CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

LA CYBERSÉCURITÉ DES RENSEIGNEMENTS PERSONNELS DANS LE NUAGE

Rapport du Comité permanent des comptes publics

John Williamson, président

OCTOBRE 2024
44e LÉGISLATURE, 1re SESSION

LA CYBERSÉCURITÉ DES RENSEIGNEMENTS PERSONNELS DANS LE NUAGE

Rapport du Comité permanent des comptes publics

Le président
John Williamson

OCTOBRE 2024

44e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DES COMPTES PUBLICS

PRÉSIDENT

John Williamson

VICE-PRÉSIDENTES

Jean Yip

Nathalie Sinclair-Desgagné

MEMBRES

Valerie Bradford

Blake Desjarlais

Iqra Khalid

John Nater

Brenda Shanahan

Jake Stewart

Arnold Viersen

Patrick Weiler

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Peter Fragiskatos

Michael Kram

Stephanie Kusie

Dane Lloyd

Brian Masse

Kelly McCauley

Maninder Sidhu

GREFFIERS DU COMITÉ

Hilary Smyth

Cédric Taquet

BIBLIOTHÈQUE DU PARLEMENT

Recherche et éducation

Dillan Theckedath, analyste

Mahdi Benmoussa, analyste

LE COMITE PERMANENT DES COMPTES PUBLICS

a l'honneur de présenter son

QUARANTE-QUATRIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(3)g) du Règlement, le Comité a étudié le Rapport 7, La cybersécurité des renseignements personnels dans le nuage, 2022 — Rapports 5 à 8 de la vérificatrice générale du Canada et a convenu de faire rapport de ce qui suit :

CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

LA CYBERSÉCURITÉ DES RENSEIGNEMENTS PERSONNELS DANS LE NUAGE

PRINCIPAUX CONSTATS DE LA VÉRIFICATRICE GÉNÉRALE DU CANADA

- Il y avait des faiblesses dans les contrôles des ministères pour prévenir les cyberattaques, les détecter et intervenir en conséquence.
- Les responsabilités et les rôles en matière de cybersécurité infonuagique étaient imprécis et incomplets.
- Le Secrétariat du Conseil du Trésor du Canada n'avait pas fourni de modèle d'établissement des coûts des services infonuagiques aux ministères ou ne leur avait proposé aucune méthode en matière de financement.
- Services publics et Approvisionnement Canada et Services partagés Canada n'avaient pas inclus de critères environnementaux dans le cadre de leurs processus d'approvisionnement en services infonuagiques[1].

1 Bureau du vérificateur général du Canada (BVG), La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, Survol.

Résumé des recommandations du comité et échéancier

Tableau 1 — Résumé des recommandations du comité et échéancier

Recommandation	Mesure recommandée	Échéancier
Recommandation 1	Le Secrétariat du Conseil du Trésor du Canada présente au Comité permanent des comptes publics de la Chambre des communes un rapport d'étape sur : A) la façon dont ont été mises en œuvre les exigences relatives aux mesures de sécurité dans les contrats de services infonuagiques qui découlent d'arrangements en matière d'approvisionnement établis par Services publics et Approvisionnement Canada; B) la façon dont il a précisé qui est responsable de la validation initiale et de la surveillance en continu des mesures de sécurité d'informatique en nuage, ainsi que les processus à suivre.	le 31 janvier 2025
Recommandation 2	Le SCT doit présenter au Comité un rapport d'étape sur la façon dont il s'est assuré que le Plan de gestion des événements de cybersécurité du gouvernement du Canada s'applique à l'environnement infonuagique en évolution et aux responsabilités partagées. En outre, le rapport d'étape doit indiquer comment le plan sera examiné et testé chaque année, et comment il sera mis à jour; il doit aussi inclure la procédure pour le suivi annuel auprès des ministères afin de s'assurer que les ministères ont finalisé et exécuté leurs plans de gestion des événements de sécurité et qu'ils le mettent régulièrement à l'essai.	le 31 janvier 2025
Recommandation 3	Le SCT doit présenter au Comité un rapport d'étape sur : A) la façon dont il documente les rôles et responsabilités nécessaires pour concevoir, mettre en œuvre, valider, surveiller, coordonner et appliquer les contrôles de sécurité nécessaires pour protéger les renseignements sensibles et personnels stockés dans le nuage et dont il communique ces rôles et responsabilités de façon proactive aux ministères; B) les mesures qu'il a prises pour s'assurer de revoir et actualiser ces rôles et responsabilités au moins tous les 12 mois.	le 31 janvier 2025

