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

Dossier : 2200-B-2023-05

[TRADUCTION FRANÇAISE]

COMMISSAIRE AU RENSEIGNEMENT

DÉCISION ET MOTIFS

AFFAIRE INTÉRESSANT UNE AUTORISATION DE CYBERSÉCURITÉ POUR DES ACTIVITÉS SUR DES INFRASTRUCTURES NON FÉDÉRALES EN VERTU DU PARAGRAPHE 27(2) 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 3 NOVEMBRE 2023

TABLE DES MATIÈRES

I. APERÇU

1. Il s'agit d'une décision concernant les conclusions du ministre de la Défense nationale (le ministre) autorisant le Centre de la sécurité des télécommunications (CST) à aider à protéger l'information électronique et les infrastructures (c.-à-d. les systèmes, les dispositifs et les réseaux informatiques) appartenant à une entité non fédérale.

2. Le CST est l'organisme national du Canada en matière de cryptologie, et assure la cyberdéfense du gouvernement du Canada. Le CST a pour mandat d'assurer la sécurité des technologies de l'information du gouvernement contre les cybermenaces. Le mandat du CST s'étend à la protection des renseignements électroniques et de l'infrastructure des entités qui ne font pas partie du gouvernement du Canada lorsque les infrastructures non fédérales importantes pour le gouvernement ont été désignées comme telles.

3. Dans certaines situations, les activités de cybersécurité du CST peuvent contrevenir à certaines lois canadiennes. Par ailleurs, lorsqu'il obtient de l'information sur la cybersécurité liée à des activités malveillantes, le CST peut incidemment acquérir de l'information qui nuit à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.

4. Dans les situations où le CST souhaite mener des activités de cybersécurité qui dépassent les limites de la loi et qui empiètent sur les intérêts des Canadiens en matière de protection de la vie privée, il doit d'abord obtenir les autorisations requises. Le législateur a créé un régime comprenant une mise en balance afin de s'assurer que la nécessité de protéger les renseignements électroniques et les infrastructures d'importance ne l'emporte pas sur le respect des intérêts des Canadiens en matière de protection de la vie privée et la primauté du droit.

5. Le régime découle d'une demande écrite de la chef du CST (la chef) au ministre pour obtenir une autorisation de cybersécurité qui énonce les activités que le CST serait autorisé à mener. Le ministre peut délivrer l'autorisation de cybersécurité si, entre autres conditions, il conclut

que les activités proposées sont raisonnables et proportionnelles. Une autorisation de cybersécurité ne devient valide qu'après que le commissaire au renseignement l'a ensuite approuvée.

6. Le [redacted], en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*), le ministre a délivré une autorisation de cybersécurité relativement à des activités visant à aider à protéger des infrastructures non fédérales (l'autorisation).

7. Le [redacted], 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*).

8. Pour les motifs ci-après, je suis convaincu que les conclusions que le 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 54 de l'autorisation sont raisonnables.

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

II. CONTEXTE LÉGISLATIF

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

10. 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.

11. Le mandat du CST comprend la cybersécurité et l'assurance de l'information. Le libellé de l'article 17 de la *Loi sur le CST* dispose que le CST peut fournir des conseils, de l'orientation

et des services pour aider à protéger l'information électronique et les infrastructures appartenant aux institutions fédérales ainsi qu'aux entités qui ne font pas partie du gouvernement fédéral, mais sont d'importance pour le gouvernement du Canada et désignées comme telles par le ministre en vertu du paragraphe 21(1) de la *Loi sur le CST* (les systèmes qui ne relèvent pas du gouvernement fédéral), par exemple dans les secteurs de la santé, de l'énergie et des télécommunications.

12. Les entités non fédérales peuvent compter sur un certain nombre de services pour protéger leurs réseaux contre divers acteurs de cybermenaces sophistiqués, comme des moyens de protection offerts sur le marché (antivirus, logiciels pare-feu, etc.) et des entreprises tierces offrant des services de sécurité en matière de technologies de l'information. Néanmoins, le législateur estime que l'expertise du CST pourrait s'avérer nécessaire pour protéger les secteurs d'importance pour le gouvernement du Canada.

13. Pour comprendre les points d'entrée vulnérables et les atteintes à l'intégrité des systèmes non fédéraux, le CST pourrait devoir accéder aux systèmes et acquérir de l'information. Ces activités, menées dans le but de protéger le système en question, pourraient néanmoins contrevenir à certaines lois et porter atteinte à l'attente raisonnable de protection en matière de vie privée des Canadiens et des personnes se trouvant au Canada. La *Loi sur le CST* exige une autorisation ministérielle, approuvée par la suite par le commissaire au renseignement, chaque fois que les activités de cybersécurité du CST contreviennent à une loi fédérale ou entraînent l'acquisition de renseignements qui nuisent à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada (paragraphes 22(4) et 27(2) de la *Loi sur le CST*). La *Loi sur le CST* établit le processus que doit suivre le CST pour obtenir une autorisation de cybersécurité.

14. Le propriétaire ou l'opérateur des systèmes non fédéraux doit amorcer le processus en demandant par écrit au CST de mener des activités de cybersécurité pour protéger les systèmes et leurs renseignements électroniques (paragraphe 33(3) de la *Loi sur le CST*). La chef doit ensuite présenter au ministre une demande écrite énonçant les faits qui lui permettraient de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire (paragraphe 33(2) de la *Loi sur le CST*). Les paragraphes 34(1) et (3) de la *Loi sur*

le CST définissent les conditions légales pour que le ministre puisse délivrer une autorisation de cybersécurité. 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 entreprendre les activités autorisées qui sont précisées dans l'autorisation.

