~~**PROTÉGÉ B**~~

Dossier : 2200-B-2024-06

Bureau du commissaire au renseignement
Office of the Intelligence Commissioner

C.P./P.O. Box 1474, Succursale/Station B
Ottawa, Ontario K1P 5P6
613-992-3044 • télécopieur 613-992-4096

[TRADUCTION FRANÇAISE]

COMMISSAIRE AU RENSEIGNEMENT

DÉCISION ET MOTIFS

AFFAIRE INTÉRESSANT UNE AUTORISATION CONCERNANT DES ACTIVITÉS DE CYBERSÉCURITÉ MENÉES DANS 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 22 OCTOBRE 2024

TABLE DES MATIÈRES

I. APERÇU

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

2. Le [...], en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c13, art 76 (*Loi sur le CST*), le ministre a délivré une autorisation de cybersécurité pour des activités menées dans des infrastructures non fédérales (autorisation) pour [...]. Il s'agit de la quatrième année consécutive où le ministre délivre une autorisation de cybersécurité concernant cette entité non fédérale.

3. Le [...], le Bureau du commissaire au renseignement a reçu l'autorisation pour que je procède à l'examen et à l'approbation selon la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*).

4. Pour les motifs ci-après, 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 ou aux catégories d'activités énumérées paragraphe 62 de l'autorisation sont raisonnables.

5. Par conséquent, conformément à l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation.

II. CONTEXTE

6. Dans le cadre de son mandat à titre d'organisme national du renseignement électromagnétique (art 15(1), *Loi sur le CST*), le CST mène des activités de cyberprotection pour défendre les systèmes, les appareils et les réseaux électroniques ainsi que l'information qu'ils contiennent contre les cybermenaces criminelles et étatiques. Le CST fournit également des avis et des conseils pour renforcer la posture de cybersécurité de ces systèmes (art 17, *Loi sur le CST*). Les systèmes peuvent appartenir à une institution fédérale – systèmes fédéraux (art 27(1), *Loi sur le CST*) – ou à une entité non fédérale désignée comme

étant d'importance pour le gouvernement du Canada – systèmes non fédéraux (art 27(2), *Loi sur le CST*) – comme des entités dans les secteurs de la santé, de l'énergie et des télécommunications, comme il est précisé dans l'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada*, qui a été délivré le 25 août 2020.

7. Pour mener efficacement ses activités de cyberprotection sur les systèmes fédéraux et non fédéraux, le CST peut devoir contrevenir à certaines lois canadiennes. De plus, le CST peut acquérir incidemment des communications ou de l'information qui interfèrent avec l'attente raisonnable de protection en matière de vie privée de Canadiens ou de personnes se trouvant au Canada. Avant de mener ces activités de cybersécurité pouvant dépasser les limites de la loi et enfreindre les intérêts en matière de protection de la vie privée des Canadiens, la *Loi sur le CST* exige que le CST obtienne une autorisation ministérielle.

8. Lorsque l'autorisation porte sur un système non fédéral, le propriétaire ou l'opérateur de ce système doit amorcer le processus en demandant au CST, dans une demande écrite, de mener des activités de cybersécurité pour protéger le système et l'information électronique qu'il contient (art 33(3), *Loi sur le CST*).

9. La chef du CST doit ensuite présenter une demande écrite au ministre en expliquant les facteurs qui lui permettraient de conclure qu'il existe des motifs raisonnables de croire que l'autorisation est nécessaire (art 33(2), *Loi sur le CST*). Le ministre doit également conclure que les conditions prévues aux paragraphes 34(1) et 34(3) de la *Loi sur le CST* ont été respectées. Le ministre établit ses conclusions dans l'autorisation, qui est fournie au commissaire au renseignement aux fins d'examen. Le commissaire au renseignement approuve les activités ou catégories d'activités indiquées dans l'autorisation ministérielle s'il est convaincu que les conclusions du ministre sont raisonnables.

10. L'autorisation ministérielle est valide lorsqu'elle est approuvée par le commissaire au renseignement (art 28, *Loi sur le CST*). Ce n'est qu'à ce moment que le CST peut mener les activités énoncées dans l'autorisation – c'est-à-dire les activités qui pourraient autrement être

illégales et porter atteinte aux intérêts en matière de vie privée des Canadiens ou des personnes au Canada.

11. Conformément au paragraphe 27(2) de la *Loi sur le CST*, le ministre peut autoriser le CST à acquérir de l'information qui provient d'un système non fédéral, passe par ce système, 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, cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation du fonctionnement. L'alinéa 184(2)e) s'applique généralement aux personnes qui gèrent la qualité du service d'un système informatique ou sa protection.

12. Même si une autorisation de cybersécurité est délivrée, la *Loi sur le CST* impose des limites aux activités du CST. Les activités du CST ne peuvent viser un Canadien ou une personne qui se trouve au Canada ou porter atteinte à la *Charte canadienne des droits et libertés* (*Charte*) (art 22(1), *Loi sur le CST*). Toutefois, au cours d'activités menées au titre d'une autorisation, le CST peut légalement acquérir incidemment de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada (art 23(4), *Loi sur le CST*). « Incidemment » s'entend de la manière dont l'information est acquise dans le cas où elle n'était pas délibérément recherchée (art 23(5), *Loi sur le CST*).

13. Lorsque le CST acquiert des renseignements personnels liés à des Canadiens ou à des personnes au Canada, des mesures législatives et politiques strictes doivent être appliquées pour l'utilisation, l'analyse et la conservation de ces renseignements. De fait, le CST est tenu d'avoir des mesures en place pour 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 (art 24, *Loi sur le CST*).