Recommandation	Mesure recommandée	Échéancier
Recommandation 4	Le SCT doit présenter au Comité un rapport d'étape sur : A) son modèle d'établissement des coûts afin d'aider les ministères à prendre des décisions éclairées au sujet de la transition vers l'infonuagique et à déterminer si des ressources et du financement additionnels sont nécessaires; B) la façon dont il aide les ministères à évaluer le financement de fonctionnement à long terme dont ils ont besoin et appuie leur accès au financement pour qu'ils puissent s'acquitter de leurs responsabilités en constante évolution à l'égard des activités liées à l'infonuagique, notamment la protection des renseignements de nature délicate.	le 31 janvier 2025
Recommandation 5	Services publics et Approvisionnement Canada doit présenter au Comité un rapport sur les critères environnementaux à utiliser dans le cadre de l'approvisionnement en services infonuagiques afin de favoriser la durabilité des pratiques d'approvisionnement et de contribuer à l'atteinte de l'objectif de carboneutralité du Canada.	le 31 janvier 2025
Recommandation 6	Services partagés Canada doit présenter au Comité un rapport indiquant les progrès réalisés relativement à l'élaboration de critères environnementaux à utiliser dans le cadre de l'approvisionnement en services infonuagiques afin de favoriser la durabilité des pratiques d'approvisionnement et de contribuer à l'atteinte de l'objectif de carboneutralité du Canada.	le 31 janvier 2025

CONTEXTE

En informatique, le terme « nuage » désigne les serveurs informatiques ainsi que les applications logicielles et les bases de données qui fonctionnent sur ces serveurs, lesquels se trouvent dans des centres de données situés partout dans le monde. Les utilisateurs ne sont pas tenus de posséder et d'exploiter leurs propres serveurs physiques ou applications

logicielles ou d'en assurer la maintenance. Ils peuvent se servir des serveurs infonuagiques sur demande et ne payent que ce dont ils ont besoin[2].

Le Secrétariat du Conseil du Trésor du Canada (SCT) a publié la Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada en 2016 et l'a mise à jour en 2018. La Stratégie enjoint aux organisations fédérales d'envisager l'infonuagique comme option privilégiée pour la prestation des services de technologies de l'information. Selon le SCT, l'infonuagique offre les avantages suivants :

- des économies d'échelle;
- des services sur demande;
- de la souplesse;
- des services régis par des contrats;
- la sécurité[3].

Il est également indiqué dans la Stratégie que les fournisseurs de services infonuagiques et les ministères fédéraux qui utilisent leurs services se partagent la responsabilité de la sécurité. Toutefois, les ministères fédéraux demeurent responsables de la confidentialité, de l'intégrité et de la disponibilité des services informatiques ainsi que de l'information connexe hébergée par un fournisseur de services infonuagiques. De plus, le Plan stratégique des opérations numériques de 2018 à 2022 du SCT « reconnaît que pour réduire le plus possible les risques pour la sécurité, les ministères qui ont recours aux services infonuagiques doivent mettre sur pied une main-d'œuvre avisée en matière d'infonuagique[4] ».

Entre avril 2018 et mars 2022, Services partagés Canada (SPC) a octroyé des contrats à 14 fournisseurs de services infonuagiques, avec lesquels Services publics et Approvisionnement Canada (SPAC) a conclu des arrangements en matière d'approvisionnement. Au cours de cette période, plusieurs ministères ont commencé à faire passer leurs applications logicielles et leurs bases de données au nuage et certains ont lancé des applications infonuagiques. D'avril 2018 à mars 2021, les organisations

2 BVG, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.1.

3 *Ibid*., paragr. 7.2.

4 *Ibid*., paragr. 7.3.

fédérales ont signalé avoir dépensé un total de 210 millions de dollars en services infonuagiques[5].

Les cyberattaques peuvent entraîner l'interruption des services ainsi que la défaillance ou même la destruction d'infrastructures essentielles (comme les services bancaires et le réseau de distribution d'énergie électrique). En outre, elles peuvent compromettre des données personnelles, porter atteinte à la réputation, occasionner des coûts financiers, perturber de manière importante les activités d'entreprises canadiennes et les services gouvernementaux et entraîner des difficultés pour la population. Les événements géopolitiques, comme les guerres ou l'agitation politique, et les conflits commerciaux internationaux peuvent accroître de façon considérable les risques liés à la cybersécurité[6].

Puisque les organisations fédérales ont commencé à faire passer des applications logicielles et des bases de données au nuage, de plus en plus de renseignements personnels de Canadiennes et de Canadiens s'y trouvent. Pour protéger les renseignements personnels dans le nuage, « le gouvernement a mis en œuvre un modèle de responsabilité partagée qui repose sur la collaboration d'un certain nombre de parties[7] ». Le tableau 2 présente des renseignements sur les rôles et les responsabilités du SCT, de SPC, de SPAC, du Centre de la sécurité des télécommunications Canada (CSTC) et de chacun des ministères.