15. Conformément au paragraphe 27(2) de la *Loi sur le CST*, le ministre peut, en vertu d'une autorisation de cybersécurité, autoriser le CST à acquérir de l'information qui provient ou passe par ces systèmes non fédéraux, qui leur est destinée ou y est stockée afin d'aider à les protéger, dans les cas visés à l'alinéa 184(2)e) du *Code criminel*, LRC 1985, c C-46, contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement. L'alinéa 184(2)e) du *Code criminel* s'applique généralement aux personnes qui gèrent la qualité du service d'un système informatique ou sa protection.

16. Le CST peut utiliser les renseignements acquis dans le cadre de l'aspect cybersécurité et assurance de l'information de son mandat pour faire en sorte de mener des activités dans le cadre d'autres aspects de son mandat, pourvu que toute restriction imposée à l'information soit respectée.

17. Malgré toute autorisation de cybersécurité, la *Loi sur le CST* impose des limites aux activités du CST. Celui-ci doit s'abstenir de mener quelque activité que ce soit visant un Canadien ou une personne se trouvant au Canada ou de contrevenir à la *Charte canadienne des droits et libertés* (la *Charte*) (paragraphe 22(1) de la *Loi sur le CST*). Toutefois, comme il est impossible pour le CST de déterminer à l'avance quels renseignements sont nécessaires, le CST peut incidemment acquérir des renseignements concernant un Canadien ou une personne se trouvant au Canada. Le mot « incidemment » signifie que l'information acquise n'a pas été délibérément recherchée (paragraphe 23(5) de la *Loi sur le CST*).

18. Dans le contexte d'une autorisation de cybersécurité, le CST explique que les renseignements relatifs à un Canadien ou à une personne se trouvant au Canada qui peuvent être acquis incidemment comprennent notamment les renseignements personnels au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21, les

communications entre un avocat et son client, les renseignements commerciaux (propriété intellectuelle, secrets commerciaux, etc.), le nom de domaine, l'adresse électronique et l'adresse IP. Il peut également s'agir de communications privées qui commencent et se terminent au Canada, et dont l'auteur a une attente raisonnable de protection en matière de vie privée. Je remarque que, bien que l'interception de communications privées constitue une infraction criminelle, l'article 50 de la *Loi sur le CST* prévoit une exemption et dispose que la partie VI du *Code criminel* (Atteinte à la vie privée) ne s'applique pas à l'interception d'une communication autorisée par le ministre.

19. En cas de telle interception de communication, il faut suivre des mesures législatives et politiques strictes pour utiliser, analyser et conserver cette information. En effet, 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 dans l'utilisation, l'analyse, la conservation et la divulgation de l'information qui se rapporte à eux (article 24 de la *Loi sur le CST*).

B. La *Loi sur le commissaire au renseignement*

20. 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 du ministre en vertu desquelles certaines autorisations sont délivrées, pour déterminer si ces conclusions sont raisonnables.

21. L'article 14 de la *Loi sur le CR* précise que, dans le cas d'une autorisation de cybersécurité, le commissaire au renseignement examine les conclusions que le ministre a tirées au titre des paragraphes 34(1) et (3) de la *Loi sur le CST*.

22. Le ministre est tenu par la loi de fournir au commissaire au renseignement tous les renseignements dont il disposait en tant que décideur (article 23 de la *Loi sur le CR*). Comme l'établit la jurisprudence du commissaire au renseignement, cette obligation vise tout renseignement verbal consigné par écrit, y compris les notes d'information ministérielles. Le commissaire au renseignement n'a cependant pas droit aux documents confidentiels du Cabinet (article 26 de la *Loi sur le CR*).

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

    a) la lettre du ministre adressée au commissaire au renseignement (non datée);
    b) l'autorisation ministérielle datée du [redacted];
    c) la note d'information de la chef du CST adressée au ministre, datée du [redacted];
    d) la demande de la chef, datée du [redacted], accompagnée de sept annexes, lesquelles comprennent notamment :
        i. la lettre de demande de l'entité non fédérale, datée du [redacted];
        ii. l'Ensemble des politiques sur la mission en matière de cybersécurité (les politiques sur la mission), approuvé le 28 février 2022;
        iii. deux arrêtés ministériels et
    e) le document intitulé Présentation sommaire – aperçu des activités].

III. LA NORME DE CONTRÔLE

24. La *Loi sur le CR* exige que le commissaire au renseignement examine si les conclusions du ministre sont raisonnables. La jurisprudence du commissaire au renseignement établit que la norme de la décision raisonnable qui s'applique au contrôle judiciaire d'un acte administratif est la même que celle qui s'applique aux examens menés par le commissaire au renseignement.

25. Dans le cadre d'un examen selon la norme de la décision raisonnable, la cour de révision doit commencer son analyse à partir des motifs du décideur administratif (*Mason c Canada (Citoyenneté et Immigration)*, 2023 CSC 21 au para 79). 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.

26. Les contraintes factuelles et juridiques pertinentes incluent le régime législatif applicable, les répercussions de la décision et les principes d'interprétation des lois. En fait, pour comprendre ce qui est raisonnable, il faut prendre en considération le contexte dans lequel la décision faisant l'objet de l'examen a été prise ainsi que le contexte dans lequel elle est examinée. Il faut donc 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*.

27. Un examen de la *Loi sur le CR* et de la *Loi sur le CST*, de même que les débats législatifs, montrent que le législateur a créé le rôle de commissaire au renseignement afin qu'il serve de mécanisme indépendant permettant d'assurer un juste équilibre entre les mesures prises par le gouvernement à des fins de sécurité nationale ainsi que le respect de la primauté du droit et des droits et libertés des Canadiens. Pour maintenir cet équilibre, je considère que le législateur m'a attribué un rôle de gardien et de surveillant des autorisations ministérielles.