14. Conformément à l'article 23 de la *Loi sur le CR*, le ministre a confirmé dans sa lettre de présentation m'avoir fourni tous les renseignements dont il disposait pour accorder l'autorisation en cause. Le dossier est donc composé de ce qui suit :

    a) L'autorisation;
    b) La note d'information de la chef du CST à l'intention du ministre;

c) La demande de la chef, qui comprend les 8 annexes suivantes :
   i. Lettre de demande de l'entité non fédérale;
   ii. Deux arrêtés ministériels;
   iii. Tableau de conservation et suppression;
   iv. Liste de recommandations du CST à l'intention de l'entité non fédérale;
   v. Rapport sur les résultats des activités de 2023;
   vi. Ensemble des politiques sur la mission en matière de cybersécurité (EPM), approuvé le 28 février 2022;
d) Le document d'information – aperçu des activités.

III. NORME DE CONTRÔLE

15. Selon l'article 12 de la *Loi sur le CR*, le commissaire au renseignement procède à un examen quasi judiciaire des conclusions sur lesquelles repose une autorisation ministérielle afin de déterminer si ces conclusions sont raisonnables.

16. La jurisprudence du commissaire au renseignement établit que la norme de la décision raisonnable, qui s'applique aux contrôles judiciaires des mesures administratives, est la même qui s'applique à mon examen.

17. Comme l'a affirmé la Cour suprême du Canada, lorsqu'elle procède à un contrôle judiciaire du caractère raisonnable, une 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, la Cour suprême du Canada a décrit de manière succincte ce qui constitue 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.

18. Les contraintes factuelles et juridiques pertinentes peuvent inclure le régime législatif applicable, l'incidence de la décision et les principes d'interprétation des lois. De fait, pour comprendre ce qui est raisonnable, il faut prendre en considération le contexte dans lequel la décision faisant l'objet du contrôle a été prise ainsi que le contexte dans lequel elle est examinée. 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*.

19. Un examen de la *Loi sur le CR* et de la *Loi sur le CST*, ainsi que des débats législatifs connexes, montre que le législateur a créé le rôle du 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, et le respect de la primauté du droit ainsi que des droits et libertés des Canadiens. J'estime que le législateur m'a attribué un rôle de gardien afin de maintenir cet équilibre. Dans mon examen des conclusions du ministre, je dois soigneusement déterminer si les intérêts importants des Canadiens et des personnes se trouvant au Canada, notamment en matière de vie privée, ont été dûment pris en compte et pondérés, et je dois m'assurer que la primauté du droit est pleinement respectée.

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

IV. ANALYSE

21. La chef a adressé au ministre une demande écrite pour une autorisation concernant des activités de cybersécurité menées dans des infrastructures non fédérales (autorisation) l'autorisant de mener des activités visant à protéger le système de l'entité non fédérale désignée comme étant d'importance pour le gouvernement du Canada. La demande décrit la nature et les objectifs d'activités de cybersécurité qui seront menées par le CST. En somme, […] acquis au moyen du système et analysé par le CST pour découvrir, isoler, prévenir et atténuer les dommages au système de l'entité.

22. Une description de l'entité non fédérale, ainsi que des activités indiquées dans l'autorisation se trouve dans l'annexe de la présente décision (annexe A). J'inclus ces informations dans une annexe pour deux raisons. Premièrement, cela empêchera qu'une partie importante de la présente décision soit caviardée, ce qui facilitera la lecture de sa version publique. Deuxièmement, cela permettra de s'assurer que la nature des faits dont j'ai été saisi, qui autrement ne seraient accessibles que dans le dossier, est incluse dans la décision.

23. D'après les faits présentés dans la demande soumise par la chef du CST le [...], le ministre a conclu qu'il avait des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions des paragraphes 34(1) et (3) de la *Loi sur le CST* ont été remplies. Suivant l'article 14 de la *Loi sur le CR*, je dois examiner si les conclusions du ministre, sur lesquelles repose l'autorisation qu'il a délivrée, sont raisonnables.

A. Paragraphe 34(1) de la *Loi sur le CST* – Déterminer si les activités sont raisonnables et proportionnelles

i. Signification du caractère raisonnable et proportionnel

24. Pour délivrer une autorisation de renseignement étranger, le ministre doit conclure « qu'il y a des motifs raisonnables de croire que l'activité en cause (*any activity* en anglais) est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités » (art 34(1), *Loi sur le CST*).

25. Le ministre doit parvenir à sa conclusion en se fondant sur sa compréhension de ce qu'impliquent des seuils raisonnables et proportionnels. La question de savoir si une activité est raisonnable et proportionnelle dépend du contexte et le ministre peut tenir compte de nombreux facteurs pour prendre sa décision. Le commissaire au renseignement doit juger si les conclusions du ministre, qui comprennent sa compréhension de ce que les seuils emportent, sont « raisonnables », et applique pour ce faire la norme de la décision raisonnable, comme cela est expliqué précédemment.

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

26. Le ministre a conclu au paragraphe 33 de l'autorisation qu'il avait des motifs raisonnables de croire que les activités autorisées dans l'autorisation sont raisonnables étant donné que l'objectif est d'aider à protéger le système de l'entité non fédérale et de potentiellement protéger les systèmes fédéraux et d'autres systèmes d'importance contre les méfaits, l'utilisation non autorisée et la perturbation.

27. Les activités indiquées dans l'autorisation permettraient au CST d'accéder à un système qui est situé au Canada. Le ministre explique que ces activités de cybersécurité peuvent mener à la collecte et à la possible conservation d'information à l'égard de laquelle des Canadiens ou des personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée. Étant donné le contexte dans lequel l'autorisation a été délivrée et la description de l'information que le CST doit acquérir pour mener efficacement ses activités, je sais que le CST recueille ce genre d'information. En effet, le dossier indique que le CST « doit » acquérir [...].