Tableau 2 — Rôles et responsabilités en matière de cybersécurité des renseignements personnels dans le nuage

SCT	Fournit des politiques et des orientations sur les services infonuagiques, notamment dans la Stratégie d'adoption de l'informatique en nuage du gouvernement; assure la coordination des interventions à la suite d'incidents de cybersécurité, comme il est décrit dans le Plan de gestion des événements de cybersécurité du gouvernement du Canada.
SPC	Fournit aux autres ministères fédéraux l'accès aux fournisseurs de services infonuagiques approuvés dans le cadre de marchés qu'il gère. Il assure aussi la gestion et la surveillance de la plupart des serveurs et des centres de données du gouvernement du Canada et un accès sécurisé au nuage.

5 *Ibid*., paragr. 7.4.

6 *Ibid*., paragr. 7.5.

7 *Ibid*., paragr. 7.6.

SPAC	Fournit des services communs au gouvernement; établit des arrangements en matière d'approvisionnement avec des fournisseurs de services infonuagiques préqualifiés dans le but de permettre à d'autres ministères d'obtenir les services logiciels qu'ils offrent. Dans certains cas, les ministères peuvent se procurer ces services directement auprès de ces fournisseurs ou d'autres fournisseurs. Pour les contrats excédant certains seuils financiers, SPAC établit le contrat et en assure la gestion au nom d'un ministère. Il évalue aussi les contrôles de sécurité matérielle des fournisseurs de services infonuagiques et de leur personnel.
CSTC	Le Centre canadien pour la cybersécurité, qui fait partie du CSTC, est la source de conseils, d'avis, de services et de soutien en matière de cybersécurité pour la population canadienne. Il doit notamment effectuer des évaluations de la sécurité des fournisseurs de services infonuagiques retenus par SPC et SPAC dans le cadre de certains de leurs processus d'approvisionnement en services infonuagiques. Il surveille aussi les réseaux ministériels et la sécurité dans le nuage et offre de la formation, des conseils et des orientations sur la sécurité infonuagique. Le CSTC aide aussi les organisations fédérales à mettre en œuvre des infrastructures numériques sécurisées.
Chacun des ministères	Les ministères (organisations fédérales) mettent en œuvre leurs propres contrôles de sécurité et assurent la surveillance des renseignements et des activités des utilisatrices et utilisateurs sur leurs propres applications logicielles. Ils demeurent en définitive responsables et comptables des risques relatifs à la sécurité découlant de leur utilisation des services infonuagiques. Les ministères sont tenus de signaler les atteintes à la protection de la vie privée au SCT et au Commissariat à la vie privée du Canada.

Source : Bureau du vérificateur général du Canada, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.7 à 7.11.

Le 15 novembre 2022, le Bureau du vérificateur général du Canada (BVG) a publié un audit qui visait à déterminer si le SCT, SPC, SPAC, le CSTC et les ministères fédéraux sélectionnés avaient mis en place « une gouvernance, des lignes directrices et des outils adéquats et efficaces pour prévenir les événements de cybersécurité qui pourraient compromettre les renseignements personnels de la population canadienne stockés dans le nuage, détecter ces événements et agir en conséquence. Pour des raisons de sécurité nationale, le nom des ministères fédéraux sélectionnés aux fins de l'audit n'est pas mentionné dans le […] rapport [d'audit][8]. »

Le 30 mars 2023, le Comité permanent des comptes publics de la Chambre des communes (le Comité) a tenu une audience sur cet audit, à laquelle ont participé les personnes suivantes :

8 *Ibid*., paragr. 7.12.

Bureau du vérificateur général du Canada — Andrew Hayes, sous-vérificateur général; Jean Goulet et Gabriel Lombardi, directeurs principaux

Centre de la sécurité des télécommunications — Rajiv Gupta, dirigeant associé, Centre canadien pour la cybersécurité

SPAC — Paul Thompson, sous-ministre et Catherine Poulin, sous-ministre adjointe, Direction générale de la surveillance

SPC — Sony Perron, président, et Costas Theophilos, directeur général, Direction de la gestion des produits et des services infonuagiques

SCT, Catherine Luelo, sous-ministre et dirigeante principale de l'information du Canada[9]

Le tableau 3 présente les définitions de termes clés employés dans le présent rapport.

