Dossier : CST-2025-08

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 DE CYBERSÉCURITÉ
POUR DES ACTIVITÉS 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 5 NOVEMBRE 2025

Canada

TABLE DES MATIÈRES

I. APERÇU

1. Il s'agit d'une décision concernant l'examen des conclusions du ministre de la Défense nationale (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 trois entités non fédérales – les gouvernements des Territoires du Nord-Ouest (GTNO), du Yukon (GY) et du Nunavut (GN) (autorisation).

2. L'autorisation renouvelle les activités de cybersécurité déjà approuvées par le commissaire au renseignement pour les trois entités et ajoute de nouvelles activités pour le GTNO. Il s'agit de la troisième année consécutive qu'une autorisation de cybersécurité est accordée à l'égard des trois gouvernements territoriaux (voir les décisions CST-2024-07, CST-2023-06), et de la quatrième année consécutive qu'une autorisation de cybersécurité est accordée à l'égard du GTNO (décision CST-2022-06).

3. Le 9 octobre 2025, 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 l'autorisation. Le Bureau du commissaire au renseignement l'a reçue le lendemain pour que je l'examine et l'approuve, conformément à 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 au paragraphe 90 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 du volet de son mandat touchant la cybersécurité, le CST mène des activités de cyberprotection afin d'aider à protéger certains systèmes, dispositifs et réseaux électroniques ainsi que l'information qu'ils contiennent contre les cybermenaces criminelles et parrainées par des États. De plus, le CST fournit des avis et des conseils pour renforcer la posture de cybersécurité de ces systèmes (art 17, *Loi sur le CST*).

7. Sous le régime de la *Loi sur le CST*, le CST est tenu d'obtenir une autorisation ministérielle pour toute activité relevant du volet de son mandat touchant la cybersécurité qui contreviendrait à toute autre loi fédérale ou qui entraînerait l'acquisition par celui-ci d'information qui porterait atteinte à une attente raisonnable de protection en matière de vie privée des Canadiens (citoyens canadiens, résidents permanents ou personnes morales formées sous le régime d'une loi fédérale ou provinciale) et des personnes se trouvant au Canada (art 22(4) et 27, *Loi sur le CST*). Afin de mener efficacement des activités de cybersécurité, le CST acquiert de telles informations.

8. La *Loi sur le CST* établit deux types distincts d'autorisations ministérielles pour les activités de cybersécurité : celles délivrées pour les systèmes fédéraux (art 27(1)) et celles délivrées pour les systèmes non fédéraux désignés comme étant d'importance pour le gouvernement fédéral – systèmes non fédéraux – (art 27(2)), par exemple ceux liés aux secteurs de la santé, de l'énergie et des télécommunications.

9. Les autorisations qui se rapportent à des systèmes non fédéraux doivent satisfaire à deux exigences. Premièrement, les systèmes doivent avoir été désignés, par arrêté ministériel, comme étant importants pour le gouvernement fédéral (art 21, *Loi sur le CST*). L'*Arrêté ministériel désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada* (Arrêté sur les SDI), émis le 25 août 2020, définit de vastes catégories de systèmes désignés, dont l'une englobe les trois gouvernements territoriaux. Deuxièmement, le processus d'autorisation doit être lancé par le propriétaire ou l'exploitant du système non fédéral qui présente une demande écrite au CST pour mener les activités en cause (art 33(3), *Loi sur le CST*).

10. L'autorisation énonce les conclusions du ministre – les motifs, en fait – à l'appui des activités ou des catégories d'activités que le CST peut mener. L'autorisation est valide pendant une période maximale d'un an si le commissaire au renseignement l'approuve (art 36, *Loi sur le CST*).

11. Malgré une autorisation, la *Loi sur le CST* impose des limites quant aux activités de cybersécurité du CST. Les activités du CST ne doivent pas viser des Canadiens ou des personnes se trouvant au Canada et ne peuvent porter atteinte à la *Charte canadienne des droits*

et libertés (art 22(1), *Loi sur le CST*). Toutefois, le CST peut acquérir incidemment de l'information qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada (art 23(4), *Loi sur le CST*). Le terme « incidemment » signifie que l'information acquise n'a pas été délibérément recherchée (art 23(5), *Loi sur le CST*). Pour utiliser, analyser, conserver ou divulguer l'information, le CST est tenu par la loi de veiller à ce que des mesures pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada soient en place (art 24, *Loi sur le CST*).

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

    a) l'autorisation;
    b) la demande de la chef du CST (la chef) au ministre (la demande) datée du 26 septembre 2025, contenant dix-sept annexes, dont les suivantes :
        i. lettres de demande des trois gouvernements territoriaux;
        ii. deux arrêtés ministériels;
        iii. Rapport sur les résultats pour 2024-2025;
        iv. deux évaluations stratégiques de cybermenaces;
        v. Ensemble des politiques sur la mission en matière de cybersécurité (EPM) approuvé en août 2025;
        vi. registre des modifications apportées à l'EPM en matière de cybersécurité, mise à jour d'août 2025;
        vii. listes des organismes au sein des réseaux des gouvernements territoriaux;
    c) les réponses aux remarques du commissaire au renseignement;
    d) la note d'information de la chef à l'intention du ministre;
    e) le document d'information – aperçu des activités.

