aux deux solutions susmentionnées, mais les capteurs sont déployés dans un environnement infonuagique. [description du traitement des données] [redacted]

17. La *Loi sur le CST* impose un certain nombre de limites et de conditions au CST en ce qui a trait à l'acquisition d'information à partir des systèmes fédéraux. Plus particulièrement, les activités du CST ne doivent pas viser un Canadien ou toute personne se trouvant au Canada. Cependant, le CST peut utiliser et conserver l'information liée à un Canadien ou à une personne se trouvant au Canada qui a été obtenue incidemment, c'est-à-dire que l'information acquise n'était pas délibérément recherchée (paragraphe 23(5) de la *Loi sur le CST*). Comme le montrent les résultats d'autorisations antérieures en matière de cybersécurité, cette acquisition faite incidemment est plutôt exceptionnelle. En outre, conformément au paragraphe 22(1) de la *Loi sur le CST*, les activités ne peuvent porter atteinte à la *Charte canadienne des droits et libertés* (*Charte*). De plus, en vertu de l'article 24 de la *Loi sur le CST*, le CST est tenu de mettre en place des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation de l'information acquise à partir de systèmes fédéraux.

18. Enfin, les activités de cybersécurité du CST ne doivent pas contrevenir aux autres lois fédérales (l'article 50 de la *Loi sur le CST* stipule que la partie VI du *Code criminel* ne s'applique pas à l'interception de communications faite en conformité avec une autorisation de cybersécurité) ni porter atteinte à une attente raisonnable en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada, à moins d'être menées au titre d'une autorisation délivrée en vertu du paragraphe 27(1) de la *Loi sur le CST* (paragraphe 22(3) de la *Loi sur le CST*), comme le stipule explicitement le paragraphe 22(4) de la *Loi sur le CST*.

19. Par conséquent, lorsque les activités de cybersécurité menées par le CST contreviendront à une loi fédérale ou porteront atteinte à la vie privée de Canadiens ou de personnes se trouvant au Canada, le CST doit demander à la ministre de délivrer une autorisation de cybersécurité conformément aux paragraphes 22(4) et 27(1) de la *Loi sur le CST*. La ministre autorise par écrit le CST à mener légalement les activités décrites dans l'autorisation même si elles peuvent exceptionnellement contrevenir à une loi fédérale ou porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

20. Tandis que l'article 33 de la *Loi sur le CST* décrit les exigences que doit remplir le CST pour présenter une demande d'autorisation ministérielle, les paragraphes 34(1) et (3) de la *Loi sur le CST* définissent les conditions prescrites par la loi qui doivent être respectées afin que la ministre puisse autoriser les activités du CST. La ministre peut délivrer une autorisation si elle est convaincue que les conditions prescrites par la loi ont été satisfaites. Cette question sera abordée plus en détail dans la section « Analyse » de la présente décision.

21. L'autorisation ministérielle n'est valide qu'une fois approuvée par le commissaire au renseignement (paragraphe 28(1) de la *Loi sur le CST*). Ce n'est qu'à ce moment-là que le CST peut exercer les activités autorisées précisées dans l'autorisation.

B. ***Loi sur le commissaire au renseignement***

22. Selon l'article 12 de la *Loi sur le CR*, le rôle du commissaire au renseignement consiste à mener un examen quasi judiciaire des conclusions de la ministre en vertu desquelles certaines autorisations — dans le cas présent, une autorisation de cybersécurité — sont délivrées, pour déterminer si ces conclusions sont raisonnables.

23. L'article 14 de la *Loi sur le CR*, qui porte sur la délivrance d'une autorisation de cybersécurité, indique que le commissaire au renseignement examine si les conclusions formulées par la ministre au titre des paragraphes 34(1) et (3) de la *Loi sur le CST* et sur lesquelles repose l'autorisation de cybersécurité délivrée sont raisonnables.

24. La ministre est tenue par la loi (article 23 de la *Loi sur le CR*) de fournir au commissaire au renseignement tous les renseignements dont elle disposait à titre de décideur. Comme le prévoit la jurisprudence du commissaire au renseignement, cette obligation vise aussi tout renseignement verbal consigné par écrit, dont ceux des séances d'information ministérielles. Le commissaire au renseignement n'a cependant pas droit d'accès aux renseignements confidentiels du Cabinet (article 26 de la *Loi sur le CR*).

25. Conformément à l'article 23 de la *Loi sur le CR*, la ministre a confirmé dans sa lettre de présentation qu'on m'avait transmis tous les documents dont elle disposait pour prendre sa décision. Par conséquent, voici les documents qui composent le dossier dont je dispose :

a) l'autorisation de la ministre, datée du 17 mai 2023;
b) la demande présentée par la chef, qui comprend quatre annexes en date du 28 avril 2023;
c) l'ensemble des politiques sur la mission en matière de cybersécurité (les politiques sur la mission), approuvé le 28 février 2022;
d) la note d'information du chef du CST adressée à la ministre, datée du 28 avril 2023;
e) la demande présentée par la chef, qui comprend quatre annexes;
f) le document intitulé « Briefing Deck – Overview of the Activities » [document d'information – aperçu des activités].