28. Lorsque le commissaire au renseignement est convaincu que les conclusions en cause du ministre sont raisonnables, il « approuve » l'autorisation (alinéa 20(1)a) de la *Loi sur le CR*). À l'inverse, lorsque ces conclusions sont déraisonnables, le commissaire « n'approuve pas » l'autorisation (alinéa 20(1)b) de la *Loi sur le CR*).

29. La décision du commissaire au renseignement peut faire l'objet d'un contrôle judiciaire par la Cour fédérale sur présentation d'une demande en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*, LRC, 1985, c F-7.

IV. ANALYSE

30. Le [redacted], la chef a transmis au ministre une demande écrite d'autorisation de cybersécurité relativement à des activités visant à protéger des infrastructures non fédérales

(la demande) dans le cadre de son mandat. [redacted]

31. L'entité non fédérale en question est d'importance pour le gouvernement du Canada, au sens de l'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada*, émis le 25 août 2020. Une description de l'entité non fédérale, ainsi que des activités précisées dans l'autorisation, figure à l'annexe de la présente décision (annexe A), laquelle n'est pas destinée à la diffusion publique. L'inclusion de ces renseignements dans l'annexe facilite la lecture de la future version publique de la présente décision et garantit qu'elle contient la nature des faits qui me sont relatés, ce qui, autrement, ne serait possible qu'en consultant le dossier.

32. En résumé, les activités proposées consistent à déployer [redacted] sur les systèmes de l'entité non fédérale. [Description de l'activité [redacted] acquises au moyen des systèmes. [redacted]

33. Compte tenu de ces faits dans la demande, le ministre a conclu que les conditions prévues aux paragraphes 34(1) et (3) de la *Loi sur le CST* étaient respectées, puis a délivré l'autorisation. Je dois maintenant déterminer si les conclusions du ministre sont raisonnables.

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

i. Déterminer si les activités sont raisonnables et proportionnelles

34. Selon le paragraphe 34(1) de la *Loi sur le CST*, pour que le ministre délivre une autorisation de cybersécurité, il 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 ».

35. Déterminer si une activité est « raisonnable » diffère de l'examen selon la norme de la « décision raisonnable » effectué par le commissaire au renseignement. Le ministre doit conclure que toute activité qui serait permise par l'autorisation est raisonnable et proportionnelle en appliquant sa compréhension de ce que ces seuils impliquent. Déterminer si une activité est raisonnable et proportionnelle constitue un exercice contextuel, et le ministre peut tenir compte d'un certain nombre de facteurs. Néanmoins, je suis d'avis que la compréhension des deux seuils doit refléter au minimum certains éléments fondamentaux. Une activité raisonnable doit être autorisée par la loi et avoir un lien rationnel avec ses objectifs. Quant à la nature « proportionnelle », il s'agit d'équilibrer les intérêts en jeu, ce qui, dans le contexte d'une autorisation de cybersécurité, inclura la protection des systèmes et l'incidence sur les intérêts des Canadiens en matière de protection de la vie privée.

36. Le commissaire au renseignement détermine si les conclusions du ministre, lesquelles comprennent sa compréhension des seuils, sont « raisonnables », en procédant à un examen quasi judiciaire selon la norme de décision raisonnable, expliquée précédemment.

ii. Examen des conclusions du ministre selon lesquelles les activités en cause sont raisonnables

37. Le ministre a conclu, au paragraphe 20 de l'autorisation, qu'il avait [TRADUCTION] « des motifs raisonnables de croire que les activités autorisées dans l'autorisation sont

raisonnables, compte tenu de l'objectif de protéger les systèmes non fédéraux contre les méfaits, l'utilisation non autorisée ou la perturbation ».

38. La délivrance de l'autorisation reflète la conclusion du ministre voulant que, même si les activités permettaient au CST d'accéder à des systèmes situés au Canada, elles ne contreviennent pas à l'interdiction législative de mener des activités du CST ciblant des Canadiens ou des personnes se trouvant au Canada. Les politiques sur la mission, approuvées le 28 février 2022 — l'ensemble des principes et des exigences stratégiques visant à guider le personnel du CST travaillant dans le cadre de l'aspect cybersécurité du mandat du CST — énonce que les activités de cybersécurité ne visent pas les personnes physiques, à condition qu'elles mettent l'accent sur la cybermenace qui pèse sur le système. Le point de vue du CST sur cette question et, par conséquent, la conclusion du ministre, me semblent raisonnables. En effet, le mandat du CST en matière de cybersécurité et d'assurance de l'information ne peut être rempli qu'en accédant à des systèmes au Canada. Je suis également convaincu que le dossier montre que le ministre a raison de conclure implicitement que les activités de cybersécurité énoncées dans l'autorisation sont axées sur la cybermenace, et non sur des personnes.