Tableau 3 — Définitions

Arrangement en matière d'approvisionnement	Méthode utilisée par SPAC pour acquérir des biens et des services en qualifiant au préalable les fournisseurs et en établissant les clauses et les conditions essentielles qui s'appliqueront à tout contrat subséquent.
Contrôles de sécurité	Tout type de contre-mesure de sauvegarde ou de protection qui vise à éviter, à détecter, à neutraliser ou à limiter les risques liés à la sécurité des biens matériels, de l'information, des systèmes informatiques ou d'autres actifs. Ces contre-mesures sont nommées « contrôles » dans le présent rapport.
Valider	Dans le contexte de la validation des mesures de sécurité, ce terme s'entend de l'examen des éléments probants confirmant que les ministères ont mis en œuvre les mesures de sécurité conformément à la Directive sur les services et le numérique.

Source : Bureau du vérificateur général du Canada, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, Définitions.

9 Comité permanent des comptes publics de la Chambre des communes, *Témoignages*, 1re session, 44e législature, 30 mars 2023, réunion no 56.

CONSTATS ET RECOMMANDATIONS

Mesures de sécurité non validées et non surveillées de manière uniforme

Le BVG a constaté que « [l'information] stockée numériquement, soit sur place dans des centres de données ou dans le nuage, est exposée à des risques de compromission[10]. »

Les « mesures de sécurité » d'informatique en nuage sont un ensemble de contrôles de base que les ministères doivent mettre en œuvre pour prévenir et détecter les cyberattaques dans leurs environnements infonuagiques. Dans le cadre des contrats qu'il avait établis entre des ministères et des fournisseurs de services infonuagiques, SPC avait vérifié si les ministères avaient mis en œuvre les mesures de sécurité dans les trente premiers jours. Toutefois, il avait seulement réalisé des suivis en continu limités par la suite. Pour les services infonuagiques établis par SPAC, personne n'avait vérifié si les ministères avaient mis des mesures de sécurité en place au départ, et personne n'effectuait de suivi de la conformité en continu. Ce manque d'uniformité dans l'application des contrôles dans l'ensemble du gouvernement fait augmenter les risques de compromission des renseignements personnels de la population canadienne qui sont stockés dans le nuage[11].

SPC n'avait pas évalué efficacement certains des contrôles et avait parfois attribué une note de passage à des ministères qui n'avaient pas correctement mis en œuvre les mesures de sécurité. Et même si SPC avait validé la mise en œuvre au sein de tous les ministères des 12 mesures de sécurité dans les 30 jours suivant l'établissement de leurs contrats avec des fournisseurs de services infonuagiques, il n'a assuré le suivi de la conformité continue que pour deux mesures de sécurité sur 12. En outre, il n'a vérifié que les aspects administratifs de ces deux mesures (notamment ceux liés à la facturation et aux rapports) et pas si elles étaient toujours en place et si elles fonctionnaient comme prévu. SPC laissait donc la surveillance en continu des mesures du point de vue de la sécurité à la discrétion de chaque ministère[12].

En conséquence, le BVG a recommandé que SPC, SPAC et le SCT fassent ce qui suit :

- étendre les exigences relatives aux mesures de sécurité aux contrats de services infonuagiques qui découlent d'arrangements en matière

10 BVG, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.16.

11 *Ibid.*, paragr. 7.26 et 7.28.

12 *Ibid*., paragr. 7.30.

d'approvisionnement établis par Services publics et Approvisionnement Canada;

- préciser qui est responsable de la validation initiale et de la surveillance en continu des mesures de sécurité d'informatique en nuage ainsi que les processus à suivre[13].

Dans son Plan d'action détaillé, le SCT a indiqué qu'il clarifiera le processus ainsi que les rôles et responsabilités relativement à la validation et à la surveillance des mesures de protection, puis il veillera à ce que l'exigence s'applique aux solutions établies par SPAC[14]. Le Ministère a également indiqué les résultats escomptés suivants, qui devaient être atteints pour le 1er avril 2023 :

> La matrice des responsabilités liées à l'informatique en nuage qui indique officiellement les personnes responsables de valider et de surveiller de façon continue les mesures de protection, de les surveiller et d'en assurer la conformité a été publiée.
>
> La procédure opérationnelle normalisée pour la validation des mesures de protection du nuage est clarifiée et elle s'applique aux marchés conclus par SPAC avec des fournisseurs de services d'informatique en nuage.
>
> Les Mesures de protection du nuage du gouvernement du Canada et la Directive sur les services et le numérique ont été mises à jour pour refléter les mesures de protection qui s'appliquent aux services d'informatique en nuage, y compris celles qui sont fournies par SPAC

En outre, le SCT :

- établira une carte de pointage pour rendre compte du niveau de conformité des ministères aux mesures de protection du nuage du gouvernement du Canada;

- collaborera avec SPC dans ses efforts pour mettre en œuvre des outils servant à automatiser la surveillance des mesures de protection pour les

13 *Ibid*., paragr. 7.31.