II. NORME DE CONTRÔLE

26. La *Loi sur le CR* stipule que le commissaire au renseignement doit examiner si les conclusions de la ministre sont raisonnables. La jurisprudence du commissaire au renseignement établit que la norme du caractère raisonnable qui s'applique au contrôle judiciaire d'une mesure administrative est la même que celle qui s'applique à mon examen.

27. Au paragraphe 99 de l'arrêt *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65 [*Vavilov*], la Cour suprême du Canada décrit brièvement en quoi consiste une décision raisonnable :

> La cour de révision doit s'assurer de bien comprendre le raisonnement suivi par le décideur afin de déterminer si la décision dans son ensemble est raisonnable. Elle doit donc se demander si la décision possède les caractéristiques d'une décision raisonnable, soit la justification, la transparence et l'intelligibilité, et si la décision est justifiée au regard des contraintes factuelles et juridiques pertinentes qui ont une incidence sur celle-ci.

28. Les contraintes factuelles et juridiques pertinentes peuvent comprendre le régime législatif applicable, l'incidence de la décision et les principes d'interprétation des lois. En fait, il est nécessaire, pour comprendre ce qui est raisonnable, de tenir compte du contexte de la décision faisant l'objet de l'examen et de celui de l'examen lui-même. Il est donc nécessaire de comprendre le rôle du commissaire au renseignement, qui fait partie intégrante du régime législatif institué par la *Loi sur le CR* et la *Loi sur le CST*.

29. L'examen de ces lois et des débats législatifs consacrés à la création de la fonction de commissaire au renseignement montrent que le législateur a créé cette fonction en tant que mécanisme indépendant visant à garantir que les mesures gouvernementales en matière de sécurité nationale établiraient un équilibre entre la primauté du droit et les droits et libertés des Canadiens. Pour maintenir cet équilibre, j'estime que le législateur m'a attribué un rôle de gardien et de surveillant des autorisations ministérielles.

30. Cela veut dire que, dans le cadre de son examen quasi judiciaire, le commissaire au renseignement doit prendre en considération les objectifs du régime législatif ainsi que le rôle de la ministre, et le sien. Je dois examiner attentivement et soupeser le droit au respect de la vie privée et autres droits importants

des Canadiens et des personnes se trouvant au Canada qui pourraient être touchés par l'autorisation faisant l'objet d'un examen.

31. Une fois convaincu que les conclusions ministérielles en cause sont raisonnables, le commissaire au renseignement « approuve l'autorisation » (alinéa 20(1)a) de la *Loi sur le CR*). Si, au contraire, les conclusions sont jugées déraisonnables, il « n'approuve pas l'autorisation » (alinéa 20(1)b) de la *Loi sur le CR*).

32. Dans le contexte d'une autorisation de cybersécurité délivrée en vertu du paragraphe 27(1) de la *Loi sur le CST* – soit la question dont je suis saisi – la jurisprudence du commissaire au renseignement prévoit que le commissaire au renseignement peut approuver « en partie » une autorisation.[1]

33. La décision du commissaire au renseignement est susceptible de contrôle judiciaire par la Cour fédérale, sur demande, en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*, LRC 1985, c F-7.

III. ANALYSE

34. Le 28 avril 2023, la chef a transmis une demande écrite d'autorisation de cybersécurité relativement à des activités visant à protéger des infrastructures fédérales (la demande) dans le cadre de son mandat. La demande en question décrit les activités que peut entreprendre le CST pour accéder à une infrastructure de l'information d'une institution fédérale ou acquérir de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée afin de protéger cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de son fonctionnement.

35. Sont aussi expliqués dans la demande les avantages de déployer des solutions de cybersécurité dans les systèmes fédéraux et de mettre en place de multiples couches de défense à la lumière de l'information sur la menace et de l'analyse des activités anormales. En outre, il y est indiqué comment l'information obtenue en vertu de cette autorisation ministérielle protège non seulement les systèmes fédéraux, mais aussi les systèmes non fédéraux importants pour le gouvernement du Canada (p. ex. énergie, finances et télécommunications). Aussi, la demande décrit comment la chef propose que le CST analyse, traite et conserve l'information acquise ainsi que les mesures en place pour protéger la vie privée des

[1] *Commissaire au renseignement – Décision et motifs*, 27 juin 2022, Dossier : 2200-B-2022-01, pages 10–11.

Canadiens et des personnes se trouvant au Canada, dans les cas où le CST acquiert incidemment de l'information sur eux.

36. En se fondant sur les faits présentés dans la demande et de façon générale dans le dossier, la ministre conclut conformément au paragraphe 33(2) de la *Loi sur le CST* qu'il y a des motifs raisonnables de croire que cette autorisation est nécessaire et que les conditions prévues aux paragraphes 34(1) et (3) de la *Loi sur le CST* sont remplies.