III. NORME DE CONTRÔLE

13. La *Loi sur le CR* exige que le commissaire au renseignement examine si les conclusions du ministre sont raisonnables. J'appliquerai donc la norme de la décision raisonnable, telle qu'elle est appliquée dans les contrôles judiciaires de mesures administratives.

14. Comme la Cour suprême du Canada l'a indiqué, lorsqu'elle procède au contrôle d'une décision selon la norme de la décision raisonnable, la cour de révision doit commencer son analyse à partir des motifs du décideur administratif. 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 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.

15. Les contraintes factuelles et juridiques pertinentes peuvent comprendre le régime législatif applicable et l'incidence de la décision. Le régime législatif applicable institué par la *Loi sur le CR* et la *Loi sur le CST* met en évidence la fonction de commissaire au renseignement en tant que mécanisme indépendant qui permet d'assurer un juste équilibre entre les mesures prises par le gouvernement à des fins de sécurité nationale et de renseignement et le respect de la primauté du droit ainsi que des droits et intérêts des Canadiens.

16. 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, lorsqu'il n'est pas convaincu qu'elles sont raisonnables, il « n'approuve pas » l'autorisation (art 20(1)b), *Loi sur le CR*). Dans les deux cas, le commissaire au renseignement doit motiver sa décision.

IV. ANALYSE

17. La demande de la chef est une demande de renouvellement des activités de cybersécurité autorisées que j'ai approuvées l'année dernière (décision CST-2024-07), avec l'ajout du déploiement de [...] au réseau du GTNO. Une description des activités de cybersécurité visées par l'autorisation figure dans l'annexe classifiée de la présente décision (annexe A). L'annexe facilite la lecture de la version de la présente décision qui sera tôt ou tard rendue publique, et permet de veiller à ce que la décision présente la nature des faits dont j'ai été saisi, lesquels ne seraient autrement accessibles que dans le dossier.

A. Dossier mis à jour

18. Dans mes décisions, je formule des remarques qui soulèvent des questions juridiques ou factuelles, dans le but d'améliorer le contenu des futurs dossiers ou de souligner autrement les questions que le CST devra examiner. Avant d'examiner les réponses du CST à certaines de mes dernières remarques, je tiens à souligner la réactivité générale du CST aux questions soulevées. Ce processus a entraîné des améliorations concrètes au processus d'autorisation ministérielle.

19. En ce qui concerne les réponses à mes remarques plus récentes, je suis convaincu que le CST fournit désormais une mise en contexte suffisante concernant l'information acquise incidemment qui se rapporte à un Canadien ou à une personne se trouvant au Canada (IRC). Le ministre reconnaît que, dans le cadre de ses activités, le CST « fera » l'acquisition d'information qui portera atteinte à une attente raisonnable de protection en matière de vie privée des Canadiens ou des personnes se trouvant au Canada ou qui contreviendra à toute autre loi fédérale. Je suis également satisfait de l'information détaillée contenue dans le rapport sur les résultats concernant les types d'informations que conserve le CST, l'échange de rapports avec les entités non fédérales, les répercussions possibles des vulnérabilités identifiées et la communication de rapports contenant de l'IRC à des partenaires internationaux (on indique qu'aucun rapport n'a été communiqué).

i. Lettres de demande

20. Dans la décision de l'année dernière (CST-2024-07), j'ai formulé une remarque selon laquelle le dossier présenté au ministre doit confirmer si l'entité non fédérale dispose du pouvoir conféré par la loi de recueillir et de communiquer l'information qui, en fin de compte, est recueillie par le CST dans le cadre de ses activités de cybersécurité. Les gouvernements territoriaux confirment dorénavant expressément leur pouvoir dans les lettres de demande.

21. À la suite de cette décision, j'ai fait d'autres remarques dans d'autres décisions de cybersécurité visant à améliorer davantage le contenu des lettres de demande. Dans la décision CST-2025-01, j'ai précisé qu'il serait utile que chaque lettre de demande donne un aperçu général des raisons pour lesquelles l'entité non fédérale demande le soutien du CST, tout en reconnaissant que

certains facteurs, comme les niveaux de classification, peuvent limiter le niveau de détail des lettres. Dans la décision CST-2025-07, j'ai mentionné que les lettres de demande pourraient être modifiées afin de mieux refléter si elles constituent la première demande d'assistance du CST qu'a fait l'entité, ou si elles visent à renouveler l'assistance en cours déjà fournie au titre d'une autorisation existante. Je constate que la lettre de GY indique que la demande est un « renouvellement » de l'entente avec le CST, mais la lettre du GN ne l'indique pas (ni la lettre du GTNO, mais elle précède ma remarque).

ii. Avis et consentement des utilisateurs

22. Une autre remarque qui a été abordée dans les décisions de cybersécurité antérieures concerne le consentement des personnes dont les informations peuvent être acquises par le CST lorsqu'il mène des activités dans les systèmes des entités non fédérales. Tel qu'il a été mentionné dans la décision CST-2025-06, le CST a entrepris de recommander aux entités non fédérales que leurs avis d'ouverture de session indiquent aux utilisateurs que l'information contenue ou communiquée dans les dispositifs et les réseaux des entités peut être utilisée à des fins de cybersécurité. Il peut s'agir d'informations personnelles et de communications privées qui peuvent être acquises incidemment et qui pourraient être utilisées, analysées, conservées ou divulguées.