14 Secrétariat du Conseil du Trésor du Canada (SCT), Plan d'action détaillé, p. 1.

fournisseurs de services d'informatique en nuage retenus par le gouvernement du Canada;

- continuera à fournir des conseils et une orientation aux ministères sur la façon de faire en sorte qu'ils effectuent les activités d'évaluation et d'autorisation de la sécurité pour les applications d'informatique en nuage au moyen d'outils comme le guide de sécurité pour les solutions du système informatique qui décrit un ensemble de tâches de sécurité à prendre en considération au moment de concevoir et de mettre en œuvre des solutions pour les systèmes de renseignements du gouvernement du Canada dans les environnements d'informatique en nuage[15].

Lors de l'audience, Sony Perron, président, SPC, a répondu ceci à une question sur les essais pour l'automatisation de la vérification des mesures de sécurité :

> Nous devrons trouver un moyen de vous transmettre cette information. En fait, il existe actuellement 12 mesures de sécurité. Sur les conseils judicieux de la vérificatrice générale, mon équipe a entrepris de vérifier que ces mesures assurent une sécurité constante, pas uniquement au début du processus, mais tout au long de celui-ci. Il s'agira davantage d'une surveillance que d'un exercice ponctuel.
>
> À l'heure actuelle, nous surveillons la conformité de chaque ministère. C'est simplement que le processus n'est pas automatisé. Ce sont les gens de l'équipe de Costa qui vérifient manuellement, sur une base régulière, autour de 200 instances de service infonuagique pour s'assurer que les ministères utilisent ce dernier conformément aux normes établies.
>
> […]
>
> Voilà pourquoi l'automatisation est un aspect important. Une intervention humaine pour régler cinq cas est une chose; toutefois, lorsque nous en sommes à 200, 400, voire 500 cas, il devient presque impossible d'avoir les yeux sur tout, tout le temps. L'automatisation nous permet de recevoir une alerte si une mesure de sécurité est en train d'être modifiée par un utilisateur du service. Au sein de chaque ministère, seul un petit nombre de personnes possède l'autorisation de modifier les mesures de sécurité. Pour diverses raisons, une personne peut décider, que ce soit de manière volontaire ou par erreur, de modifier l'un des éléments du dispositif de sécurité. Nous devons toujours

15 *Ibid*.

être en mesure d'être alertés de ce genre d'incidents, afin de pouvoir y remédier en temps utile[16].

En conséquence, le Comité recommande :

Recommandation 1

Que, d'ici le 31 janvier 2025, le Secrétariat du Conseil du Trésor du Canada présente au Comité permanent des comptes publics de la Chambre des communes un rapport d'étape sur : A) la façon dont ont été mises en œuvre les exigences relatives aux mesures de sécurité dans les contrats de services infonuagiques qui découlent d'arrangements en matière d'approvisionnement établis par Services publics et Approvisionnement Canada; B) la façon dont il a précisé qui est responsable de la validation initiale et de la surveillance en continu des mesures de sécurité d'informatique en nuage, ainsi que les processus à suivre.

Lacunes en ce qui concerne les plans de gestion des événements de cybersécurité

Lorsqu'un événement de cybersécurité se produit, les principales organisations chargées de la sécurité et les ministères doivent être en mesure d'intervenir rapidement et de manière coordonnée. Cela requiert l'établissement de plans de gestion des événements de cybersécurité qui ont été mis à l'essai et validés (c.-à-d. dont l'efficacité a été prouvée dans le cadre d'exercices de simulation). « La capacité du gouvernement à détecter les cyberattaques à l'échelle du gouvernement et à intervenir en conséquence dépend de la capacité de chaque ministère à le faire à l'échelle ministérielle[17].»

Le BVG a constaté que, dans le cadre des contrats ou des accords de fourniture de services en nuage conclus avec 14 fournisseurs de services en nuage « aucun des ministères n'avait défini de manière suffisamment détaillée les obligations des ministères ou des fournisseurs de services infonuagiques en ce qui concerne la gestion des incidents de sécurité et des atteintes à la vie privée, notamment la rapidité avec laquelle les parties doivent intervenir et la personne chargée de communiquer les incidents et les atteintes (et à qui il faut les communiquer)[18]. »

16 Comité permanent des comptes publics de la Chambre des communes, *Témoignages*, 1re session, 44e législature, 30 mars 2023, réunion no 56, 1600 et 1610.