37. Par conséquent, la ministre a autorisé le CST à mener les activités décrites au paragraphe 36 de l'autorisation :

a) accéder à un système fédéral et déployer, à la demande d'un client fédéral, des solutions au niveau de l'hôte, des solutions axées sur les réseaux et des solutions infonuagiques;
b) acquérir toute information à l'aide des solutions susmentionnées, y compris l'information ayant trait à un Canadien ou à une personne se trouvant au Canada qui provient ou passe par les systèmes fédéraux, qui y est destinée ou y est stockée;
c) utiliser, analyser, conserver ou divulguer l'information acquise en vertu de cette autorisation afin de découvrir, d'isoler, de prévenir ou d'atténuer des dommages aux systèmes fédéraux;
d) mettre en place des mesures d'atténuation, telles qu'elles sont décrites dans la demande, pour contrer les cybermenaces.

38. Je dois maintenant déterminer si les conclusions de la ministre – relativement aux conditions énoncées aux paragraphes 34(1) et (3) de la *Loi sur le CST* et sur la base desquelles l'autorisation a été délivrée en vertu du paragraphe 27(1) de la *Loi sur le CST* – sont raisonnables.

A. *Paragraphe 34(1) de la Loi sur le CST*

i. Signification du caractère raisonnable et proportionnel

39. Selon le paragraphe 34(1) de la *Loi sur le CST*, pour que la ministre délivre une autorisation de cybersécurité, elle doit conclure « 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 ».

40. Déterminer si une activité est « raisonnable » en vertu du paragraphe 34(1) fait partie des obligations de la ministre et diffère de l'examen de la « norme de la décision raisonnable » effectué par le commissaire au renseignement. La ministre conclut que toute activité qui serait permise par l'autorisation est raisonnable en appliquant sa compréhension de ce que ce terme signifie. Le commissaire au renseignement détermine si les conclusions de la ministre sont raisonnables, en procédant à un examen quasi judiciaire selon la norme de la décision raisonnable, expliquée précédemment.

41. Pour déterminer si une activité est raisonnable et proportionnelle en vertu du paragraphe 34(1), il faut aussi tenir compte du contexte. La ministre pourrait être d'avis qu'en raison du contexte, un certain nombre de facteurs doivent être pris en compte. Néanmoins, je suis d'avis que, pour que les conclusions de la ministre soient raisonnables, sa compréhension de la signification de ces termes doit au moins refléter les aspects sous-jacents suivants.

42. Selon la jurisprudence du commissaire au renseignement, le caractère « raisonnable » énoncé au paragraphe 34(1) de la *Loi sur le CST* s'entend d'une activité juste, éclairée, logique, bien fondée et justifiée compte tenu des objectifs devant être atteints. J'ajoute qu'il est nécessaire que l'activité soit légale au sens qu'elle doit être permise par la loi. Le rôle du commissaire au renseignement se limite à l'examen du caractère raisonnable des conclusions formulées par la ministre compte tenu des exigences énoncées aux paragraphes 34(1) et (3) de la *Loi sur le CST*. Si une autorisation de cybersécurité comprend des activités que la loi ne permet pas à la ministre d'inclure, je suis d'avis qu'une telle conclusion devrait faire l'objet d'un examen à la lumière du critère du « caractère raisonnable ».

43. Essentiellement, une activité raisonnable est autorisée par la *Loi sur le CST* et est justifiée compte tenu de ses objectifs. Les objectifs de l'activité doivent correspondre aux objectifs de la loi. Dans le contexte de la présente demande, cela signifie que les objectifs des activités autorisées doivent contribuer au mandat du CST en matière de cybersécurité et de l'assurance de l'information.

44. Pour ce qui est de la notion de « proportionnalité », elle requiert d'équilibrer les intérêts en jeu. Une comparaison utile est la mise en balance effectuée dans un examen du caractère raisonnable alors que des droits garantis par la *Charte* sont en jeu. Dans ce contexte, un décideur doit procéder à une mise en balance des droits garantis par la *Charte* et des objectifs de la loi en se demandant comment protéger au mieux la valeur en jeu consacrée par la *Charte* compte tenu des objectifs visés par la loi (voir par exemple l'affaire *Doré c. Barreau du Québec*, 2012 CSC 12, aux paragraphes 55-58). Il ne suffit pas

de simplement procéder à la mise en balance des garanties d'une part et des objectifs de la loi d'autre part. Une cour de révision doit se demander s'il existait d'autres possibilités raisonnables qui donneraient davantage effet aux protections conférées par la *Charte* eu égard aux objectifs applicables (*Law Society of British Columbia c. Trinity Western University*, 2018 CSC 32, aux paragraphes 80 à 82).