23. Dans ce dossier, le CST explique qu'il a communiqué avec les trois entités non fédérales et a demandé qu'elles fournissent un aperçu des mesures prises pour fournir des avis d'ouverture de session à leurs utilisateurs. De plus, le CST a maintenant intégré cette question à ses procédures pour les nouveaux clients non fédéraux et est en train de demander cette information à d'autres clients non fédéraux existants. Je reconnais que le CST ne peut pas obliger les entités non fédérales à prendre des mesures précises, et que les exigences en matière d'avis et de consentement peuvent varier selon le territoire. Néanmoins, le CST s'engage à continuer de fournir à ses clients non fédéraux le libellé recommandé à utiliser dans les avis d'ouverture de session. Je suis reconnaissant de l'engagement continu du CST à donner suite à mes remarques.

iii. Possibilité de communiquer de l'information se rapportant à des Canadiens à des systèmes d'importance à l'extérieur du Canada

24. Dans ma récente décision CST-2025-07, j'ai formulé une remarque sur la nécessité pour le ministre de comprendre parfaitement comment l'IRC recueillie et conservée par le CST pourrait être communiquée à des fins de cybersécurité à des personnes ou à des catégories de personnes désignées, y compris les propriétaires ou exploitants de systèmes d'importance désignés par arrêté ministériel en vertu de l'article 21 de la *Loi sur le CST*. En somme, j'ai décrit comment l'*Arrêté ministériel désignant les destinataires de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui a été acquise, utilisée ou analysée dans le cadre des volets du mandat du CST touchant la cybersécurité et l'assurance de l'information* émis le 13 juin 2023, conformément à l'article 45 de la *Loi sur le CST* (arrêté ministériel de l'article 45), permet la communication d'IRC aux propriétaires ou exploitants de systèmes d'importance. J'ai constaté que le dossier ne reflétait pas les désignations de l'information électronique et des infrastructures de l'information des gouvernements de l'Ukraine et de la Lettonie comme des systèmes d'importance ni la possibilité qui en découle que l'IRC puisse donc être communiquée à ces gouvernements.

25. Le CST a indiqué que toute communication d'IRC à l'Ukraine ou à la Lettonie serait indiquée dans le rapport des résultats, tout comme tout autre partenaire international à qui de l'IRC a été communiquée. Le CST confirme également que l'annexe 2 de l'Arrêté sur les SDI ne contient actuellement aucune désignation.

26. Le point principal de ma remarque tient toujours. L'arrêté ministériel actuel permet la communication d'IRC à des propriétaires ou des exploitants de tout système d'importance. Le dossier comprend l'Arrêté sur les SDI d'août 2020. En l'absence de la mention d'un arrêté ministériel désignant un système d'importance, le dossier risque de donner au ministre et à moi-même un portrait incomplet du fait qu'il s'agit de la seule directive désignant les systèmes d'importance. La façon dont l'IRC est traitée et peut éventuellement être communiquée – en particulier à l'extérieur du Canada – est utile pour chacune de nos évaluations et devrait se refléter correctement dans le dossier.

iv. Mise à jour de l'EPM en matière de cybersécurité

27. Le dossier comprend une version récemment modifiée de l'EPM en matière de cybersécurité datée du 8 août 2025, ainsi qu'un registre des modifications qui indique les dispositions nouvelles et modifiées de l'EPM. Certaines modifications ont été apportées pour s'aligner sur l'*Ensemble de politiques sur la mission en matière de renseignement étranger*, tandis que d'autres donnent suite à des remarques que j'ai formulées dans des décisions antérieures. Dans l'ensemble, je constate que l'EPM fournit des libellés supplémentaires et d'autres exemples pour clarifier les paramètres acceptables de certaines activités, l'interdiction de mener des activités visant des Canadiens ou des personnes se trouvant au Canada et pour refléter la nouvelle Stratégie nationale de cybersécurité de 2025. Certains changements sont également apportés pour clarifier la section relative à la divulgation d'IRC lorsqu'il existe des motifs raisonnables de croire que l'information est utile en cas de danger imminent de mort ou de lésions corporelles graves. L'EPM indique maintenant que tout cas de ce genre doit être signalé expressément à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (plutôt qu'aux « organismes d'examen compétents »); je m'attends à ce que ces cas soient également inclus dans les rapports sur les résultats et les rapports de fin d'autorisation.

28. D'autres modifications apportées à l'EPM concernent les calendriers de conservation de l'IRC et de l'information se rapportant à des non-Canadiens acquise au titre d'une autorisation, et les exigences liées aux communications protégées par le secret professionnel.

29. Je remarque que les modifications apportées aux dispositions sur le secret professionnel reflètent celles décrites dans une décision de renseignement étranger (CST-2025-04, paragraphes 58 à 60), qui insiste sur l'importance de limiter l'accès aux communications potentiellement protégées par le secret professionnel. Dans ma décision, j'ai suggéré que le CST envisage de délimiter son processus avec des termes plus définitifs et je suis d'avis que la restriction selon laquelle « une fois reconnue, le personnel limitera strictement l'accès à la communication selon le principe du besoin de savoir » prévue dans l'EPM constitue une étape positive dans cette direction.

v. Incident de conformité

30. Tel qu'il a été mentionné dans la décision de l'année dernière au paragraphe 78, le rapport de fin d'autorisation de 2022-2023 pour les activités liées au GTNO a décrit un incident de conformité concernant la trop longue conservation de certaines informations en raison d'une obligation de préservation de la preuve. Le plus récent rapport de fin d'autorisation pour la période du 30 novembre 2023 au 14 novembre 2024 fournit une mise à jour de l'incident et des mesures prises pour y remédier.