17 BVG, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.35.

18 *Ibid.*, paragr. 7.33

Le Plan de gestion des événements de cybersécurité du gouvernement du Canada (avril 2020) désigne les ministères et les organismes centraux chargés de la coordination des interventions dans le cadre des événements ayant des répercussions sur l'ensemble du gouvernement. Selon le Plan, les organisations fédérales doivent veiller à l'amélioration continue de leur capacité à réagir aux événements de cybersécurité. « Ils doivent notamment tester les plans et les procédures, mettre en œuvre les leçons apprises, tenir à jour des listes de personnes à qui ont été assignées des responsabilités établies dans le plan et former le personnel, y compris le personnel chargé de la cybersécurité[19]. »

Le BVG a constaté que le SCT et le CSTC avaient mené des exercices sur les leçons apprises et élaboré un rapport, des recommandations et un plan d'action pour améliorer les interventions futures. Toutefois, le SCT n'a pas respecté les exigences établies dans le plan concernant la mise à l'essai des plans et des procédures et la tenue à jour du plan. Plus précisément, dans son examen des plans ministériels de gestion des événements de cybersécurité des trois ministères sélectionnés pour l'audit, le BVG a constaté ce qui suit :

- Chacun des trois ministères avait effectué des exercices de simulation et des tests de la sécurité de leurs applications annuellement.

- Chacun des ministères avait préparé des plans, mais deux ministères sur trois ont indiqué au BVG qu'ils n'avaient ni les fonds ni la capacité nécessaire pour assurer leur pleine mise en œuvre.

- Sur les trois ministères sélectionnés, deux n'avaient pas terminé la définition des rôles et des responsabilités internes pour la gestion des incidents.

- Même si le SCT a commencé à recueillir de l'information auprès des ministères en septembre 2021, au moment de notre audit, il ne savait pas si tous les ministères avaient mis en œuvre des plans de gestion des événements de cybersécurité[20].

En conséquence, le BVG a recommandé que le SCT fasse ce qui suit :

- au moins une fois par année, vérifier que le Plan de gestion des événements de cybersécurité du gouvernement du Canada s'applique à

19 *Ibid*., paragr. 7.36.

20 *Ibid.*, paragr. 7.37 à 7.39.

l'environnement infonuagique en évolution et aux responsabilités partagées, le revoir et le tester, et le mettre à jour au besoin;

- assurer un suivi chaque année pour s'assurer que les ministères finalisent, exécutent et mettent régulièrement à l'essai leurs plans de gestion des événements de sécurité[21].

Dans son Plan d'action détaillé, le SCT a déclaré qu'il « assurera la pertinence du PGEC GC [Plan de gestion des événements de cybersécurité du gouvernement du Canada] et veillera à ce qu'il soit examiné et testé chaque année, et mis à jour au besoin. Le SCT veillera à ce que les ministères utilisent le PGEC GC[22]. » Le Ministère a également indiqué les jalons suivants :

> Automne 2022 — Mise à jour et publication du PGEC GC.
>
> Mars 2023 — Exploration d'options d'outils pour permettre aux ministères de faciliter les exercices de simulation d'informatique en nuage.
>
> Avril 2023 — Inclusion d'une exigence voulant que les ministères soumettent leur PGEC conjointement avec leur Plan sur les services et le numérique[23].

Lors de l'audience, Catherine Luelo, sous-ministre et dirigeante principale de l'information du Canada, Secrétariat du Conseil du Trésor, a fait le point sur le PGEC :

> En novembre 2022, nous avons mis à jour le Plan de gestion des événements de cybersécurité du gouvernement du Canada. Il s'agit du plan que nous avons mis en place pour réagir aux incidents de cybersécurité qui visent l'organisation gouvernementale. Ce plan, dont la première version a été publiée en 2015, est continuellement mis à l'épreuve, examiné et ajusté, comme le veut la pratique courante pour tout type de plan de cybersécurité. En fait, il y a environ quatre semaines, nous avons effectué une simulation à l'échelle du gouvernement. Cet examen comprenait une composante infonuagique, ce qui nous a permis de commencer à mettre à l'épreuve nos mesures d'intervention en cas de cyberincidents dans le nuage.
>
> De plus, nous avons publié en janvier une nouvelle version de la stratégie d'informatique en nuage qui était en préparation depuis plusieurs mois. Nous avons remplacé l'expression l'« informatique en nuage d'abord » par l'« informatique en

21 *Ibid.*, paragr. 7.40.

22 SCT, Plan d'action détaillé, p. 1 et 2.

23 *Ibid.*

> nuage intelligente » afin de refléter concrètement que nous n'allons pas adopter systématiquement l'infonuagique, mais que nous allons plutôt prendre des décisions équilibrées en fonction de plusieurs facteurs, dont le facteur financier… L'approche de l'informatique en nuage d'abord était la bonne pour donner son élan au gouvernement. Il fallait commencer à orienter les gens vers la nouvelle technologie, et cette approche a permis de mettre le navire sur la bonne voie, pour ainsi dire[24].