45. En l'occurrence, il faut que la ministre effectue un exercice de mise en balance et conclue que les activités qui seraient permises en vertu de l'autorisation ne portent atteinte que de façon minimale aux droits à la vie privée des Canadiens et des personnes se trouvant au Canada. Il importe également que la nature intrusive de l'activité ne l'emporte pas sur les objectifs de l'activité. S'il est nécessaire d'atteindre ces objectifs, des mesures doivent être mises en place pour restreindre l'acquisition, la conservation et l'utilisation de l'information.

ii. Examen de la conclusion de la ministre selon laquelle les activités en cause sont raisonnables

46. La ministre a conclu, au paragraphe 10 de l'autorisation, qu'elle avait [traduction] « des motifs raisonnables de croire que les activités autorisées dans l'autorisation sont raisonnables, compte tenu de l'objectif d'aider à protéger les systèmes fédéraux contre les méfaits, l'utilisation non autorisée ou la perturbation ».

47. J'estime que la conclusion de la ministre est raisonnable. Il existe un lien rationnel clair entre les activités de cybersécurité proposées par le CST et leur objectif, lequel consiste à aider à protéger des systèmes fédéraux. Il ressort clairement du dossier que ces activités de cybersécurité particulières contribuent au mandat du CST en matière de cybersécurité et d'assurance de l'information. J'estime aussi que la ministre a bien compris et expliqué pourquoi ces activités sont nécessaires pour aider à protéger les systèmes fédéraux.

48. Je crois néanmoins qu'il est utile d'ajouter certains commentaires relativement à l'une des activités pour lesquelles une autorisation est demandée, soit [traduction] « la prise de mesures d'atténuation, tel qu'il est décrit dans la demande, pour contrer les cybermenaces » (paragraphe 36(d) de l'autorisation). Un certain nombre de mesures d'atténuation sont décrites dans la demande – [types de mesures d'atténuation]

[redacted]

49. Le CST a clairement le pouvoir de prendre des mesures d'atténuation (alinéa 23(3)a) de la *Loi sur le CST*). Effectivement, le volet de son mandat touchant la cybersécurité et l'assurance de l'information prévoit précisément que le Centre fournit des « services afin d'aider à protéger » les systèmes fédéraux et qu'il ne peut y avoir cybersécurité sans mesures d'atténuation (paragraphe 17a)(i) de la *Loi sur le CST*). Il reste à déterminer si les mesures d'atténuation doivent être incluses dans une autorisation de cybersécurité en vertu du paragraphe 27(1) de la *Loi sur le CST*, qui énonce ce qui suit :

> Le ministre peut délivrer au Centre une autorisation de cybersécurité habilitant ce dernier, dans la réalisation du volet de son mandat touchant la cybersécurité et l'assurance de l'information et malgré toute autre loi fédérale, 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. (non souligné dans l'original)

50. Pour ce qui est d'interpréter la *Loi sur le CST*, mon rôle consiste à déterminer si l'interprétation de la ministre est raisonnable (*Vavilov*, au paragraphe 123). En me fondant sur l'inclusion d'activités liées à la prise de mesures d'atténuation dans l'autorisation, j'en déduis que la ministre a interprété le paragraphe 27(1) comme ne se limitant pas aux activités consistant à « accéder » aux systèmes et à « acquérir » de l'information, mais incluant aussi la prise de mesures d'atténuation. Bien que je reconnaisse qu'une interprétation raisonnable possible du paragraphe en question pourrait être que seules les activités qui pourraient ou devraient être autorisées en vertu d'une autorisation de cybersécurité sont celles consistant à « accéder » aux réseaux et à « acquérir » de l'information, après avoir lu la disposition en entier, dans le contexte du mandat en matière de cybersécurité énoncé dans la *Loi sur le CST*, je suis convaincu que l'interprétation de la ministre est raisonnable. En effet, en lisant la disposition en entier et en tenant compte de l'objectif de demander une autorisation ministérielle, il est justifié de comprendre que les termes « accéder », « acquérir » et « afin d'aider à protéger » comprennent des mesures d'atténuation.

51. Parce que des mesures d'atténuation pourraient contrevenir à une loi fédérale ou porter atteinte aux droits à la vie privée de Canadiens ou de toute personne se trouvant au Canada, l'interprétation de la ministre pourrait en fait être la seule interprétation raisonnable. Les autorisations ministérielles et les

examens effectués par le commissaire au renseignement sont des mécanismes permettant de veiller à ce que toute contravention à la loi ou toute atteinte aux droits à la vie privée soit adéquatement justifiée. Le paragraphe 22(4) énonce explicitement ce principe. En tant que gardien, mon rôle dans le régime d'autorisation de cybersécurité consiste à assurer un équilibre adéquat entre la nécessité de protéger les systèmes fédéraux et la protection des droits des personnes. Cela signifie que, si le CST souhaite mener une activité de cybersécurité qui pourrait avoir une incidence sur la primauté du droit ou les droits en matière de vie privée, l'autorisation ministérielle et l'examen mené par le commissaire au renseignement sont nécessaires. Bien que je note que la chef explique dans sa demande que le CST estime qu'il est « improbable » que les activités d'atténuation constituent une infraction, elle reconnaît qu'il y a un risque que ces mesures puissent contrevenir au *Code criminel*. Par conséquent, il semble que ces activités devraient effectivement être autorisées par la ministre et approuvées par le commissaire au renseignement.

iii. Examen de la conclusion de la ministre selon laquelle les activités en cause sont proportionnelles

52. La ministre a conclu au paragraphe 13 de l'autorisation qu'elle avait des motifs raisonnables de croire que les activités autorisées sont [traduction] « proportionnelles compte tenu de la façon dont elles sont menées ».