31. Le présent dossier ne fournit aucune mise à jour sur ces étapes. Je suis convaincu que le prochain rapport de fin d'autorisation traitera de la levée de l'obligation de préservation de la preuve pertinente et confirmera la suppression des informations conservée pendant trop longtemps. Je suis toujours du même avis formulé dans la décision CST-2024-06 que les exceptions au traitement habituel de l'information au titre d'une autorisation, comme celles causées par l'obligation de préservation de la preuve, devraient être énoncées dans l'autorisation.

B. Les conclusions du ministre sont-elles raisonnables (art 34(1), *Loi sur le CST*)

32. Le ministre conclut qu'il existe des motifs raisonnables de croire que les activités autorisées sont raisonnables parce que les cyberattaques sont de plus en plus sophistiquées et difficiles à détecter. Les conclusions expliquent que le CST doit acquérir de grandes quantités d'informations pour détecter et analyser les cybercompromissions et qu'il n'est pas possible de savoir à l'avance quelles informations seront particulièrement utiles ou nécessaires. Enfin, le ministre conclut que l'acquisition de l'information est nécessaire pour prendre des mesures d'atténuation en temps réel, afin de prévenir les cybercompromissions.

33. Le ministre se fie également à la compromission antérieure de l'un des gouvernements territoriaux et aux preuves continues de vulnérabilités et d'activités malveillantes vécues par chacun des gouvernements territoriaux. Enfin, il s'appuie sur la confidentialité et l'importance des infrastructures de l'information des gouvernements territoriaux ainsi que de l'information qu'elles contiennent.

34. Le caractère raisonnable et proportionnel doit être évalué « compte tenu de la nature de l'objectif à atteindre » (art 34(1), *Loi sur le CST*).

35. Une autorisation relative à un système non fédéral comme celle dont je suis saisi doit servir à protéger son infrastructure de l'information contre les méfaits, l'utilisation non autorisée ou la perturbation de son fonctionnement. À l'inverse, l'autorisation relative à un système fédéral doit servir à aider à protéger l'infrastructure du système fédéral.

36. Les conclusions du ministre sur le caractère raisonnable et proportionnel énoncent l'objectif de différentes façons. La première description du ministre de l'objectif est d'aider à protéger les « systèmes fédéraux et les systèmes d'importance » (soulignement ajouté). Le paragraphe 57 des conclusions du ministre mentionne également l'information acquise à partir de capteurs déployés utilisés « pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes fédéraux et, par la suite, à ceux désignés comme des systèmes d'importance ». Le ministre termine ensuite en énonçant l'objectif comme étant « d'aider à protéger l'information électronique et les infrastructures de l'information de chacun des gouvernements territoriaux ».

37. D'après une lecture globale et contextuelle du dossier (*Vavilov*, paragraphe 97), je suis toujours convaincu que l'objectif à atteindre n'a pas changé par rapport aux autorisations antérieures. Le paragraphe 15 de la demande fait une distinction utile entre le « principal objectif » de protéger les infrastructures des gouvernements territoriaux et plusieurs « sous-objectifs », y compris l'utilisation de l'information acquise pour aider à protéger les systèmes fédéraux et d'autres systèmes non fédéraux d'importance. De même, le paragraphe 59 de l'autorisation fait référence à la protection des infrastructures des gouvernements territoriaux [...] protéger les systèmes fédéraux et autres systèmes non fédéraux d'importance. À mon avis, ces deux références représentent le plus fidèlement l'objectif général compris lors de la lecture du dossier au complet, qui est d'abord et avant tout de protéger les systèmes des gouvernements territoriaux.

38. À la lumière de ce qui précède, les futures autorisations doivent veiller à ce que l'objectif soit décrit de façon uniforme tout au long de l'autorisation et de la demande et qu'il reflète correctement le type d'autorisation recherchée. Conformément à la *Loi sur le CST*, l'objectif

principal d'une autorisation relative à une entité non fédérale doit être de protéger les systèmes de cette entité.

39. J'ai déjà fait valoir qu'une justification précise devrait être formulée pour justifier la nécessité de poursuivre les activités qui ont déjà été autorisées à plusieurs reprises (décision CST-2024-06 au para 78; décision CST-2024-07 au para 84). Ici, les motifs détaillés du ministre quant à la nécessité de l'autorisation font également office de justification. Le ministre fonde sa conclusion sur l'importance stratégique de l'Arctique pour le Canada, la posture actuelle de chaque gouvernement territorial en matière de cybersécurité ainsi que les cybermenaces auxquelles les territoires ont été confrontés et devraient continuer d'y être confrontées.

40. Je remarque que le dossier ne comprend pas de mises à jour sur l'état des recommandations en suspens du CST que le GTNO était en train de mettre en œuvre. Je comprends que la situation peut s'expliquer par le changement global dans la justification de la participation du CST, qui s'éloigne de l'intervention en cas d'un incident en particulier pour maintenir une présence plus proactive en raison de l'importance stratégique des territoires. Néanmoins, j'avais mentionné la même absence dans la décision de l'année dernière (para 33) et je m'attendais à ce qu'elle soit abordée dans le dossier de cette année. Bien que la description du ministre des motifs pour lesquels l'autorisation est nécessaire dans ce cas me permet d'être convaincu que sa conclusion est raisonnable, j'insiste à nouveau sur le fait que je m'attends à ce que le dossier permette au ministre de comprendre les progrès réalisés, y compris en ce qui a trait aux recommandations précises que le CST avait formulées précédemment.