En conséquence, le Comité recommande :

Recommandation 2

Que, d'ici le 31 janvier 2025, le Secrétariat du Conseil du Trésor du Canada présente au Comité permanent des comptes publics de la Chambre des communes un rapport d'étape sur la façon dont il s'est assuré que le Plan de gestion des événements de cybersécurité du gouvernement du Canada s'applique à l'environnement infonuagique en évolution et aux responsabilités partagées. En outre, le rapport d'étape doit indiquer comment le plan sera examiné et testé chaque année, et comment il sera mis à jour; il doit aussi inclure la procédure pour le suivi annuel auprès des ministères afin de s'assurer que les ministères ont finalisé et exécuté leurs plans de gestion des événements de sécurité et qu'ils le mettent régulièrement à l'essai.

Confusion des ministères par rapport à leurs rôles en matière de cybersécurité

Le BVG a constaté que « les organisations ne savaient pas exactement qui devait faire quoi dans certains domaines, par exemple, qui devrait évaluer les contrôles de sécurité des technologies de l'information pour ce qui est des exigences relatives à l'emplacement des données.[25] » Plus spécifiquement, la matrice des responsabilités et des rôles liés à l'infonuagique du gouvernement du Canada du SCT ne comprenait pas ou ne modifiait pas les responsabilités et les rôles qui ont évolué ou qui ont été ajoutés depuis mars 2018 (date de la dernière mise à jour de la matrice)[26].

Les rôles et responsabilités en matière de sécurité infonuagique sont énoncés dans de multiples documents. Par conséquent, le BVG a constaté que les ministères étaient confus quant à certains de leurs rôles et responsabilités. Par exemple, la Directive sur les

---

24 Comité permanent des comptes publics de la Chambre des communes, *Témoignages*, 1re session, 44e législature, 30 mars 2023, réunion no 56, 1550.

25 BVG, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.41.

26 *Ibid.*, paragr. 7.45.

services et le numérique indique que les ministères doivent veiller à ce que les données stockées dans le nuage, y compris les données de nature délicate et les renseignements personnels, soient conservées au Canada. Toutefois, après avoir passé en revue les contrats et arrangements en matière d'approvisionnement établis par SPC et SPAC, le BVG a constaté que les parties concernées ne comprenaient pas toutes cette exigence[27].

Selon le BVG, faute de « bien comprendre qui veille à ce que les données stockées dans le nuage restent au Canada, les organisations risquent de ne pas savoir si les renseignements personnels sont en fait stockés dans un autre pays et, le cas échéant, s'ils sont donc assujettis à des lois différentes (et possiblement inférieures) en matière de protection de la vie privée et à des protocoles différents en matière de sécurité[28] ».

En conséquence, le BVG a recommandé ce qui suit :

> En consultation avec le Centre de la sécurité des télécommunications du Canada, Services partagés Canada, Services publics et Approvisionnement Canada et les ministères, le Secrétariat du Conseil du Trésor du Canada devrait documenter les rôles et responsabilités nécessaires pour concevoir, mettre en œuvre, valider, surveiller, coordonner et appliquer les contrôles de sécurité nécessaires pour protéger les renseignements sensibles et personnels stockés dans le nuage et communiquer ces rôles et responsabilités de façon proactive à tout ministère qui a recours aux services infonuagiques ou qui envisage d'y avoir recours. Le Secrétariat devrait revoir et actualiser ces rôles et responsabilités au moins tous les 12 mois[29].

Dans son Plan d'action détaillé, le SCT a indiqué qu'il « veillera à ce que les rôles et les responsabilités nécessaires pour les mesures de sécurité soient clairement documentés et communiqués de façon proactive aux ministères[30] ». Le Ministère s'est également engagé à atteindre les jalons suivants :

> Octobre 2022 — Publication de la matrice des responsabilités liées à l'informatique en nuage.
>
> Mars 2023 — Examen de la matrice des responsabilités.
>
> Septembre 2023 — Augmentation des communications proactives.

27 *Ibid*., paragr. 7.46.

28 Ibid.

29 *Ibid*., paragr. 7.47.

30 SCT, Plan d'action détaillé, p. 2.

Mars 2023 — Octroi de mises à jour à la collectivité concernant les cycles d'examen[31].

Lors de l'audience, Catherine Luelo a déclaré que, depuis l'audit, le gouvernement a mis à jour le document sur les rôles et les responsabilités liés à l'infonuagique, y compris une matrice connexe, et l'a publié à l'interne pour que les équipes concernées puissent y avoir accès[32].