53. Je suis convaincu que la conclusion de la ministre à cet égard est raisonnable. Le dossier révèle clairement que la ministre a effectué un exercice de mise en balance lorsqu'elle a analysé la façon dont l'acquisition de l'information des systèmes fédéraux et la protection de la vie privée sont prises en compte dans les politiques et les pratiques de cybersécurité du CST.

54. Les lois fédérales auxquelles il pourrait y avoir contravention, et plus particulièrement les dispositions en jeu, sont en nombre limité et n'entraîneraient que peu de conséquences sur le public canadien. Je note aussi que, surtout parce que le CST obtiendra le consentement des institutions fédérales pour accéder à leurs systèmes, la possibilité de contrevenir aux lois canadiennes sera faible. En outre, le CST propose de mener ses activités de façon à limiter les infractions potentielles. Ainsi, je suis convaincu qu'en cas de contravention à une loi fédérale, l'impact de l'atteinte sera limité.

55. Comme il a été indiqué plus tôt, l'information acquise par le CST ne concerne aucune personne en particulier. Si une communication privée impliquant un Canadien devait être interceptée

exceptionnellement, le CST explique qu'il ne la conservera que dans les limites des conditions permises dans la *Loi sur le CST*. Aussi, l'accès à l'information acquise est restreint aux employés désignés du CST qui ont été formés pour manipuler ce type d'information et l'utiliser selon le besoin de savoir dans le cadre de leur travail.

56. La ministre était clairement au courant des droits au respect à la vie privée en jeu et a exposé les mesures en place pour les protéger. Par conséquent, elle en est arrivée à la conclusion que les activités proposées ne l'emportent pas sur toute atteinte potentielle aux droits des Canadiens en matière de vie privée.

B. ***Paragraphe 34(3) – Conditions d'autorisation – Cybersécurité***

57. Le paragraphe 34(3) de la *Loi sur le CST* dispose que la ministre peut délivrer une autorisation de cybersécurité seulement si elle conclut qu'il y a des motifs raisonnables de croire que les quatre conditions suivantes sont remplies :

a) l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire;

b) le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu;

c) l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information des institutions fédérales;

d) 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 aux informations électroniques ou aux infrastructures de l'information des institutions fédérales.

i. L'information acquise ne sera pas conservée plus longtemps que ce qui est nécessaire

58. L'autorisation décrit comment l'information évaluée aux fins de la protection de systèmes fédéraux est conservée conformément aux politiques du CST, à la *Loi sur la Bibliothèque et les Archives du Canada*, LC 2004, c 11, et à la *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21. Un calendrier de conservation pour les différentes catégories d'information recueillie est inclus, et la ministre a conclu que l'information ne serait pas conservée plus longtemps qu'il n'est nécessaire.

59. Je comprends que l'objectif du CST est d'évaluer l'information recueillie sans délai et de conserver l'information utile seulement si elle s'avère toujours utile.

60. Une fois l'information acquise, la ministre explique qu'une période de conservation de [redacted] est nécessaire pour donner au CST le temps d'analyser l'information dans le cas d'un cyberévénement et d'examiner son évolution au fil du temps. Cela permet également au CST de comparer les nouvelles vulnérabilités découvertes par rapport à son information non évaluée et de déterminer si elles existent au sein des réseaux fédéraux du gouvernement du Canada.

61. Dans le délai de [redacted], le CST évalue si l'information est nécessaire ou essentielle. Le critère du caractère « nécessaire » s'applique à l'information qui ne concerne pas un Canadien ou une personne se trouvant au Canada. Tel qu'il est défini dans l'autorisation, ce type d'information est considérée nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux lorsqu'elle est requise pour comprendre les cyberactivités malveillantes, [redacted] afin d'aider à protéger les systèmes fédéraux. Le critère du caractère « essentiel » pour sa part s'applique à l'information liée à un Canadien ou à une personne se trouvant au Canada. L'information est considérée essentielle si, sans elle, le CST ne pouvait être en mesure de découvrir, d'isoler, de prévenir ou d'atténuer les dommages causés aux systèmes fédéraux. D'après les autorisations antérieures, l'information qui répond au critère du caractère « essentiel » est extrêmement rare. L'information qui n'est pas évaluée ou qui n'est pas jugée nécessaire ou essentielle est automatiquement supprimée au plus tard [redacted] après la date de son acquisition.

62. L'information qui a été jugée nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes fédéraux peut être conservée « indéfiniment » ou jusqu'à ce qu'elle ne soit plus utile à ces fins. Je comprends que ce critère signifie que l'information pourrait être utile indéfiniment, mais qu'elle ne sera plus conservée lorsque son utilité à ces fins cessera.