41. Le ministre explique que les activités de cybersécurité énoncées dans l'autorisation entraîneront l'acquisition d'informations à l'égard desquelles les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée. Je souligne, toutefois, que je suis convaincu que les activités de cybersécurité énoncées dans l'autorisation respectent l'exigence prévue par la loi selon laquelle les activités du CST ne doivent pas viser des Canadiens ou des personnes se trouvant au Canada.

42. Compte tenu de ce qui précède, j'estime que les conclusions du ministre quant au caractère raisonnable des activités énoncées dans l'autorisation sont raisonnables.

C. Les conclusions du ministre sont-elles proportionnelles (art 34(1), *Loi sur le CST*)

43. Le ministre conclut également qu'il a des motifs raisonnables de croire que les activités autorisées sont « proportionnelles compte tenu de la manière dont elles sont menées, et parce qu'elles ont un lien rationnel avec l'objectif à atteindre et ne porteront qu'une atteinte minimale aux droits et libertés de tiers », ainsi qu'à la capacité de tiers d'accéder à de l'équipement ou à des infrastructures ou de les utiliser.

44. Pour en arriver à cette conclusion, le ministre s'appuie, comme l'année dernière, sur sept mesures et contrôles internes qu'applique le CST après l'acquisition de l'information. Je peux suivre le raisonnement du ministre lorsqu'il s'est appuyé sur ces mesures. L'accès à l'information acquise se limite aux employés désignés du CST qui sont formés pour manipuler ce type d'information et qui l'utilisent selon le principe du besoin de savoir pour effectuer leur travail. Le ministre était conscient des droits en matière de vie privée en jeu et il a énoncé les mesures mises en place pour les protéger.

45. Dans la décision de l'année dernière concernant les trois mêmes entités, j'ai souligné que le dossier n'indiquait pas la quantité totale d'informations (c.-à-d. des « items ») acquises au cours d'une autorisation antérieure. Un nombre total estimatif de « données » acquis est maintenant fourni, et on a expliqué le passage de la mesure en « items » à la mesure en « données ». Les chiffres fournis confirment que le CST a acquis un nombre considérable de données, mais ne conservait qu'une petite partie, ce qui représente bien moins de 1 % du total.

46. En ce qui concerne les lois fédérales auxquelles le CST pourrait contrevenir, je suis convaincu que le ministre conclut raisonnablement qu'elles seront proportionnelles parce que les activités doivent respecter la portée de celles décrites dans la demande. À titre de mesure de protection supplémentaire, en cas de contravention à une loi fédérale qui ne figure pas dans la demande, la chef en informera le ministre et le commissaire au renseignement.

47. Comme l'indique l'exposé à l'intention du ministre, le déploiement prévu d'un autre type de solution de cybersécurité ([…]) pour le GTNO représente […]. Le déploiement est à la demande

expresse du GTNO, la demande insistant sur la compromission sophistiquée du réseau du GTNO.

48. Dans de nombreuses parties du dossier, les mentions du déploiement des solutions existantes ont simplement été mises à jour pour inclure également la mention de la solution qui doit être déployée. Je l'interprète comme portant à croire implicitement que le fonctionnement de la nouvelle solution dans ce nouveau contexte ne devrait pas différer fondamentalement de celui des solutions déjà déployées, ni modifier de manière fondamentale l'évaluation du ministre du caractère proportionnel des activités.

49. Néanmoins, les conclusions du ministre auraient pu être renforcées en établissant expressément une telle évaluation. Comme il est indiqué dans le nouveau libellé dans l'EPM mis à jour, les évaluations des risques peuvent « aider à décider si les risques potentiels que pose une activité sont raisonnables et proportionnels » lorsque l'on prend en considération l'objectif de l'activité. Je remarque qu'une note de bas de page qui ferait partie des modifications apportées à l'EPM (qui ne semble pas avoir réellement été incluse dans l'EPM mis à jour) indique que les changements qui pourraient nécessiter une évaluation des risques comprennent le déploiement d'une activité ou d'un service dans une nouvelle catégorie de clients, comme une entité non fédérale. Cela semble être le cas ici.

50. Comme je l'ai mentionné précédemment, les déploiements dans des systèmes non fédéraux sont sans doute l'activité la plus incidemment intrusive pour les Canadiens et les personnes se trouvant au Canada (décision CST-2024-06 au para 80). Je souligne que, dans ce cas particulier, le déploiement pourrait englober non seulement les ministères principaux du gouvernement territorial, mais aussi des agences et organismes indépendants qui font « partie de son réseau » et qui sont confrontés à des enjeux particuliers et accrus en matière de protection de la vie privée ([…]). Il ne me semble pas clair, d'après le dossier, si une évaluation des risques tenant compte de ce contexte a été effectuée.

51. En fin de compte, en m'appuyant sur le déploiement demandé par le gouvernement territorial et sur le fait que rien dans le dossier ne laisse entendre que le nouveau déploiement modifierait

fondamentalement le caractère proportionnel des activités, je suis convaincu que les conclusions du ministre concernant le caractère proportionnel des activités sont raisonnables.