39. Le ministre avance deux arguments pour faire valoir que les activités sont raisonnables. Premièrement, le ministre explique qu'il est raisonnable que le CST participe à l'intervention en matière de cybersécurité. [redacted] selon les renseignements fournis par la chef, le ministre signale que les systèmes de l'entité non fédérale [redacted]. Par conséquent, le ministre conclut que l'état actuel de la situation des systèmes d'information en matière de cybersécurité n'est pas suffisamment développé pour [redacted] En effet, le ministre explique que [description de l'activité] [redacted]

40. La justification du ministre établit en termes généraux la suite des interventions du CST, ajoutant qu'il a [redacted] à l'entité non fédérale pour établir et sécuriser sa situation en matière de cybersécurité. Il explique que [redacted]

41. Deuxièmement, le ministre explique que les activités pour lesquelles une approbation est demandée dans l'autorisation sont raisonnables, parce que ces activités permettraient au CST de repérer et de mieux comprendre les cyberactivités malveillantes ou d'autres indicateurs d'atteintes, pour ainsi conseiller l'entité fédérale sur la façon de protéger ses systèmes et de prendre des mesures d'atténuation [redacted], ainsi que sur la façon de fournir des renseignements susceptibles d'aider à protéger les systèmes fédéraux et d'autres systèmes d'importance. Essentiellement, les activités seraient raisonnables, car elles seraient efficaces.

42. Le ministre s'appuie sur la demande de la chef pour tirer des conclusions sur l'état des systèmes de l'entité non fédérale ainsi que sur l'efficacité des activités de cybersécurité proposées. J'estime que cela est raisonnable. Je ne m'attends pas à ce que le ministre détienne cette expertise; ce n'est d'ailleurs pas son rôle. En effet, la *Loi sur le CST* dispose expressément que la demande de la chef « expose les faits qui permettraient au ministre de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions de sa délivrance sont remplies » (paragraphe 33(2) de la *Loi sur le CST*). Néanmoins, une conclusion ministérielle raisonnable dans le cadre de l'autorisation doit être justifiée et intelligible (*Vavilov,* para 99), ce qui signifie que même lorsque le ministre fait siennes les conclusions de la chef, il doit démontrer qu'il comprend les raisons qui justifient ses conclusions.

43. Je suis d'avis que les conclusions du ministre témoignent de cette compréhension. Ses conclusions indiquent qu'il a tenu compte des besoins actuels de l'entité non fédérale et des activités proposées du CST, et qu'il en était satisfait. Il existe un lien rationnel clair entre les activités de cybersécurité proposées par le CST et leur objectif, lequel consiste à aider à protéger les infrastructures non fédérales — bien que je soulève que le dossier aurait pu

fournir des détails supplémentaires sur le lien entre [redacted] Il est également évident, à l'examen du dossier, que les activités de cybersécurité sont fondées et qu'elles aident à remplir le mandat du CST en matière de cybersécurité et d'assurance de l'information quant à l'entité non fédérale. Compte tenu de la nature de l'objectif et des renseignements figurant au dossier concernant la nature des activités, j'estime raisonnable la conclusion du ministre lorsqu'il qualifie les activités de raisonnables.

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

44. Le ministre a conclu, au paragraphe 30 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités autorisées sont : [TRADUCTION] « proportionnelles compte tenu de la façon dont elles sont menées et parce qu'elles sont liées de façon rationnelle à l'objectif et portent une atteinte minimale aux droits et libertés des tiers ».

45. Les activités pour lesquelles une autorisation est demandée permettraient au CST d'acquérir un grand volume d'information générée par l'entité non fédérale ou résidant avec elle. En effet, l'efficacité des activités repose sur l'acquisition d'un grand volume d'information. Le ministre explique donc que les mesures et les contrôles en place rendent les activités proportionnelles, car ils aident à s'assurer que le CST utilise et conserve seulement l'information nécessaire ou essentielle pour protéger les systèmes non fédéraux et protéger toute information qui pourrait toucher un intérêt des Canadiens en matière de protection de la vie privée. Les notions du caractère nécessaire et essentiel sont analysées ci-après dans cette décision.

46. Le ministre présente les mesures et les contrôles énumérés ci-dessous pour démontrer que les activités sont proportionnelles :

    a) seule l'information nécessaire pour protéger les systèmes sera recueillie;

b) les renseignements ne sont conservés que s'ils sont considérés comme nécessaires pour découvrir, isoler, prévenir ou atténuer les dommages causés au système, aux systèmes fédéraux et aux autres systèmes d'importance;
c) les renseignements qui portent sur un Canadien ou sur une personne se trouvant au Canada ne sont conservés que s'ils sont jugés essentiels pour découvrir, isoler, prévenir ou atténuer les dommages causés au système, aux systèmes fédéraux et aux autres systèmes d'importance;
d) les renseignements non évalués ne sont pas conservés plus de [redacted];
e) la plupart des analyses et des mesures d'atténuation sont effectuées au moyen de processus automatisés qui limitent l'accès des employés du CST à l'information;
f) l'accès aux renseignements acquis en vertu de l'autorisation est réservé aux employés autorisés du CST qui ont reçu la formation appropriée et qui ont besoin de les connaître pour accomplir leurs fonctions;
g) tous les renseignements sont protégés conformément à Les politiques sur la mission;
h) chaque recherche effectuée sur les renseignements non évalués acquis est vérifiable conformément aux politiques sur la mission et aux autres politiques organisationnelles;
i) la technologie utilisée est sujette à un contrôle de conformité aux lois et aux politiques.

47. Je remarque que les mesures énoncées aux points a) à d) reflètent essentiellement les exigences énoncées au paragraphe 34(3) de la *Loi sur le CST* et qui s'appliquent aux autorisations de cybersécurité. Je ne crois pas qu'il soit particulièrement utile pour le ministre de justifier qu'une condition légale a été satisfaite — en l'espèce, que les activités sont proportionnelles — en s'appuyant sur la satisfaction de conditions légales distinctes ((telles qu'énoncées aux alinéas 34(3)a) et aux sous-alinéas 34(3)c)(ii) et d)(ii)) qui doivent elles-mêmes être satisfaites de façon indépendante.