28. Néanmoins, lors de la délivrance d'une autorisation de cybersécurité, le ministre reconnaît que toute information liée à des Canadiens ou à des personnes se trouvant au Canada acquise au cours des activités n'est pas délibérément recherchée, mais incidemment acquise – et ne contrevient donc pas à l'interdiction, établie dans la loi, de chercher délibérément de l'information qui visent, ou de mener des activités qui visent, des Canadiens ou des personnes se trouvant au Canada (art 22(1). *Loi sur le CST*). En effet, le paragraphe 23(3) de la *Loi sur le CST* précise que malgré l'interdiction de mener des activités qui visent des Canadiens ou des personnes se trouvant au Canada, le CST peut mener des activités de cybersécurité pour protéger les systèmes et atténuer les dommages – ce qui inclut les systèmes situés au Canada. Je suis convaincu que les activités de cybersécurité indiquées dans l'autorisation ne visent pas des Canadiens ou des personnes se trouvant au Canada.

29. Tout comme dans décision de l'année dernière concernant cette entité non fédérale (décision 2200-B-2023-05), le ministre fournit deux raisons principales pour justifier le caractère raisonnable des activités de cybersécurité. Premièrement, les activités indiquées

dans l'autorisation sont efficaces et complètent les autres activités de cybersécurité de l'entité non fédérale. Le ministre explique que les activités permettent au CST de repérer et de mieux comprendre les cyberactivités malveillantes et d'autres indicateurs de compromission afin de conseiller l'entité non fédérale sur la façon de protéger son système et de prendre des mesures d'atténuation. Les renseignements recueillis peuvent également aider à protéger les systèmes fédéraux et d'autres systèmes d'importance.

30. Deuxièmement, [...], les activités de cybersécurité du CST sont nécessaires pour continuer de réparer et de rebâtir l'infrastructure de l'information et de la protéger contre d'autres cybermenaces. Le ministre explique que même si l'entité non fédérale a fait des progrès importants concernant la mise en œuvre des recommandations du CST pour améliorer sa posture de cybersécurité, il y a une présence continue d'activités malveillantes dans le système et certaines des recommandations clés n'ont pas encore été complétées.

31. Afin de souligner la menace permanente pour le système de l'entité non fédérale, le ministre mentionne trois rapports communiqués à l'entité non fédérale l'an dernier – [...]. Il fournit également des détails sur un auteur de menaces précis ayant ciblé des entités œuvrant dans le même secteur d'importance pour le gouvernement du Canada que l'entité non fédérale.

32. En résumé, selon le ministre, la sensibilité et l'importance des renseignements détenus par l'entité non fédérale, la compromission qu'elle a précédemment connue et les preuves continues d'activités malveillantes et de vulnérabilités précisées dans les trois rapports communiqués à l'entité pendant la période couverte par l'autorisation précédente, sont des motifs permettant de conclure que les activités autorisées dans l'autorisation sont raisonnables.

33. Je n'ai aucune difficulté à trouver raisonnable la conclusion du ministre selon laquelle les activités de cybersécurité indiquées dans l'autorisation sont efficaces. Je reconnais aussi que les renseignements dans le dossier appuient la conclusion selon laquelle la posture de cybersécurité de l'entité non fédérale nécessite toujours le soutien du CST. De fait, dans les deux premières autorisations concernant cette entité non fédérale, le caractère raisonnable des conclusions du ministre était appuyé par les cyberattaques – décrites dans le dossier – et

l'incapacité de l'entité à lutter contre les cybermenaces typiques ou attendues. Les activités de cybersécurité du CST étaient nécessaires pour détecter les menaces et les atténuer. Dans l'autorisation de l'année dernière, le ministre a confirmé que […], la posture de cybersécurité de l'entité fédérale n'était toujours pas suffisamment développée à ce moment pour lutter contre les cybermenaces. Sur la base des renseignements contenus dans le dossier, la justification sous-jacente pour laquelle les conclusions du ministre dans les autorisations passées étaient raisonnables – une posture de cybersécurité insuffisamment robuste – continue de s'appliquer dans la présente autorisation.

34. Néanmoins, je suis préoccupé par certains éléments de la conclusion du ministre, en particulier en ce qui concerne le recours à la présence de menaces permanentes et aux recommandations en suspens du CST pour justifier la présence continue du CST dans le système.

35. En ce qui a trait aux menaces permanentes, le ministre s'appuie sur les trois rapports communiqués à l'entité non fédérale à titre de preuve indiquant la présence continue d'activités malveillantes et de vulnérabilités. Il y a très peu de renseignements au dossier au sujet de ces activités malveillantes et de ces vulnérabilités, et certains renseignements sont imprécis. Le ministre et la chef indiquent simplement que deux rapports concernaient des « vulnérabilités ». L'incidence de ces vulnérabilités sur le système n'est pas abordée. Le ministre et la chef affirment qu'un troisième rapport impliquait […], mais le rapport sur les résultats indique que le rapport concernait […]. […] Il n'est pas clair s'il s'agit de la même vulnérabilité.

36. L'existence des rapports communiqués à l'entité non fédérale au sujet d'une « vulnérabilité » ne constitue pas nécessairement une preuve venant appuyer le caractère raisonnable de la présence continue du CST dans le système non fédéral. L'existence d'un rapport ne donne pas de renseignements sur l'incidence de la vulnérabilité sur le système. Le dossier n'explique pas si la « vulnérabilité » est grave ou le résultat d'une omission sans conséquence. Parallèlement, le dossier n'explique pas pourquoi […] menace le système. Pour pouvoir s'appuyer sur l'incidence de la vulnérabilité, comme le fait le ministre, le dossier doit refléter la nature de cette incidence. Si les conclusions du ministre s'appuient sur la

présence continue des vulnérabilités, la demande de la chef devrait refléter de manière robuste le lien entre les vulnérabilités incluses dans les rapports et l'incidence sur le système.