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

52. Lorsque le ministre conclut qu'il y a des motifs raisonnables de croire que les activités sont raisonnables et proportionnelles en vertu du paragraphe 34(1) de la *Loi sur le CST*, il peut délivrer une autorisation de cybersécurité pour aider à protéger les systèmes non fédéraux s'il conclut qu'il a des motifs raisonnables de croire que les trois conditions énoncées au paragraphe 34(3) de la *Loi sur le CST* sont remplies :

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

    ii. l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux;

    iii. les mesures en place 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 au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire (alinéa 34(3)a))

53. Le ministre estime qu'il est nécessaire de conserver l'information non évaluée jusqu'à 12 mois parce qu'il n'est pas possible pour le CST de déterminer à l'avance quelles informations seront utiles pour découvrir et prévenir les cyberactivités malveillantes. Comme l'a expliqué le ministre, cette durée est nécessaire pour permettre une analyse rétroactive. En effet, l'efficacité des activités du CST dépend de la capacité à recouper et à analyser de multiples sources d'informations déjà acquises, y compris les indicateurs de compromission découverts. De nouvelles vulnérabilités sont continuellement découvertes, et une période de conservation de 12 mois permet au CST de remonter aux origines d'un événement ou d'examiner son évolution au fil du temps. Le fait de comparer une compromission avec des données non évaluées ou des activités malveillantes non détectées aide le CST à élaborer de meilleures mesures d'atténuation

et des cyberinterventions qui peuvent être utilisées non seulement pour les systèmes non fédéraux dans le cas présent, mais aussi pour les autres systèmes désignés comme étant d'importance et les systèmes fédéraux.

54. Il s'agit d'une condition de l'autorisation, que toutes les informations acquises sont traitées conformément à la politique opérationnelle pertinente du CST. L'information est conservée conformément à l'EPM, qui contient un calendrier de conservation pour les différentes catégories d'informations qui peuvent être acquises.

55. Le ministre explique que les périodes de conservation tiennent compte de la période minimale obligatoire de deux ans prévue dans la *Loi sur la protection des renseignements personnels* pour des renseignements personnels utilisés à des fins administratives (*Règlement sur la protection des renseignements personnels*, DORS/83-508, art 4), et par le pouvoir de gestion de l'information et d'aliénation ou d'élimination des documents conféré par la *Loi sur la Bibliothèque et les Archives du Canada*, LC 2004, c 11.

56. Avant la fin de 12 mois, toutes les informations non évaluées seront automatiquement supprimées, à moins qu'elles ne soient jugées « nécessaires » ou « essentielles » pour aider à protéger les systèmes non fédéraux. Les informations jugées « nécessaires » ou « essentielles » peuvent être conservées jusqu'à ce qu'elles « ne soient plus utiles dans le cadre du volet du mandat du CST touchant la cybersécurité et l'assurance de l'information ». Le critère du caractère « nécessaire » s'applique à l'information qui, de par sa nature, ne contient aucun élément se rapportant à un Canadien ou à une personne se trouvant au Canada. Le critère du caractère « essentiel » s'applique à l'information identifiée comme se rapportant à un Canadien ou une personne se trouvant au Canada.

57. L'information conservée parce qu'elle est essentielle doit être examinée par un gestionnaire des opérations tous les trimestres afin de vérifier si elle est toujours essentielle; l'information qui n'est plus essentielle doit être supprimée. Je remarque que la mise à jour de l'EPM n'a pas corrigé une divergence apparente que j'ai précédemment soulignée en ce qui concerne le libellé de cette exigence; tandis que l'autorisation prévoit que les gestionnaires des opérations

« doivent examiner » l'IRC conservée, l'EPM indique qu'on leur « rappelle d'examiner » (décisions CST-2025-07 au para 45 et CST-2025-01 aux paras 78 à 82).

58. En tenant compte de la définition des termes « nécessaire » et « essentiel », il est utile de reconsidérer la délimitation dans la *Loi sur le CST* entre les autorisations de cybersécurité pour les systèmes fédéraux et celles qui concernent les systèmes non fédéraux. Dans le cas des autorisations de cybersécurité relatives à des entités non fédérales, le ministre doit conclure que l'information acquise par le CST au titre de l'autorisation sera nécessaire, ou, dans le cas d'IRC essentielle, pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes d'importance (art 34(3)c)(ii) et 34(3)d)(ii)) (soulignement ajouté).

59. Je souligne que le terme « essentiel » n'est pas défini de façon uniforme dans l'ensemble du dossier. Le paragraphe 71 de l'autorisation, qui définit le terme aux fins de l'autorisation, reprend tel quel le libellé de la loi. Toutefois, le paragraphe 66 de l'autorisation stipule que l'information est conservée si elle est essentielle ou nécessaire pour aider à protéger les « systèmes fédéraux et les systèmes d'importance » (soulignement ajouté). Le paragraphe 123 de la demande comprend une définition ne mentionnant que les systèmes d'importance, mais élargissant la portée du critère « essentiel » afin d'inclure l'information jugée comme donnant un aperçu de […], dans le but d'aider à protéger les systèmes d'importance. L'EPM comprend également cette même définition plus large, mais s'étend à la protection des systèmes fédéraux ou des systèmes d'importance (annexe E de l'EPM).

60. Je considère que le nombre accru de mentions de l'information jugée essentielle pour protéger à la fois les systèmes fédéraux et les systèmes non fédéraux d'importance reflète l'expérience du CST selon laquelle, en pratique, l'information qui est essentielle à la protection des systèmes non fédéraux sera également essentielle à la protection des systèmes fédéraux, et vice versa. En effet, vu sous l'angle de cette expérience, la distinction faite dans la *Loi sur le CST* sur ce point commence à sembler être artificielle.