63. Compte tenu des importantes restrictions à l'accès à l'information non évaluée, j'estime raisonnable la conclusion de la ministre concernant la période d'évaluation de [redacted].

64. Je suis également d'accord avec la ministre lorsqu'elle conclut que l'information qui est nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes fédéraux peut être conservée jusqu'à ce qu'elle ne soit plus utile. Bien sûr, les auteurs de menace étrangers et

plus particulièrement les auteurs parrainés par des États étrangers utilisent souvent les mêmes techniques et indicateurs de compromission aussi longtemps qu'ils demeurent efficaces. Il est justifié de conserver l'information pendant le temps nécessaire pour réagir à cette menace. Je note néanmoins que cela repose sur la prémisse que le critère « jusqu'à ce que l'information ne soit plus utile » laisse entendre nécessairement que des examens périodiques de l'information seront effectués. Il ne ressort pas clairement du dossier si le CST a des procédures en place pour surveiller et examiner l'utilité ou le caractère essentiel de l'information conservée.

65. Je soulève d'ailleurs la question dans mes remarques.

ii. Le consentement des personnes ne peut raisonnablement être obtenu

66. Tel qu'il est expliqué dans l'autorisation, avant de déployer des solutions au niveau de l'hôte, des solutions axées sur les réseaux et des solutions infonuagiques en matière de cybersécurité, le CST doit obtenir le consentement écrit des propriétaires des systèmes des institutions fédérales. Pour leur part, les institutions fédérales doivent, conformément à la pratique normalisée du gouvernement, aviser les utilisateurs que leurs activités sur les appareils et les réseaux sont surveillées aux fins de cybersécurité et d'assurance de l'information. Dans certaines situations, il est impossible d'obtenir le consentement de personnes avant d'interagir avec ces infrastructures fédérales de l'information. Cela serait notamment le cas lorsqu'un utilisateur externe est en contact avec un fonctionnaire fédéral.

67. J'estime que la conclusion de la ministre à l'égard de cette condition est raisonnable.

iii. Toute information acquise est nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages causés au système fédéral

68. Les conclusions de la ministre expliquent comment les auteurs de menace déguisent leurs activités et leurs comportements malveillants afin de réduire la probabilité de détection. Ils le font au moyen d'applications, de courriels, de clavardage et de processus qui semblent légitimes à l'utilisateur ou la cible, mais qui contiennent des codes ou des liens malveillants menant à l'exfiltration d'information de nature délicate, ce qui inclut l'installation de logiciels malveillants sur l'ordinateur ciblé. Grâce aux solutions au niveau de l'hôte, aux solutions axées sur les réseaux et aux solutions infonuagiques [description de comment l'information est nécessaire] [redacted]

[redacted]

69. J'estime que la conclusion de la ministre est raisonnable. Les exemples fournis montrent que l'information acquise en vertu de l'autorisation est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information des institutions fédérales. Effectivement, le CST doit acquérir de l'information précise sur les systèmes fédéraux qu'il doit protéger.

iv. Les mesures en place font en sorte que l'information acquise sur des Canadiens ou des personnes se trouvant au Canada sera utilisée, analysée ou conservée seulement si elle est essentielle pour isoler, prévenir ou atténuer des dommages causés aux systèmes fédéraux

70. Les conclusions de la ministre décrivent les mesures visant à protéger les droits des Canadiens et des personnes se trouvant au Canada en matière de protection de la vie privée. La ministre précise que l'accès à l'information acquise en vertu de l'autorisation est limité aux personnes qui possèdent les qualifications nécessaires pour mener des activités de cybersécurité et qui ont suivi la formation sur les procédures de manipulation de l'information, et que la grande majorité de l'analyse de l'information est effectuée au moyen de processus automatisés, ce qui permet de limiter l'accès des employés à l'information non évaluée.

71. La ministre précise également que l'information concernant des Canadiens ou des personnes se trouvant au Canada ne peut être conservée que si elle est jugée essentielle. Comme il a été mentionné précédemment, l'information est définie comme étant essentielle lorsque le CST serait autrement incapable de découvrir, d'isoler ou de prévenir des dommages aux systèmes fédéraux. Le dossier indique aussi que l'information est essentielle [traduction] « lorsqu'elle fournit un aperçu [redacted] afin d'aider à protéger les systèmes fédéraux ». Je suis d'avis que la compréhension du terme « essentiel » du CST ne se situe pas au-delà des interprétations acceptables.

72. L'ensemble des politiques relatives à la mission de cybersécurité – c'est-à-dire toutes les politiques qui s'appliquent aux activités de cybersécurité – inclus dans le dossier indique que c'est un analyste qui procède à l'analyse du caractère essentiel de l'information acquise (EPM 8.2.2). Cette analyse

s'effectue au moyen de processus manuels ou automatisés, avant que l'information soit conservée. Aussi, il faut consigner les justifications du caractère « essentiel ».