37. Comme je l'ai indiqué dans des décisions antérieures, le ministre s'appuie à juste titre sur l'expertise technique du CST pour étayer ses conclusions. Quoi qu'il en soit, lorsqu'elles s'appuient sur cette expertise, les conclusions du ministre devraient démontrer une compréhension des répercussions des constatations techniques du CST.

38. Mon inquiétude concernant le recours aux recommandations en suspens est également liée au manque de clarté du dossier. Dans l'autorisation de l'année dernière, le ministre a justifié le caractère raisonnable de ses conclusions en partie par l'existence de […] recommandations en suspens devant être achevées en 2024.

39. D'après les conclusions du ministre dans l'autorisation de l'année dernière, j'avais cru comprendre qu'à la suite de l'achèvement des […] recommandations en suspens – dont il prévoyait la mise en œuvre en 2024 – le soutien du CST ne serait plus nécessaire. En effet, comme je l'ai indiqué dans la décision de l'année dernière : « Cela devrait alors permettre à l'entité non fédérale de lutter contre les cybermenaces typiques ou attendues. » (para 42)

40. Pourtant, comme il a été expliqué par le ministre et la chef dans cette autorisation, […] recommandations clés doivent encore être complétées. De plus, […] recommandations clés en suspens actuelles sont différentes des […] recommandations en suspens de l'année dernière (comme il est indiqué à l'annexe A). Puisque le ministre s'appuie sur les recommandations pour conclure que les activités du CST sont raisonnables, le dossier doit indiquer de manière claire et cohérente les recommandations clés qui restent à mettre en œuvre, ainsi que les répercussions des recommandations en suspens sur la posture de cybersécurité de l'entité.

41. À cet égard, dans la décision de l'année dernière, j'ai indiqué que le dossier aurait pu fournir des détails supplémentaires sur la relation entre les […] recommandations en suspens et l'état du système de l'entité non fédérale. Cette question a été abordée dans le dossier qui m'a été présenté. Le ministre explique pourquoi, sans les recommandations finales en place, le

système de l'entité non fédérale demeure vulnérable. Je trouve cette conclusion du ministre raisonnable.

42. Enfin, malgré mes inquiétudes, la conclusion du ministre selon laquelle le système demeure vulnérable, ainsi que le fait que les activités de cybersécurité du CST sont efficaces, viennent appuyer les conclusions indiquant que les activités proposées sont raisonnables. Les conclusions du ministre sont raisonnables, parce que les activités de cybersécurité du CST sont nécessaires alors que la posture de cybersécurité de l'entité est encore en cours de développement. Il existe un lien rationnel entre les activités de cybersécurité et la protection du système de l'entité non fédérale.

43. Dans mes observations à la fin de la décision, je reviens sur certaines répercussions du renouvellement d'une autorisation de cybersécurité pour une période prolongée.

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

44. Le ministre a conclu, au paragraphe 35 de l'autorisation, qu'il avait des motifs raisonnables de croire que les activités autorisées sont « proportionnelles compte tenu de la façon dont elles sont exercées ».

45. Je suis convaincu que les conclusions du ministre sur la proportionnalité sont raisonnables en ce qui concerne les activités autorisées décrites au paragraphe 62 de l'autorisation. Il reconnaît que les cyberactivités proposées peuvent mener à l'acquisition de grands volumes d'information afin de déceler les cybermenaces. Bien qu'il puisse y avoir des droits en matière de vie privée à l'égard d'une partie de l'information, le ministre explique que le CST est intéressé par tous les comportements anormaux touchant l'information, et non par son contenu.

46. Le ministre présente des mesures et des contrôles pour démontrer que les activités sont proportionnelles. Je constate que les mesures correspondent à celles qui ont été incluses dans l'autorisation ayant fait l'objet de la décision 2200-B-2024-05 en ce qui concerne une entité non fédérale. Le ministre énonce sept mesures et contrôles internes appliqués par le CST :

a) aucune information non évaluée n'est conservée plus longtemps que [...] à compter de la date à laquelle elle a été acquise;
b) le CST conserve moins de 1 % de toutes les données initialement acquises au moyen d'activités de cybersécurité;
c) l'analyse et l'atténuation sont principalement effectuées par des processus automatisés qui limitent l'exposition des employés à l'information non évaluée et toute l'information est protégée conformément à la politique d'exploitation du CST;
d) chaque fouille effectuée dans l'information acquise non évaluée peut faire l'objet d'un audit pour assurer la conformité avec l'EPM;
e) l'accès à l'information acquise en vertu de la présente autorisation est limité aux employés qui ont besoin d'en avoir connaissance dans le cadre de leur travail. Avant d'accéder à de l'information non évaluée, les employés doivent réussir un examen annuel noté portant sur les exigences établies par les lois et les politiques qui s'appliquent au traitement de ce type d'information;
f) toutes les technologies de cybersécurité sont passées en revue pour veiller à ce qu'elles soient conformes aux lois et aux politiques;
g) les mêmes conditions s'appliquent à l'information utilisée par le CST pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes fédéraux et autres systèmes d'importance.