48. Par ailleurs, je fais observer que l'élément c) énonce que les renseignements liés au Canada peuvent être conservés lorsqu'ils sont essentiels à la protection de l'entité non fédérale ou

d'autres systèmes et systèmes d'importance fédéraux, mais que le sous-alinéa 34(3)d)(ii) de la *Loi sur le CST* limite la conservation de renseignements liés au Canada dans le but de protéger les systèmes désignés, au sens du paragraphe 21(1), comme étant d'importance pour le gouvernement du Canada dans le cas des autorisations délivrées en vertu du paragraphe 27(2). Je reconnais que les renseignements acquis et conservés en vertu de la présente autorisation pourraient servir à d'autres aspects du mandat du CST, mais je souligne que la conservation initiale doit respecter les exigences législatives.

49. En ce qui concerne certaines des autres mesures, le dossier manque de renseignements précis. Premièrement, bien que [TRADUCTION] « la majeure partie de l'analyse » soit effectuée au moyen de processus automatisés qui limitent l'accès des employés, rien ne précise les éléments de l'analyse qui sont menés par les employés. Le ministre et moi-même, en tant que commissaire au renseignement, devrions comprendre les éléments non informatisés de l'analyse, surtout s'il s'agit de l'information la plus susceptible de toucher un intérêt en matière de protection de la vie privée. Il s'agit de renseignements importants pour établir le caractère proportionnel des activités.

50. Deuxièmement, même si on a déclaré que les activités permettraient d'acquérir et d'utiliser seulement l'information nécessaire pour aider à protéger les systèmes de l'entité non fédérale, je constate que les conclusions du ministre et le dossier, dans son ensemble, ne précisent pas le type d'information acquise. La demande de la chef décrit des catégories de renseignements qui seraient recueillis en vertu de l'autorisation et qui ne semblent pas soulever des enjeux en matière de protection de la vie privée. Toutefois, la demande explique également que le CST peut acquérir incidemment des renseignements qui risquent de nuire à une attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada, [types d'information] [redacted] Dans la demande, il est expliqué que ces renseignements sont [redacted] Je comprends que le CST ne s'intéresse pas au contenu des renseignements pour lesquels il existe une attente raisonnable en matière de protection de la vie privée [redacted], mais plutôt dans ce qu'il peut révéler au sujet [redacted] — et que les renseignements ne seront conservés que lorsqu'il est essentiel de protéger les systèmes de l'entité non fédérale.

Néanmoins, étant donné que l'acquisition de renseignements est automatisée, il n'est pas établi à quel moment des renseignements canadiens connexes seront recueillis incidemment.

51. Toutefois, je ne crois pas que l'absence de détails soit fatale au caractère raisonnable des conclusions du ministre. Je suis d'avis que l'appui du ministre sur les mesures et les contrôles en place, à l'exception des mesures qui reflètent les exigences du paragraphe 34(3), étaye sa conclusion selon laquelle les activités sont proportionnelles. De plus, les conclusions du ministre reflètent clairement sa compréhension que les activités de cybersécurité particulières permettant d'obtenir de l'information sont nécessaires pour atteindre l'objectif de protection du système. Dans la mesure où des renseignements pouvant contenir un élément lié à un intérêt des Canadiens en matière de protection de la vie privée seraient acquis et conservés, l'accès à ces renseignements et leur utilisation seraient limités.

52. En ce qui concerne les lois canadiennes susceptibles d'être enfreintes, l'autorisation mentionne que leur nombre est limité, car le CST mènerait ses activités uniquement sur les systèmes pour lesquels il a reçu le consentement exprès du propriétaire de l'infrastructure non fédérale. Étant donné que le CST détiendra le consentement requis pour accéder aux systèmes, le risque d'éventuelles infractions aux lois canadiennes est très peu élevé. En cas de violation d'une loi fédérale, ses répercussions seront limitées et, en cas de contravention à une loi fédérale qui ne figure pas dans la demande de la chef, cette dernière en informera le ministre et le commissaire au renseignement.

53. La section 5.3 des politiques sur la mission, approuvées le 28 février 2022 — l'ensemble des principes et des exigences stratégiques visant à guider le personnel du CST travaillant dans le cadre de l'aspect cybersécurité du mandat du CST — énonce que le CST peut démontrer la nécessité, ainsi que le caractère raisonnable et proportionnel de ses activités de cybersécurité au moyen de mesures appliquées dans la collecte, l'utilisation, l'analyse, la conservation et dans la transmission de l'information. En ce qui concerne la proportionnalité des activités, les politiques disent ceci : [TRADUCTION] « utiliser et analyser l'information conservée de manière à assurer la proportionnalité de la démarche par rapport à l'objectif (p. ex. utiliser les méthodes les moins intrusives possibles, équilibrer les besoins logistiques avec les droits à la

protection de la vie privée des Canadiens et des personnes se trouvant au Canada) ». Je suis d'avis que cet équilibre a été réalisé.

54. En somme, le dossier révèle que le ministre savait que les activités permettraient d'obtenir un grand volume d'information. Il a estimé que, compte tenu de l'objectif des activités, de la nature de l'information acquise et des mesures en place pour limiter l'accès à l'information, l'équilibre militait en faveur de permettre au CST de mener les activités évoquées. Je conclus que le ministre a suffisamment justifié ses conclusions et qu'elles sont appuyées par le dossier. Par conséquent, je suis convaincu que les conclusions du ministre concernant la proportionnalité des activités sont raisonnables.

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

55. Le paragraphe 34(3) de la *Loi sur le CST* prévoit que le ministre peut délivrer une autorisation de cybersécurité seulement s'il conclut qu'il y a des motifs raisonnables de croire que les trois 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) l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux; et
>
> c) 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 systèmes non fédéraux.