73. En plus de décrire les cas dans lesquels l'information qui pourrait permettre d'identifier un Canadien est conservée, le dossier fournit de l'information sur la façon dont cette information peut être divulguée, ce qui reprend l'obligation légale prévue à l'article 44 de la *Loi sur le CST*. Je note que les rapports suivant l'expiration de l'autorisation que j'ai reçus conformément à l'article 52 de la *Loi sur le CST* démontrent qu'il est extrêmement rare qu'une telle information soit conservée, et je crois comprendre que cette information n'a jamais été divulguée à l'extérieur du CST.

74. Compte tenu de ce qui précède, je suis d'avis que le dossier montre que les politiques et les pratiques du CST prennent au sérieux la conservation, l'analyse et l'utilisation de l'information concernant des Canadiens ou des personnes se trouvant au Canada. Je suis convaincu que les conclusions ministérielles sont raisonnables puisqu'une infime partie de l'information sera utilisée, analysée ou conservée que si elle s'avère essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques et aux infrastructures de l'information des institutions fédérales.

IV. REMARQUES

75. Je tiens à reconnaître les efforts déployés par le CST pour intégrer certaines remarques que j'ai formulées dans des décisions antérieures. Plus particulièrement, les explications additionnelles relatives au calendrier de conservation du CST m'ont été utiles lors de l'examen du dossier. En outre, j'ai apprécié l'engagement du CST à m'avertir en cas de contravention à une loi fédérale qui n'apparaît pas dans l'autorisation ministérielle ainsi que lorsque des communications entre un avocat et son client ont été utilisées, analysées, conservées ou divulguées. J'ai aussi apprécié les détails additionnels sur l'identité des personnes au sein du CST qui ont accès à toute communication confidentielle recueillie.

76. En vue d'achever le dossier de cette décision, j'aimerais être informé, comme la ministre, lorsque le CST déploie des capacités d'atténuation sur le nuage pendant la période de validité de cette autorisation et lorsque le CST fournit des services de cybersécurité à de nouvelles institutions fédérales consentantes.

77. J'aimerais formuler trois autres remarques pour aider à l'examen et à la rédaction d'autorisations ministérielles futures. Ces observations ne modifient pas mes constatations concernant le caractère raisonnable des conclusions de la ministre.

i. Décision de l'ancien CR – [redacted]

78. Dans la demande de 2022-2023, le CST a demandé une autorisation ministérielle pour [description de l'activité] [redacted] Dans sa décision en date du 27 juin 2022, l'ancien commissaire au renseignement (ancien CR) n'avait pas approuvé cette activité. Il avait déterminé qu'il y avait un manque d'information dans les conclusions de la ministre et dans le dossier établissant comment l'activité autorisée est couverte par le paragraphe 27(1) de la *Loi sur le CST*.

79. Plus précisément, l'ancien CR a indiqué ce qui suit :

> Le libellé du paragraphe 27(1) ne prévoyait ni ne permettait, *prima facie* (à première vue), la délivrance d'une autorisation à l'extérieur de la portée consistant 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 est destinée ou y est stockée. Toutefois, la chef du CST a suggéré ce paragraphe dans la demande, et la ministre en a convenu, comme étant l'autorité législative pour l'activité autorisée [redacted]
>
> … la notion de [redacted] offre une protection plus étendue que la notion d'infrastructures de l'information des institutions fédérales trouvée dans la disposition susmentionnée.

80. Dans sa note de service adressée à la ministre en date du 28 avril 2023, la chef décrit la décision de l'ancien CR comme reflétant un oubli dans la rédaction législative. Bien que [redacted] de la *Loi sur le CST* exige du CST qu'il obtienne une autorisation ministérielle afin de [redacted], le paragraphe 27(1) de la *Loi sur le CST* ne reconnaît pas l'activité. La chef indique que les documents présentés à l'ancien commissaire au renseignement [traduction] « n'expliquaient pas suffisamment cette incongruité pour le convaincre que l'activité pouvait être autorisée. »

81. La chef renchérit que l'activité avait été incluse dans la demande de l'année précédente par excès de prudence. Elle visait à couvrir tout cas qui aurait pu déclencher le besoin d'obtenir une autorisation ministérielle. Ce serait un cas où [description de l'activité] [redacted]

82. Enfin, la chef indique que, suivant la décision de l'ancien CR, [traduction] « le programme de conformité du CST a depuis réalisé une analyse de [redacted] et, en collaboration avec l'avocat du ministère de la Justice du CST, a conclu que [redacted] Ainsi, l'activité a été retirée de l'autorisation actuelle qui m'a été présentée.

83. J'ai deux préoccupations importantes concernant l'explication donnée par le CST concernant cette importante question soulevée par l'ancien CR. Premièrement, lorsqu'une demande est présentée en vue d'obtenir une autorisation ministérielle relativement à une activité proposée, il incombe au CST de convaincre la ministre qu'il existe des motifs raisonnables de croire que, entre autres conditions, cette activité doit tout d'abord être nécessaire, puis raisonnable et proportionnelle. Cela pourrait comprendre l'obtention d'analyses de conformité adéquates et de conseils juridiques, qui devront par la suite être inclus dans les documents présentés à la ministre et moi-même s'ils s'avèrent nécessaires pour comprendre les enjeux.