47. Le ministre se fie largement aux mesures appliquées à l'information après son acquisition pour étayer sa conclusion au sujet de la proportionnalité. Le ministre confirme que dans le cadre de ses activités de cybersécurité, le CST obtient un large éventail d'informations afin de protéger les systèmes fédéraux et non fédéraux. Cela inclut un accès à une grande quantité d'information, comme [...], à l'égard de laquelle des Canadiens et des personnes se trouvant au Canada peuvent avoir une attente raisonnable de protection en matière de vie privée. L'information conservée représente moins de 1 % de toutes les données initialement acquises. Je constate que le dossier n'indique pas la quantité totale d'information ayant été acquise par le passé. Bien que 1 % puisse sembler minime, l'accès du CST au système non fédéral est vaste. Le ministre et le commissaire au renseignement profiteraient de renseignements supplémentaires en lien avec le volume total de données recueillies pour

mieux déterminer la proportionnalité des activités menées par le CST et la manière dont elles portent le moins possible atteinte à la vie privée des Canadiens et des personnes se trouvant au Canada.

48. Le rapport sur les résultats indique que durant l'autorisation précédente, le CST a conservé 40 « articles » (en anglais, *items*) acquis à partir du système non fédéral – ce qui représente moins de 1 % du total des données acquises. Il s'agit de la première autorisation dans laquelle il y a des chiffres précis à l'égard de l'information conservée. Je félicite le CST pour avoir donné suite aux remarques passées en fournissant au ministre et à moi-même des renseignements supplémentaires sur les répercussions concrètes des autorisations. Je tiens compte de ces progrès à des fins de responsabilité ministérielle ainsi qu'à des fins de transparence. Je ferais toutefois remarquer qu'un contexte supplémentaire afin de comprendre ce qui constitue un « article » serait utile pour le ministre et moi.

49. Dans l'autorisation, le ministre explique certains des progrès ayant été réalisés dans le cadre de la mise en œuvre des recommandations du CST et des éléments qui demeurent en suspens. La période de temps nécessaire est principalement attribuable au processus d'approvisionnement. J'estime qu'il s'agit d'une explication raisonnable. Cependant, le dossier ne fournit pas de calendrier indiquant quand les recommandations en suspens pourraient être achevées ou quand les activités de cybersécurité du CST ne seront plus nécessaires. La durée de temps requise par le CST pour atteindre cet objectif pourrait être un facteur à prendre en considération lors de l'examen visant à déterminer si les activités sont proportionnelles, et j'aborde davantage cette question dans mes observations.

50. Le ministre explique que l'accès à l'information pouvant être liée aux droits des Canadiens en matière de vie privée est limité aux employés désignés du CST qui sont formés pour traiter ce type d'information et l'utiliser selon le principe du « besoin de savoir » dans le cadre de leur travail. Cela limite l'accès à l'information pouvant être liée aux droits des Canadiens en matière de vie privée. Même si le ministre était conscient des droits en matière de vie privée en jeu, je réitère mon commentaire formulé dans la décision 2200-B-2024-05 concernant une entité non fédérale, lequel indiquait que ses conclusions auraient pu être plus

précises quant à la probabilité qu'ils puissent être enfreints et à l'importance des éventuelles atteintes – et décrire les mesures en place pour les protéger.

51. Je peux comprendre pourquoi le ministre estime qu'il est justifié de se fonder sur ces mesures. Il conclut que les activités proposées justifient toute atteinte potentielle aux droits des Canadiens en matière de vie privée. Il explique également comment les activités avaient pour objectif l'atteinte d'un équilibre raisonnable entre elles. Je suis convaincu que les intérêts des Canadiens et des personnes se trouvant au Canada ont été pris en considération et que la pondération effectuée était raisonnable.

52. En ce qui concerne les lois fédérales qui pourraient être enfreintes, l'autorisation indique qu'elles sont limitées, car les activités auraient seulement lieu dans un système pour lequel le CST a reçu le consentement explicite du propriétaire pour mener des activités. Puisque le CST a obtenu son consentement, les infractions possibles aux lois canadiennes sont faibles. Je reviens sur la question du consentement au paragraphe 72 de cette décision. Si une loi fédérale est enfreinte, l'incidence de la violation sera limitée et si une loi fédérale ne figurant pas dans la demande de la chef est enfreinte, la chef informera le ministre et le commissaire au renseignement.

53. Les conclusions du ministre démontrent sa compréhension des intérêts en matière de protection de la vie privée et des mesures en place pour les protéger, ainsi que des possibles répercussions sur la primauté du droit. Compte tenu de ces éléments, il a conclu que les activités étaient proportionnées. J'estime que ses conclusions sont justifiées et intelligibles. En conséquence, je suis convaincu que les conclusions du ministre concernant le caractère proportionnel des activités sont raisonnables.

B. Paragraphe 34(3) de la *Loi sur le CST* – Les conditions nécessaires à la délivrance d'une autorisation

54. Lorsque le ministre estime que les activités sont raisonnables et proportionnelles au titre du paragraphe 34(1) de la *Loi sur le CST*, il peut délivrer une autorisation de cybersécurité pour aider à protéger des systèmes non fédéraux s'il conclut qu'il y a des motifs raisonnables de

croire que les trois conditions suivantes, énoncées au paragraphe 34(3) *Loi sur le CST*, 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;
c) les mesures en place pour s'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à des Canadiens ou à des personnes 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 au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire (art 34(3)a)

55. L'information est conservée conformément aux exigences définies dans les politiques du CST et régies par un calendrier de conservation. Le ministre explique également que les exigences du CST concernant la gestion de l'information et la disposition de dossiers énoncées dans les politiques du CST sont conformes à la *Loi sur la protection des renseignements personnels*, LRC, 1985, c P-21 et à la *Loi sur la Bibliothèque et les Archives du Canada*, LC 2004, c 11.

56. Le ministre explique que les activités de cybersécurité du CST sont […]. Comme il est impossible pour le CST de déterminer au préalable quelle information sera utile pour découvrir des activités malveillantes, il acquiert une grande quantité d'information non évaluée […].