61. Ce point ne modifie cependant pas le fait que les conditions sont expressément énoncées dans la *Loi sur le CST*. Pour qu'elle soit conservée, l'IRC acquise au titre d'une autorisation délivrée en vertu du paragraphe 27(2) doit être essentielle pour découvrir, isoler, prévenir ou atténuer les

dommages aux systèmes non fédéraux d'importance (art 34(3)d)(ii)) (soulignement ajouté). Comme je l'ai évalué à l'égard de l'objectif de l'autorisation, je suis convaincu que les conclusions du ministre respectent cette condition, mais je souligne qu'il faudrait prendre soin d'être uniforme en formulant les critères « essentiel » et « nécessaires », d'une manière qui reflète la condition prévue par la loi.

62. J'estime que la conclusion du ministre concernant la période d'évaluation de 12 mois est raisonnable. En effet, le fait de conserver l'information pendant la durée nécessaire permet au CST de mener efficacement ses activités de cybersécurité et d'élaborer les cyberinterventions requises afin de suivre le rythme de l'évolution rapide des techniques utilisées par les auteurs de menaces liées à des logiciels malveillants. Cela permet une meilleure protection des systèmes non fédéraux, et par conséquent, des systèmes fédéraux. Je souscris également à la conclusion du ministre selon laquelle l'information « nécessaire » ou « essentielle » pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux peut être conservée jusqu'à ce qu'elle ne soit plus utile, à condition qu'elle soit toujours « nécessaire » ou « essentielle » à cette fin.

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

63. Les conclusions du ministre réaffirment que les activités de cybersécurité du CST ne sont efficaces que si le CST est en mesure d'acquérir une vaste gamme d'informations. La demande indique que les mesures commerciales en place chez les entités non fédérales sont insuffisantes pour détecter et contrer les méthodes et les capacités sophistiquées déployées par des auteurs de menace avancés et tenaces. Les activités de renseignement étranger du CST lui donnent une connaissance hors du commun des capacités, des intentions et des activités de ces auteurs.

64. Le ministre donne des exemples de la façon dont le CST peut utiliser l'information acquise au titre de l'autorisation pour appuyer des activités au titre d'autres autorisations de cybersécurité et d'autres volets de son mandat, y compris les activités autorisées concernant d'autres systèmes non fédéraux d'importance.

65. Compte tenu de ce qui précède, je suis convaincu que les conclusions du ministre sont raisonnables.

> *iii. Les mesures visant à protéger la vie privée permettront de faire en sorte 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 (alinéa 34(3)d))*

66. 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 de l'information qui se rapporte à eux et qui a été acquise dans le cadre des volets de son mandat touchant la cybersécurité et l'assurance de l'information. J'insiste, comme je l'ai fait précédemment, sur le fait que de telles mesures revêtent une importance encore plus grande lorsque le rôle (ou la portée du réseau) d'une entité non fédérale est directement et intrinsèquement lié à de l'information confidentielle à l'égard de laquelle il existe une attente raisonnable de protection en matière de vie privée (décision CST-2024-06).

67. En ce qui concerne la conservation de l'IRC, le ministre réitère que l'information ne peut être utilisée ou conservée que si elle est essentielle pour découvrir, isoler ou prévenir des dommages aux systèmes non fédéraux. Le ministre précise en outre que l'information doit être traitée conformément à l'article 8 de l'EPM, qui prévoit que les justifications relatives au caractère essentiel – déterminées au moyen de processus manuels ou automatisés – doivent être consignées (art 8.2.2, EPM). À mon avis, cette mesure contribue à faire en sorte que le CST respecte son obligation prévue à l'article 24 et appuie les conclusions du ministre.

68. De plus, le ministre énonce des conditions et des restrictions supplémentaires pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada. Notamment, le CST mettra en œuvre des mesures raisonnables pour limiter l'accès à l'information et effectuera, dans la mesure du possible, des analyses au moyen de processus automatisés qui limitent l'exposition des employés à l'information non évaluée. Le CST établira et tiendra à jour des procédures pour vérifier si ses activités sont menées conformément à l'autorisation.

69. Pour que le CST communique de l'IRC, il faut que la communication soit nécessaire pour aider à protéger les systèmes des gouvernements territoriaux, les systèmes fédéraux ou d'autres systèmes d'importance. Les conclusions du ministre et le dossier reflètent la condition prévue à l'article 44 de la *Loi sur le CST*. L'information est seulement communiquée aux personnes ou aux catégories de personnes désignées en vertu de l'article 45, qui traite de l'Arrêté ministériel. Ces personnes ou catégories de personnes comprennent les propriétaires ou les administrateurs de systèmes ou de réseaux informatiques utilisés par le gouvernement fédéral ou une entité non fédérale, ainsi que les personnes et les catégories de personnes autorisées au sein d'entités étrangères avec lesquelles le CST a conclu des ententes.

70. Avant de communiquer de l'IRC, le CST a également en place des mesures qui doivent être suivies (art 24, EPM), dont la suppression de l'information nominative. L'EPM définit les niveaux d'approbation requis pour la communication de l'IRC, dont les approbations doivent être consignées.