84. En l'occurrence, il semblerait, d'après les explications fournies par la chef, qu'une analyse de conformité et la consultation d'un conseiller juridique ont eu lieu après que l'ancien CR n'a pas donné son aval afin que le CST [description de l'activité] [redacted]

85. Deuxièmement, d'après le dossier qui m'a été fourni, je suis incertain et perplexe quant à la raison pour laquelle l'activité en question, qui semble-t-il est actuellement menée, ne requiert plus une autorisation ministérielle. En effet, lorsqu'un décideur refuse une demande visant à mener une activité et apprend par la suite que l'activité en question est quand même menée, je m'attendrais à ce qu'une explication soit fournie dans le dossier, autre qu'un simple énoncé indiquant que le CST a obtenu un avis juridique surtout dans un contexte *ex parte*. Je me serais attendu à la même chose si l'ancien commissaire au renseignement avait autorisé l'activité et qu'au fil des ans, le CST avait changé de position et conclu que l'activité ne nécessitait plus une autorisation ministérielle.

86. En outre, et peut-être plus important encore, le fait de comprendre pourquoi des modifications ont été apportées aux demandes antérieures permet à la ministre et au commissaire au renseignement de mieux comprendre les activités autorisées.

ii. Effet des mesures d'atténuation sur les lois canadiennes et le droit au respect de la vie privée

87. Le dossier décrit un certain nombre de mesures d'atténuation que le CST peut prendre conformément à l'autorisation. Tel qu'il est indiqué, la chef est d'avis qu'il existait un risque que de telles mesures contreviennent à une loi fédérale. Les demandes futures bénéficieraient d'un dossier qui inclut plus d'information sur la façon dont les mesures d'atténuation proposées pourraient contrevenir aux lois canadiennes ou porter atteinte au droit à la vie privé des Canadiens ou des personnes se trouvant au Canada, le cas échéant.

iii. Période de conservation de l'information nécessaire et essentielle

88. L'ensemble des politiques sur la mission en matière de cybersécurité n'établit pas de période de conservation pour l'information nécessaire et essentielle, mais indique plutôt qu'elle doit être conservée [traduction] « selon les calendriers de conservation de l'organisation ». Il serait utile que des périodes de conservation précises soient établies dans le document évolutif ou que les calendriers organisationnels pertinents soient inclus dans une demande future.

89. Dans un autre ordre d'idées, les termes « essentielle » et « nécessaire » sont utilisés dans la *Loi sur le CST* relativement à différents types d'information. Je constate à la lecture du dossier que le CST leur donne la même interprétation. Quoiqu'il soit mineur, il pourrait s'agir d'un élément dont il faut tenir compte dans la prochaine révision législative de la *Loi de 2017 sur la sécurité nationale*.

iv. Le critère de conservation indiquant « jusqu'à ce que l'information ne soit plus utile à ces fins »

90. Comme je l'ai indiqué dans ma décision, le dossier ne traite aucunement des procédures en place pour examiner l'utilisation de l'information et supprimer toute information qui « n'est plus utile ». Aussi, il n'y a aucune mention de la fréquence des examens périodiques.

91. De l'information additionnelle portant sur les procédures en place et la fréquence d'examen de l'information pour déterminer si elle est toujours utile sur le plan opérationnel pour protéger les systèmes fédéraux serait pertinente afin que je sois entièrement convaincu que le CST conserve l'information concernant la vie privée conformément aux critères énoncés.

v. Références aux politiques sur la mission en matière de cybersécurité

92. À plusieurs reprises, le dossier fait référence aux politiques sur la mission en matière de cybersécurité — un document de plus de 100 pages, sans préciser les dispositions particulières de ces politiques. Dans les instances judiciaires et quasi judiciaires, il est pratique courante que de telles références soient fournies afin que le décideur ait une bonne compréhension du dossier. Dans l'avenir, j'aimerais que de telles références soient incluses.

V. CONCLUSIONS

93. D'après mon examen du dossier, je suis convaincu que les conclusions que la ministre a tirées au titre des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités énumérées au paragraphe 36 de l'autorisation sont raisonnables.

94. J'approuve donc, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, l'autorisation de cybersécurité pour des activités visant à protéger des infrastructures fédérales, délivrée par la ministre le 17 mai 2023.

95. Ainsi que le déclare la ministre et comme le dispose le paragraphe 36(1) de la *Loi sur le CST*, cette autorisation vient à expiration un an après le jour de mon approbation.

96. Comme le prescrit l'article 21 de la *Loi sur le CR*, une copie de la présente décision sera remise à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement afin de l'aider à réaliser son mandat au titre des alinéas 8(1)a) à c) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, LC 2019, c 13, art 2.

Le 13 juin 2023

(Original signé)

L'honorable Simon Noël, C.R.
Commissaire au renseignement