57. De plus, le CST traite l'information non évaluée, principalement à l'aide de moyens automatisés qui limitent l'exposition des employés du CST à l'information contenue dans un dossier. L'utilisation de processus automatisés permet de s'assurer que les employés interagissent uniquement avec l'information nécessaire pour élaborer des mesures de détection et d'atténuation, ou pour déterminer les processus de conservation et de traitement.

58. La période de conservation de l'information non évaluée est de […], alors que l'information jugée « nécessaire » ou « essentielle » pour aider à protéger le système non fédéral, ou les

systèmes fédéraux et les systèmes désignés comme étant d'importance, peuvent être conservée « indéfiniment ou jusqu'à ce qu'elle ne soit plus utile à ces fins ».

59. Comme expliqué par le ministre, il y a souvent une période entre le moment où la compromission débute et celui où elle est découverte. Par conséquent, l'efficacité des activités du CST dépend de la capacité à recouper et à analyser de l'information de multiples sources déjà acquise, y compris les indicateurs de compromission découverts. La période de conservation [...] de l'information non évaluée permet au CST de remonter aux origines d'un événement ou d'examiner son évolution au fil du temps. De nouvelles vulnérabilités sont découvertes sur une base continue. La comparaison entre une atteinte à l'intégrité et des données non évaluées ou des activités malveillantes non détectées aide le CST à élaborer de meilleures mesures d'atténuation et des moyens de défense qui peuvent être utilisés non seulement pour le système non fédéral, mais aussi pour les autres systèmes d'importance et les systèmes fédéraux.

60. Après la période [...], l'information non évaluée sera automatiquement supprimée, à moins qu'elle soit jugée « nécessaire » ou « essentielle » pour aider à protéger le système non fédéral ou les systèmes fédéraux et les systèmes désignés comme étant d'importance. L'accès à l'information non évaluée est strictement contrôlé et limité aux personnes autorisées à mener ou à soutenir des activités de cybersécurité (art 10.2 de l'EPM). La liste du personnel ayant un accès approuvé à l'information non évaluée est surveillée aux fins de reddition de comptes. L'information non évaluée ne peut pas être divulguée à l'extérieur du CST. Dans la demande, la chef confirme que l'entité non fédérale en question connaît l'utilisation de cette information et l'accepte.

61. Comme il est indiqué dans le dossier, le critère du caractère « nécessaire » s'applique à l'information qui ne se rapporte pas à un Canadien ou à une personne se trouvant au Canada; quant au critère du caractère « essentiel », il s'applique à l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada. L'information est jugée « nécessaire » quand elle est requise pour comprendre la cyberactivité malveillante, y compris [...], dans le but d'aider à protéger des systèmes non fédéraux. Par sa nature, cette information ne contient pas d'éléments liés à des Canadiens ou à des personnes se trouvant au Canada et est donc

moins sensible que l'information jugée « essentielle ». Le but est d'aider à réaliser des analyses de détection et de prévention et à renforcer davantage l'écosystème de cyberdéfense.

62. L'information sur les Canadiens et les personnes se trouvant au Canada est considérée comme « essentielle » si, sans elle, le CST n'était pas en mesure de découvrir, d'isoler, de prévenir ou d'atténuer des dommages au système non fédéral. Cela peut inclure [...]. L'information acquise peut être hautement sensible pour les Canadiens, et la plupart des analyses sont faites suivant des processus automatisés qui détectent les comportements anormaux et limitent l'exposition des employés au contenu des fichiers.

63. L'information qui a été jugée nécessaire ou essentielle pour découvrir, isoler, prévenir ou atténuer les dommages causés au système non fédéral est conservée conformément à l'article 11.2 de l'EPM. Le programme de conformité interne du CST envoie des rappels trimestriels aux analystes de la cybersécurité afin de s'assurer que les données conservées dans un dépôt ministériel qui n'ont pas été jugées nécessaires ou essentielles soient supprimées dans les [...] suivants leur acquisition. De plus, les gestionnaires opérationnels doivent revalider sur une base trimestrielle si l'information demeure essentielle. L'information qui n'est plus essentielle doit être supprimée.

64. Je suis d'avis que le ministre explique raisonnablement la raison pour laquelle il faut conserver l'information pendant la durée nécessaire – [...] pour l'information non évaluée et jusqu'à ce qu'elle ne soit plus utile pour l'information qui est « nécessaire » ou « essentielle ». Ces périodes de conservation permettent au CST de mener des activités de cybersécurité de manière efficace. Je suis également convaincu que les importantes restrictions visant les employés du CST concernant l'accès à l'information non évaluée, les rappels trimestriels qu'ils reçoivent afin de vérifier les dépôts ministériels, ainsi que ceux fournis aux gestionnaires opérationnels afin de confirmer que la conservation de l'information liée aux Canadiens demeure essentielle, soutiennent le caractère raisonnable des conclusions du ministre.

ii. L'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux (art 34(3c)

65. Les activités de cybersécurité du CST ne sont efficaces qu'avec l'acquisition d'information. Le ministre explique que les auteurs de menaces [...] délibérément. Afin d'atténuer efficacement les cybermenaces sophistiquées décrites dans le présent cas et de prévenir les cybermenaces potentielles, le CST doit acquérir un large éventail d'information qui peut ensuite être évaluée pour repérer les activités malveillantes. L'information comprend [...].

66. Rien dans le dossier ne donne à entendre que le CST peut atteindre les mêmes résultats de cybersécurité en employant des activités de cybersécurité différentes qui permettent d'acquérir moins d'information, tout particulièrement de l'information se rapportant à des Canadiens. Les conclusions du ministre contiennent des exemples de la façon dont l'information acquise au titre de cette autorisation peut aussi être utilisée par le CST pour appuyer des activités au titre d'autres autorisations de cybersécurité et sous d'autres volets de son mandat.