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

56. L'autorisation décrit en quoi l'information évaluée aux fins de la protection de systèmes non 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*. Le dossier comprend un calendrier de conservation des différentes catégories de

renseignements à acquérir. Au paragraphe 31, le ministre conclut qu'il a des motifs raisonnables de croire que le CST ne conservera pas les renseignements plus longtemps que ce qui est raisonnablement nécessaire pour réaliser l'aspect de cybersécurité de son mandat. Je remarque que la chef écrit, dans la demande, que l'entité non fédérale peut, en tout temps, demander au CST de supprimer les renseignements qu'il a acquis à partir ou par l'intermédiaire de ses systèmes.

57. Étant donné qu'il n'est pas possible pour le CST de déterminer à l'avance les renseignements dont il a besoin, l'efficacité de ses activités dépend de l'évaluation, [redacted] du volume important d'information qu'il acquiert. L'objectif consiste à évaluer l'information acquise sans retard important afin de mieux comprendre et de retenir l'information utile. Toutefois, étant donné que certaines atteintes peuvent être repérées seulement après le début d'une activité malveillante, l'efficacité des activités du CST dépend également de la capacité d'évaluer l'information déjà acquise.

58. Le ministre explique qu'une période de conservation de [redacted] constitue une [TRADUCTION] « période d'analyse raisonnable » qui donne au CST le temps de remonter aux origines d'un événement cybernétique et d'examiner son évolution au fil du temps. Il permet également au CST de comparer les nouvelles vulnérabilités par rapport à ses renseignements non évalués et de déterminer si elles existent au sein des réseaux fédéraux du gouvernement du Canada et d'autres systèmes d'importance. Après une période de [redacted], les renseignements seront automatiquement supprimés, sauf s'ils sont jugés nécessaires ou essentiels pour aider à protéger les systèmes de l'entité non fédérale, les systèmes fédéraux ou les autres systèmes d'importance.

59. Le critère du caractère « nécessaire » s'applique aux renseignements qui ne concernent pas un Canadien ou une personne se trouvant au Canada. Comme il est écrit dans l'autorisation et la section des définitions des politiques sur la mission, l'information est jugée nécessaire lorsqu'elle est requise pour comprendre les activités cybernétiques malveillantes, y compris les tendances de comportement, les capacités, les intentions ou les tendances de vulnérabilité, pour aider à protéger les institutions fédérales et les systèmes non fédéraux d'importance.

60. Pour sa part, le critère du caractère [TRADUCTION] « essentiel » défini dans l'autorisation et la section des définitions des politiques sur la mission s'applique aux renseignements acquis incidemment au sujet d'un Canadien ou d'une personne se trouvant au Canada. L'information est jugée essentielle lorsque, sans elle, le CST ne serait pas en mesure de protéger les systèmes non fédéraux d'importance, les institutions fédérales et l'information électronique qui s'y trouve. Les renseignements au sujet de Canadiens qui sont conservés font l'objet d'un suivi interne au CST, conformément aux exigences stratégiques énoncées tout au long des politiques sur la mission.

61. Selon le tableau de conservation et suppression (« *Retention and Disposition Table* ») que comporte le dossier, les renseignements jugés nécessaires ou essentiels peuvent être conservés [TRADUCTION] « jusqu'à ce qu'ils ne soient plus utiles à ces fins, ou à moins de restrictions imposées par le client ». Je comprends que le critère [TRADUCTION] « jusqu'à ce qu'ils ne soient plus utiles » signifie que les renseignements pourraient être utiles indéfiniment, mais qu'ils ne seront plus conservés lorsque leur utilité à ces fins cessera.

62. En ce qui concerne les renseignements qui sont jugés « essentiels » et qui portent sur un Canadien ou sur une personne se trouvant au Canada, les gestionnaires de l'exploitation doivent examiner les renseignements sur une base trimestrielle afin de déterminer s'ils sont toujours essentiels. Les renseignements qui ne sont plus essentiels doivent être supprimés. Le dossier n'indique pas que le CST effectue des examens périodiques des renseignements qui ont été jugés « nécessaires ».

63. Compte tenu des importantes restrictions à l'accès à l'information non évaluée et du fait que les cyberactivités malveillantes ne peuvent être détectées qu'après le passage du temps, j'estime raisonnable la conclusion du ministre concernant la période d'évaluation de [redacted]. Cependant, je remarque que, dans une décision antérieure concernant les infrastructures non fédérales, j'ai demandé que le CST fournisse des exemples concrets pour appuyer son explication de la conservation de l'information non évaluée pendant [redacted]. Le fondement logistique de ce qui constitue une [TRADUCTION] « période d'analyse raisonnable » devrait être établi plus clairement pour le ministre et moi-même. Mon

commentaire n'est que renforcé, puisque le CST mène [redacted]

64. Je suis également d'accord avec le ministre lorsqu'il conclut que les renseignements qui sont nécessaires ou essentiels pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes non fédéraux peuvent être conservés jusqu'à ce qu'ils ne soient plus utiles ou à moins d'une directive imposée par l'entité non fédérale, dans la mesure où un examen périodique est mené sur les renseignements au sujet de Canadiens et de personnes se trouvant au Canada. Il est justifié de conserver l'information pendant le temps nécessaire pour réagir à cette menace.

ii. Toute information acquise est nécessaire pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes de l'entité non fédérale

65. Grâce à ses solutions de cybersécurité, le CST obtient un accès étendu aux infrastructures d'information de l'entité non fédérale pour la détection et l'analyse plus poussée des activités anormales. Les conclusions du ministre expliquent comment [description de comment l'information est nécessaire] [redacted] Il n'est pas possible pour le CST de prédire [redacted] Par conséquent, le CST doit acquérir la vaste gamme de renseignements [redacted]

