

Dossier : CST-2025-01



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

AFFAIRE INTÉRESSANT UNE AUTORISATION DE CYBERSÉCURITÉ POUR DES  
ACTIVITÉS SUR DES INFRASTRUCTURES NON FÉDÉRALES  
EN VERTU DU PARAGRAPHE 27(2) DE LA  
*LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS ET*  
DE L'ARTICLE 14 DE LA *LOI SUR LE COMMISSAIRE AU RENSEIGNEMENT*



## DÉCISION

1. Le [...], 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 de la Défense nationale (ministre) a délivré une autorisation de cybersécurité pour des activités menées dans des infrastructures non fédérales (l'autorisation) – [...].
2. Le [...], le Bureau du commissaire au renseignement a reçu l'autorisation à des fins d'examen et d'approbation, au titre de la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*).
3. Dans la lettre datée du [...], l'entité non fédérale a demandé que le Centre de la sécurité des télécommunications (CST) mène des activités de cybersécurité sur son infrastructure d'information. Cette demande [...]. En effet, comme l'a affirmé le ministre, l'un des objectifs de l'autorisation est de permettre au CST de fournir des services essentiels de cybersécurité à l'entité non fédérale [...]. Une compromission de l'information et des systèmes électroniques de l'entité non fédérale [...].
4. Dans sa lettre accompagnant l'autorisation, le ministre exprime que, compte tenu de la prévalence des menaces pour la cybersécurité et de l'importance de protéger [...], il me serait reconnaissant de pouvoir procéder rapidement à mon examen « dans toute la mesure du possible ».
5. Je suis d'accord avec le ministre pour dire que mon examen doit être effectué rapidement. Je suis convaincu que le contexte de la présente autorisation est un cas où il serait avantageux pour l'entité non fédérale, et par extension pour les Canadiens, que les solutions de cybersécurité du CST soient mises en œuvre le plus tôt possible. [...] est de la plus haute importance.
6. Je suis convaincu que l'entité non fédérale en question appartient à une catégorie d'infrastructures d'information désignée par le ministre comme étant d'importance pour le gouvernement fédéral (art 21(1), *Loi sur le CST*).

7. Je suis également convaincu que les conclusions que le ministre a tirées en application des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités énumérées au paragraphe 76 de l'autorisation sont raisonnables.
8. Après avoir examiné les conclusions du ministre et le dossier, je suis convaincu que le CST prendra les mesures appropriées pour protéger l'information se rapportant à des Canadiens qui sera recueillie dans le cadre des activités de cybersécurité du CST. De telles informations ne doivent être conservées que conformément aux obligations du CST prévues dans sa loi et ses politiques.
9. Je constate que dans sa lettre de demande au CST, l'entité non fédérale indique que le CST doit masquer tous les renseignements personnels ou exclusifs avant qu'ils ne soient communiqués. Je crois comprendre que le CST se conformera à cette demande.
10. L'entité non fédérale n'a pas été victime d'une cybercompromission connue. L'autorisation a donc été délivrée de façon proactive pour s'assurer que les systèmes de l'entité non fédérale sont protégés et [...].
11. Comme il est indiqué dans la décision CST-2024-07, le ministre peut délivrer une autorisation de cybersécurité à des fins proactives ou préventives, pourvu qu'il existe un fondement factuel pour obtenir l'aide du CST. En effet, le volet du mandat du CST touchant la cybersécurité et l'assurance de l'information comprend précisément de fournir « des avis, des conseils et des services afin d'aider à protéger » les systèmes d'importance pour le gouvernement fédéral (art 17(a), *Loi sur le CST*). Le fondement factuel exige que, même sans cybercompromission existante, une cybermenace pour l'entité non fédérale doit être suffisamment démontrée. Je suis convaincu que le dossier et les conclusions du ministre établissent ce fondement factuel.
12. Dans la décision CST-2024-05, j'ai conclu que l'alinéa 20(1)a) de la *Loi sur le CR* n'exige pas que je rende ma décision écrite et mes motifs simultanément. En effet, la Loi me permet d'approuver une autorisation ministérielle et, par la suite, de donner tous mes motifs

dans le délai prévu par la loi de 30 jours. Je suis d'avis que, lorsque le commissaire au renseignement juge que les conclusions du ministre sont raisonnables dans un contexte qui nécessite ou tire avantage d'une approbation accélérée, la rédaction des motifs du commissaire au renseignement ne devrait pas retarder la mise en œuvre des solutions de cybersécurité du CST.

13. Je trouve que la présente situation est un tel contexte.
14. Par conséquent, conformément à l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation visant des activités de cybersécurité sur des infrastructures non fédérales; l'ensemble de mes motifs suivront.
15. 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.



(Original signé)

---

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