67. Pour ces motifs, je suis convaincu que les conclusions du ministre sont raisonnables et qu'il a des motifs raisonnables de croire que l'acquisition d'information est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages au système non fédéral.

iii. Les mesures permettant de protéger la vie privée permettront de veiller à ce que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à des Canadiens ou à des personnes se trouvant au Canada soit utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux (art 34(3)d)

68. L'article 24 de la *Loi sur le CST* exige que le CST ait des mesures en place pour 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 d'information qui se rapporte à eux et qui a été acquise dans la réalisation des volets de son mandat touchant la cybersécurité et l'assurance de l'information.

69. Le ministre répète que l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada ne peut être conservée que si elle est évaluée comme étant essentielle, à savoir que le CST juge que sans elle, il serait incapable de découvrir, d'isoler, de prévenir ou d'atténuer des dommages au système de l'entité non fédérale. Comme il est indiqué à la section 8.2.2 de l'EPM, le critère du caractère essentiel est évalué par des employés du CST accrédités et formés, à l'aide de processus manuels ou automatisés. Les employés doivent consigner les raisons pour lesquelles ils estiment que l'information est essentielle. Cette façon de procéder limite l'accès au contenu de l'information qui est très sensible pour les Canadiens et l'exposition à l'information non évaluée. À mon avis, ces mesures contribuent à la conformité à l'obligation législative établie à l'article 24 de la *Loi sur le CST* et soutiennent les conclusions du ministre.

70. Comme il est indiqué à la section 24 de l'EPM, des mesures sont en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada lorsque des renseignements qui les concernent sont divulgués. Par exemple, les renseignements personnels peuvent être supprimés afin d'éviter de dévoiler l'identité d'une personne. Lorsque de l'information liée à un Canadien est divulguée, l'EPM établit les niveaux requis d'approbation de la divulgation. Ces approbations doivent être documentées.

71. Les conclusions du ministre et le dossier expliquent comment l'information relative à des Canadiens ou à des personnes se trouvant au Canada peut être divulguée, ce qui correspond à l'obligation énoncée à l'article 44 de la *Loi sur le CST*. L'information est communiquée uniquement aux personnes ou aux catégories de personnes désignées en vertu de l'*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*. Ces destinataires comprennent les propriétaires et les administrateurs d'un système ou d'un réseau informatique utilisé par le gouvernement du Canada ou une entité non fédérale, ainsi que les personnes et les catégories de personnes au sein d'entités étrangères avec lesquelles le CST a conclu des ententes. Afin de recevoir de l'information divulguée par le CST qui se

rapporte à des Canadiens ou à des personnes se trouvant au Canada, l'information doit être nécessaire pour aider à protéger des systèmes non fédéraux ou fédéraux.

72. Dans sa lettre de demande au CST, l'entité non fédérale a demandé que toute l'information personnelle ou confidentielle qui peut être recueillie et conservée soit masquée avant la divulgation. De plus, toute l'information qui n'est pas pertinente pour le mandat du CST doit être supprimée en conformité avec le calendrier de conservation du CST. Je comprends donc que toute divulgation d'information acquise au titre de l'autorisation devra d'abord respecter cette directive. Je réitère une observation formulée dans la décision 2200-B-2024-05 concernant une entité non fédérale selon laquelle les enjeux relatifs à la collecte et à l'utilisation de l'information personnelle et au consentement des personnes dont l'information peut être acquise doivent demeurer des enjeux centraux et être abordés dans les autorisations de cybersécurité. En effet, l'information pour laquelle il existe une attente raisonnable de protection en matière de vie privée partagée dans le système d'une entité non fédérale pourrait finir par être conservée par le CST, un organisme du gouvernement du Canada à des fins de cybersécurité. Le ministre devrait être en mesure de comprendre facilement que l'entité non fédérale a la compétence en première instance de recueillir l'information, et qu'il existe un fondement juridique pour sa communication au CST.

73. L'EPM énonce les politiques pour contrôler et protéger l'information concernant des Canadiens ou des personnes se trouvant au Canada qui est acquise au titre d'une autorisation de cybersécurité. À mon avis, lorsqu'elles sont suivies, ces mesures constituent un moyen efficace pour le CST de protéger suffisamment cette information comme l'exige la loi.

74. Les communications privées canadiennes, [...], qui sont incidemment acquises, sont prises en compte dans le rapport relatif à une autorisation qui a pris fin ayant été fourni au ministre, et une copie de celui-ci a également été fournie au commissaire au renseignement (art 52, *Loi sur le CST*). Le dernier rapport indique qu'aucune communication privée n'a été acquise, conservée ou divulguée.

75. Compte tenu de ce qui précède, je suis donc convaincu que la conclusion du ministre est raisonnable et qu'il a des motifs raisonnables de croire que l'information concernant des

Canadiens ou des personnes se trouvant au Canada ne sera utilisée, analysée ou conservée que si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages au système de l'entité non fédérale.

76. Je note que dans une observation figurant dans la décision de l'année dernière concernant cette entité non fédérale, j'ai indiqué que je m'attendais à ce que le CST fournisse au ministre et à moi-même des précisions pour mieux comprendre la nature, la fréquence et le volume de la conservation d'information liée aux intérêts des Canadiens en matière de vie privée. Comme cela a été mentionné précédemment, cela a été abordé dans le rapport sur les résultats – avec la mise en garde de fournir un contexte supplémentaire sur ce qui constitue un « article » et la quantité totale de données conservées. Selon la nature du type d'information liée aux Canadiens conservée étant décrite dans le rapport sur le résultat, on comprend aisément pourquoi sa conservation est essentielle. Lorsque le caractère essentiel de la conservation de l'information liée aux Canadiens n'est pas évident, je demeure d'avis que le dossier devrait expliquer pourquoi la conservation de ce type d'information est essentielle – surtout lorsque, comme c'est le cas ici, certaines informations sont conservées à titre d'information essentielle, mais ne sont pas incluses dans les rapports destinés à l'entité non fédérale.