66. Le ministre explique que toute information acquise sera utilisée par les processus automatisés du CST pour aider à repérer les activités malveillantes. Les activités de cybersécurité ne seront efficaces qu'avec l'acquisition de l'information. Le ministre fournit des exemples qui montrent comment les renseignements obtenus en vertu de l'autorisation sont nécessaires pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes non fédéraux. Pour ces motifs, je conclus que les conclusions du ministre sont raisonnables.

iii. Les mesures en place font en sorte que les renseignements recueillis sur des Canadiens ou des personnes se trouvant au Canada seront utilisés, analysés ou conservés seulement s'ils sont essentiels pour isoler, prévenir ou atténuer des dommages causés aux systèmes de l'entité non fédérale

67. Comme il a été mentionné précédemment, dans le cadre de ses activités de cybersécurité, le CST peut acquérir incidemment des renseignements au sujet d'un Canadien ou d'une personne se trouvant au Canada, ce qui pourrait porter atteinte à une attente raisonnable en matière de protection de la vie privée. L'article 24 de la *Loi sur le CST* exige que le CST mette en place des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada lorsqu'il utilise, analyse, conserve et divulgue des renseignements à leur sujet acquis dans le cadre des aspects de son mandat de cybersécurité et d'assurance de l'information. Au paragraphe 45 de l'autorisation, le ministre conclut qu'il a des motifs raisonnables de croire que les mesures requises à l'article 24 sont en place.

68. Le ministre précise que l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada ne peut être conservée que si elle est jugée essentielle. Cette condition est également énoncée dans les politiques de la mission. 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 de l'entité non fédérale, aux systèmes fédéraux et aux autres systèmes d'importance. Je suis d'avis que la compréhension du terme « essentiel » du CST est raisonnable.

69. La section 8.2.2 des politiques de la mission énonce qu'un employé autorisé du CST applique le [TRADUCTION] « critère du caractère essentiel » des renseignements obtenus. Cette analyse s'effectue au moyen de processus manuels ou automatisés. L'employé doit fournir des justifications lorsqu'il croit que des renseignements sont essentiels. À mon avis, cette mesure contribue au respect de l'obligation prévue dans la loi. Je reviendrai à la question des justifications du caractère essentiel dans mes remarques.

70. Les conclusions du ministre précisent que l'accès aux renseignements non évalués acquis en vertu de l'autorisation est limité aux employés autorisés du CST qui sont dûment accrédités pour mener des activités de cybersécurité et qui ont reçu la formation obligatoire sur les procédures de traitement de l'information. De plus, la majeure partie de l'analyse de l'information se fait au moyen de processus automatisés, ce qui limite l'accès des employés à l'information non évaluée.

71. La conclusion du ministre et le dossier expliquent également comment les renseignements concernant des Canadiens ou des personnes se trouvant au Canada peuvent être divulgués, ce qui correspond à l'obligation énoncée à l'article 44 de la *Loi sur le CST*. Les renseignements ne sont divulgués qu'aux personnes ou catégories de personnes désignées dans l'[TRADUCTION] *Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu de l'aspect de cybersécurité et de l'assurance de l'information du mandat du CST* émis le 13 juin 2023 en vertu de l'article 45 de la *Loi sur le CST* [description de personnes ou de catégories de personnes] [redacted] Pour recevoir des renseignements communiqués par le CST qui concernent un Canadien ou une personne se trouvant au Canada, ces renseignements doivent être nécessaires pour aider à protéger l'information électronique ou l'infrastructure d'information de l'entité non fédérale.

72. Les communications privées canadiennes, [redacted], qui sont acquises incidemment, sont comptabilisées dans les rapports de fin d'autorisation à l'intention du ministre, dont une copie est transmise au commissaire au renseignement, en application de l'article 52 de la *Loi sur le CST* (rapport présenté au titre de l'article 52). Le plus récent rapport présenté au titre de l'article 52 montre qu'aucune communication de ce type n'a été acquise, conservée ou transmise.

73. Compte tenu de ce qui précède, je suis d'avis que le dossier montre que la politique et les pratiques du CST prennent au sérieux la conservation, l'analyse et l'utilisation des

renseignements portant sur des Canadiens ou sur des personnes se trouvant au Canada. Les politiques et les pratiques appuient les conclusions du ministre selon lesquelles les renseignements au sujet de Canadiens ou de personnes se trouvant au Canada ne seront utilisés, analysés ou conservés que s'ils sont essentiels pour découvrir, isoler, prévenir ou atténuer les dommages causés aux systèmes de l'entité non fédérale. J'estime que les conclusions du ministre à cet effet sont raisonnables.

V. REMARQUES

74. Bien que je sois convaincu que les conclusions du ministre sont raisonnables, j'aimerais formuler quatre remarques pour faciliter l'examen et la rédaction des futures autorisations ministérielles. Ces remarques ne modifient pas mes conclusions concernant le caractère raisonnable des conclusions du ministre.

i. Les renseignements au sujet de Canadiens ou de personnes se trouvant au Canada

75. Bien que le dossier fait état de types de renseignements portant sur un Canadien ou sur une personne se trouvant au Canada et qui pourraient être acquis incidemment et conservés par la suite, aucune information ne précise les renseignements qui ont été effectivement conservés. Comme il a été mentionné précédemment, le CST consigne les justifications du caractère essentiel, mais aucune information à ce sujet n'est fournie au ministre. [redacted] et je suis d'avis que le CST devrait avoir une bonne compréhension de la nature et du volume de l'information qui est conservée et utilisée, particulièrement en ce qui concerne les renseignements portant sur un Canadien ou sur une personne se trouvant au Canada. Cette compréhension devrait être encore plus solide lorsque le CST met en œuvre les [redacted]

76. Je m'attendrais à ce que le CST nous fournisse, au ministre et à moi-même, une meilleure compréhension de la nature, de la fréquence et du volume de la conservation de l'information lorsque des intérêts des Canadiens en matière de protection de la vie privée sont en jeu. En

effet, le CST devrait fournir ces renseignements chaque fois [redacted]. La façon dont les activités ont [redacted] peut constituer un facteur pour déterminer si une activité est raisonnable et proportionnelle.