71. Je remarque que, dans les lettres de demande adressées au CST, chaque entité non fédérale demande que tous les renseignements personnels, l'information qui identifie l'entité non fédérale ou l'information exclusive de l'entité non fédérale soient masqués avant qu'ils ne soient communiqués à l'extérieur du CST et de l'entité non fédérale. L'autorisation du ministre elle-même prévoit que la communication de l'information acquise demeure assujettie à de telles conditions. Dans la décision CST-2025-01, j'ai souligné que diverses références dans le dossier ont rendu incertaine la façon dont ces demandes de masquage interagissent avec les politiques du CST dans l'EPM et la façon dont elles sont donc opérationnalisées. Je m'attends à ce que les dossiers à venir fournissent des éclaircissements à ce sujet.

72. L'EPM établit des politiques détaillées visant à contrôler et à protéger l'IRC qui est acquise au titre d'une autorisation de cybersécurité. À mon avis, lorsqu'elles sont suivies, ces mesures permettent au CST de respecter efficacement l'exigence prévue par la loi de protéger suffisamment cette information. Je suis donc convaincu que les conclusions du ministre sont raisonnables.

V. REMARQUES

73. J'aimerais faire les trois remarques suivantes, qui ne modifient pas mes constatations concernant le caractère raisonnable des conclusions du ministre.

A. Clarification du rapport sur les résultats

74. Le rapport sur les résultats comprend des statistiques sur le nombre d'utilisateurs surveillés par l'une des solutions de cybersécurité déployées dans les réseaux des gouvernements territoriaux. Je remarque que le nombre d'utilisateurs surveillés varie considérablement par rapport au plus récent rapport de fin d'autorisation; les nombres d'utilisateurs ont [...] dans les trois territoires. Aucune explication n'est fournie.

75. Comme il a été mentionné précédemment dans la décision (CST-2024-02 au para 87), lorsque l'information présentée dans un rapport sur les résultats ou le rapport de fin d'autorisation varie considérablement d'un rapport à l'autre, une explication doit être fournie. Par conséquent, je m'attends à ce que le prochain rapport de fin d'autorisation fournisse une explication de la variation des nombres d'utilisateurs.

B. Portée de l'autorisation

76. Comme il est devenu la norme, la demande comprend des annexes qui énumèrent les ministères et organismes « au sein » du réseau de chaque gouvernement territorial qui sont admissibles aux activités de cybersécurité et d'assurance de l'information du CST. Ma comparaison des listes des organismes qui sont décrits comme étant « au sein » d'un des réseaux du gouvernement territorial montre que [certains organismes] qui faisaient partie de l'annexe de l'année dernière ont été retirés sans explication. Je reconnais que le CST ne contrôle pas les organismes qui utilisent les infrastructures de l'information appartenant à chacun des gouvernements territoriaux. Toutefois, étant donné que la liste indique la portée potentielle de l'autorisation et de l'information qui pourrait être acquise, et que la nature d'un organisme peut déterminer s'il détient de l'information qui soulève des considérations particulières en matière de protection de la vie privée, le fait qu'un organisme est ajouté ou retiré de la liste d'admissibilité pourrait être

pertinent pour le ministre et moi-même. Le CST doit donc s'efforcer de veiller à ce que la liste soit exacte et de résumer toute modification apportée à la liste dans le dossier.

C. Évaluation de la sensibilité de l'IRC

77. Comme il est indiqué dans le dossier, l'EPM est traité comme un document évolutif qui est mis à jour périodiquement pour tenir compte de l'évolution des lois et des politiques. Je suis convaincu que les mises à jour les plus récentes améliorent les directives mises à la disposition des employés du CST qui mettent en œuvre les activités énoncées dans les autorisations. Les modifications apportées à l'EPM et les divers organismes qui utilisent les infrastructures électroniques des gouvernements territoriaux m'amènent à faire la remarque suivante.

78. Dans des décisions antérieures, j'ai souligné le fait que les activités de cybersécurité peuvent mener à la collecte d'informations hautement sensibles, par exemple de l'information sur l'état de santé d'une personne. L'EPM explique que le CST utilise une approche contextuelle pour déterminer le niveau de sensibilité de l'IRC et que des mesures de protection de la vie privée plus strictes sont en place pour l'IRC plus sensible. Ce cadre s'applique également à la communication de l'information.

79. Bien qu'il ne soit pas possible d'énumérer de façon exhaustive les facteurs à prendre en considération au moment d'évaluer la sensibilité de l'IRC, je tiens à m'assurer que les employés du CST sont conscients de la sensibilité de l'information qui se rapporte à des institutions fondamentales canadiennes, comme nos processus judiciaires (p. ex., la confidentialité des délibérations), les institutions démocratiques (p. ex., la communication entre les électeurs et leurs représentants élus) et la presse libre (p. ex. la protection des sources journalistiques). J'encourage le CST à envisager de mentionner expressément ces éléments dans l'EPM comme des facteurs à prendre en considération au moment d'évaluer la sensibilité de l'IRC.

VI. CONCLUSIONS

80. 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* à l'égard des activités énumérées au paragraphe 90 de l'autorisation sont raisonnables.

81. J'approuve donc, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, l'autorisation de cybersécurité pour des activités menées dans des infrastructures non fédérales délivrée par le ministre le 9 octobre 2025.

82. 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.

83. 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 réaliser les éléments de son mandat au titre des alinéas 8(1)a) à c) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, LC 2019, c 13, art 2.

Le 5 novembre 2025

(Original signé)

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