V. REMARQUES

77. J'aimerais faire les deux remarques suivantes qui ne changent rien à mes conclusions concernant le caractère raisonnable des conclusions du ministre.

A. Renouvellement des autorisations de cybersécurité pour des périodes prolongées

78. Le ministre indique que les cybercompromissions deviennent de plus en plus difficiles à détecter, surtout sans les activités de cybersécurité du CST. Effectivement, il indique que « les mesures de sécurité disponibles sur le marché ayant été mises en place par [l'entité non fédérale] ne sont pas suffisantes pour repérer et contrer les cybermenaces persistantes et de plus en plus complexes. » Cela nous amène à nous demander si les mesures de sécurité disponibles sur le marché seront suffisantes un jour à elles seules. Même si l'autorisation de l'année dernière reconnaissait que les activités de cybersécurité du CST dans le système de l'entité non fédérale prendraient fin tôt ou tard (à l'époque, cela était prévu pour 2024), le

dossier de cette année n'indique pas quand les recommandations en suspens pourraient être achevées, ou ne suggère pas que la présence du CST ne sera plus nécessaire lorsque les recommandations seront entièrement mises en œuvre.

79. La *Loi sur le CST* ne limite pas la période durant laquelle le CST peut aider une entité non fédérale. Cependant, la justification de la présence continue du CST mentionnée dans les conclusions du ministre pourrait devoir changer au fil du temps. Je mentionne cela parce que si l'autorisation de cybersécurité de cette entité non fédérale était renouvelée une fois les recommandations mises en œuvre – ou s'il n'y avait plus d'explication raisonnable pour expliquer le temps pris pour mettre en œuvre les recommandations en suspens – les conclusions du ministre pourraient devoir changer pour répondre à la norme de la décision raisonnable que je dois appliquer.

80. Les autorisations de cybersécurité constituent une intrusion dans la vie privée étant donné la collecte nécessaire d'informations à l'égard desquelles les Canadiens peuvent avoir une attente raisonnable de protection en matière de vie privée – même si la collecte est accessoire à la protection du système. Je considère que le degré d'intrusion est encore plus élevé dans le cas des autorisations de cybersécurité en soutien des entités non fédérales, car le CST – un organisme du gouvernement du Canada – recueille de l'information à laquelle il n'aurait autrement pas accès. Et bien sûr, l'intrusion est exacerbée au fil du temps. Par conséquent, il est important que la justification de la poursuite de cette collecte accessoire sur une période prolongée soit suffisamment étudiée et étayée dans les conclusions du ministre.

B. Incident de conformité

81. Un incident de conformité est décrit dans le rapport de 2022-2023 relatif à une autorisation qui a pris fin résumant les résultats des activités menées dans le cadre de l'autorisation ministérielle de 2022. Le ministre a été informé qu'à la suite d'une demande présentée par le ministère de la Justice, le CST a conservé de l'information en raison d'un litige, laquelle avait été recueillie en vertu de l'autorisation et aurait autrement été supprimée dans un délai déterminé. L'équipe de conformité interne du CST, en collaboration avec le ministère de la Justice, a mené une étude examinant la conservation de l'information en raison d'un litige. Le CST examine actuellement les options pour assurer la conformité dans le cadre du

traitement ce type d'information. Je suis d'avis que de telles exceptions en ce qui concerne le traitement de l'information recueillie conformément à une autorisation devraient ultimement être reflétées dans les conditions établies dans l'autorisation.

82. Même si la non-conformité ne remet pas en cause la validité de toute autorisation que j'ai précédemment approuvée, l'incident de conformité n'est pas mentionné dans ce dossier. Je suis d'avis que le ministre, en sa qualité de décideur, aurait dû disposer des informations dans le dossier dont il était saisi pour déterminer si elles étaient pertinentes pour ses conclusions. Le rapport relatif à une autorisation qui a pris fin est une source d'information importante pour le ministre et moi afin que nous puissions voir les activités qui ont été menées. En effet, ce rapport n'est pas seulement destiné à satisfaire à une exigence légale. Il fournit des détails sur les activités entreprises dans le cadre de l'autorisation qui pourraient être pertinents pour la délivrance de futures autorisations. Pour ces raisons, je suis d'avis que l'information pertinente du rapport devrait, s'il y a lieu – par exemple, lorsqu'il y a eu un problème de conformité et ce qui a été fait pour le corriger – être incluse dans le dossier dont le ministre est saisi.

VI. CONCLUSIONS

83. D'après mon examen du dossier, je suis convaincu que les conclusions que le ministre a tirées au titre des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités énumérées au paragraphe 62 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 concernant des activités de cybersécurité menées dans des infrastructures non fédérales délivrée par le ministre le [...].

85. Comme le ministre l'a indiqué, et en vertu du paragraphe 36(1) de la *Loi sur le CST*, cette autorisation expire un an après la date de mon approbation.

86. Conformément à 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 accomplir 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. Dans la décision de l'année dernière, j'ai indiqué que j'étais d'avis qu'il serait avantageux de rendre public le rôle du CST dans le soutien et la reconstruction de la posture de cybersécurité de l'entité non fédérale – si le temps écoulé le permettait. Je réitère le même point de vue en ce qui concerne cette autorisation.

Le 22 octobre 2024

(Original signé)

L'honorable Simon Noël, c.r.
Commissaire au renseignement