77. Je m'attends également à ce que ces renseignements figurent dans le rapport présenté au ministre au titre de l'article 52 dans les 90 jours suivant la dernière période de validité de l'autorisation. Je reconnais qu'il contient le nombre de communications privées interceptées et de communications entre un avocat et son client. Cependant, les préoccupations des Canadiens en matière de protection de la vie privée dans le contexte de la cybersécurité vont au-delà de ces deux catégories. Enfin, si les renseignements à figurer à l'avenir dans le rapport présenté au titre de l'article 52 sont connus lorsque la chef présente une demande au ministre pour les mêmes activités, je suis d'avis que le ministre et moi-même devrions les recevoir afin que nous puissions mieux comprendre les répercussions réelles sur les intérêts des Canadiens en matière de protection de la vie privée.

ii. Références aux politiques de la mission en matière de cybersécurité

78. J'estime qu'il est nécessaire de réitérer une remarque faite dans ma décision dans le dossier 2200-B-2023-02, rendue le 13 juin 2023. À plusieurs reprises, le dossier fait référence aux politiques de la mission — un document de plus de 100 pages, mais sans renvoyer aux dispositions particulières de la politique. Dans les instances judiciaires et quasi judiciaires, en particulier lorsqu'il n'y a pas d'audience, il faut inclure dans la documentation écrite un renvoi aux dispositions précises des lois et des politiques afin de permettre au décideur de bien comprendre la question dont il est saisi. Je demande que cette pratique soit suivie dans les dossiers futurs.

79. De plus, cette version des politiques de la mission a subi plusieurs modifications par rapport à la version précédente qui figure dans l'autorisation de l'an dernier. Je demande que, dans les dossiers à venir, les modifications pertinentes soient mises en évidence, d'une façon ou d'une autre, afin de faciliter leur examen de l'évolution du droit et des politiques.

iii. [redacted]

80. Le [description de l'activité] [redacted] dans le contexte d'une autorisation de cybersécurité a été traitée en profondeur dans une observation faite dans le dossier 2200-B-2023-02. En résumé, l'ancien commissaire au renseignement n'avait pas approuvé une activité particulière [redacted] et, dans l'affaire dont je suis saisi, le CST ne demandait plus l'autorisation de l'activité au motif que l'approbation ministérielle de l'activité n'était pas nécessaire. J'ai soulevé une préoccupation par rapport au manque d'explication dans le compte rendu qui a mené à cette conclusion. Je reconnais que le dossier dont je suis actuellement saisi porte sur le paragraphe 27(2) de la *Loi sur le CST*, alors que le dossier 2200-B-2023-02 a été déposé au titre du paragraphe 27(1) de la *Loi sur le CST*, mais je souligne que le libellé de chacune de ces deux dispositions reflète celui de l'autre. Ma préoccupation demeure entière et je m'attends à ce que le CST fournisse une réponse satisfaisante dans le contexte d'une future demande d'autorisation de cybersécurité.

iv. Documents à l'appui de la décision du ministre

81. J'ai remarqué que la lettre que le ministre m'a adressée n'est pas datée. De plus, le bloc-signature de l'autorisation comprend une ligne [TRADUCTION] « Délivrée à », mais cette dernière n'est pas remplie. Les documents à l'appui de la décision du ministre sont assujettis à l'examen quasi judiciaire du commissaire au renseignement; il doit s'agir de documents officiels dûment remplis par le décideur. Ils font partie du cadre de justification et de responsabilisation établi par le législateur en ce qui a trait aux activités de collecte de renseignements et de cybersécurité, et j'espère que le ministre abordera cette question dans les dossiers à venir.

82. De plus, le paragraphe 11 de l'autorisation énonce par erreur que [TRADUCTION] « en tant que ministre de la Défense nationale, j'ai délivré une autorisation [redacted]. L'autorisation comporte quelques autres divergences (comme le paragraphe 20 de l'autorisation, où le ministre conclut qu'il a des motifs raisonnables de croire que les activités autorisées aideront à protéger les systèmes fédéraux, plutôt que les systèmes non fédéraux). Bien que je

reconnaisse que les erreurs de rédaction font partie de la réalité, une autorisation contenant trop de ces erreurs pourrait miner le caractère raisonnable des conclusions du ministre.

VI. CONCLUSIONS

83. D'après mon examen du dossier, je suis convaincu que les conclusions tirées par le ministre en vertu des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités énumérées au paragraphe 54 de l'autorisation sont raisonnables.

84. 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 les infrastructures non fédérales, délivrée par le ministre le 6 octobre 2023.

85. Ainsi que le déclare le 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.

86. 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.

87. Si le passage du temps le permet, je suis d'avis que le public aurait éventuellement avantage à savoir que le CST a joué un rôle important dans le soutien et le rétablissement de la situation de l'entité non fédérale en matière de cybersécurité.

Le 3 novembre 2023

(Original signé)

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