En conséquence, le Comité recommande :

Recommandation 3

Que, d'ici le 31 janvier 2025, le Secrétariat du Conseil du Trésor du Canada présente au Comité permanent des comptes publics de la Chambre des communes un rapport d'étape sur : A) la façon dont il documente les rôles et responsabilités nécessaires pour concevoir, mettre en œuvre, valider, surveiller, coordonner et appliquer les contrôles de sécurité nécessaires pour protéger les renseignements sensibles et personnels stockés dans le nuage et dont il communique ces rôles et responsabilités de façon proactive aux ministères; B) les mesures qu'il a prises pour s'assurer de revoir et actualiser ces rôles et responsabilités au moins tous les 12 mois.

Absence de modèle d'établissement des coûts ou de méthode de financement à long terme

Lorsque le SCT a publié sa Stratégie d'adoption de l'infonuagique en 2018, il n'avait pas élaboré ni diffusé de méthode de financement à long terme ou de modèle d'établissement des coûts pour accompagner la Stratégie. Le SCT n'a pas non plus été en mesure de fournir de tels documents au BVG aux fins de son audit. Par conséquent, le BVG n'a pas pu « déterminer comment un tel modèle ou une telle méthode permettrait de remédier aux difficultés rencontrées par les ministères au moment de comprendre les coûts du passage de l'information vers le nuage et de la sécurisation de celle-ci ainsi que le financement requis pour assurer la protection à long terme de cette information[33] ».

31 *Ibid*.

32 Comité permanent des comptes publics de la Chambre des communes, *Témoignages*, 1re session, 44e législature, 30 mars 2023, réunion no 56, 1550.

33 BVG, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.51.

Lorsque les organisations fédérales doivent décider si leurs applications ou services seront hébergés dans un centre de données de SPC ou dans le nuage, le coût est un facteur important. Il en est ainsi parce que l'adoption de l'infonuagique transfère aux organisations fédérales certains coûts du stockage de données qui étaient auparavant pris en charge par SPC; elles doivent aussi endosser la responsabilité « de financer l'exploitation de l'infonuagique et les nouvelles responsabilités en matière de cybersécurité qui les accompagnent », notamment « la création d'équipes dotées de compétences en infonuagique et en cybersécurité, l'achat d'outils de cybersécurité et le maintien des activités et de la sécurité en continu[34] ».

Même si du financement à court terme a été mis à la disposition des ministères pour les aider à déplacer leurs applications vers le nuage, des responsables ont indiqué qu'ils ne savaient toujours pas comment les ministères financeront l'exploitation continue de l'infonuagique. Parallèlement, « les dépenses ministérielles en services infonuagiques à l'échelle du gouvernement ont augmenté considérablement d'une année à l'autre, passant de 35 millions de dollars en 2018 à près de 120 millions de dollars en 2021[35] ». Par exemple, en l'absence de financement à long terme pour l'exploitation en continu, les trois ministères sélectionnés aux fins de l'audit « se servaient de diverses mesures de financement à court terme pour appuyer l'exploitation de l'infonuagique et la cybersécurité. Ils procédaient notamment à la réaffectation de fonds destinés à d'autres fins[36]. »

Même si les grands ministères peuvent avoir la capacité d'absorber certains des coûts de l'adoption de l'infonuagique et des mesures de sécurité, cette approche n'est vraisemblablement pas durable à long terme, et les petits ministères pourraient être incapables d'assumer même une partie de ces coûts. En outre, « le financement de la cybersécurité à même les ressources prévues pour les autres activités de technologie de l'information risquerait de compromettre celles-ci[37] ».

En conséquence, le BVG a recommandé que le SCT, en consultation avec SPC et d'autres ministères, fasse ce qui suit :

- élaborer et fournir un modèle d'établissement des coûts afin d'aider les ministères à prendre des décisions éclairées au sujet de la transition vers

34 *Ibid*., paragr. 7.52.

35 *Ibid*., paragr. 7.53.

36 *Ibid*., paragr. 7.56.

37 *Ibid*., paragr. 7.57.

l'infonuagique et à déterminer si des ressources et du financement additionnels sont nécessaires;

- aider les ministères à évaluer le financement de fonctionnement à long terme dont ils ont besoin et appuyer leur accès au financement pour qu'ils puissent s'acquitter de leurs responsabilités en constante évolution à l'égard des activités liées à l'infonuagique, notamment la protection des renseignements de nature délicate dans le nuage[38].

Dans son Plan d'action détaillé, le SCT a déclaré qu'il « élaborera et fournira un modèle d'établissement des coûts et des outils pour aider les ministères à prendre des décisions éclairées sur le passage à l'informatique en nuage et à déterminer les ressources et le financement requis[39] ». Il a également indiqué les jalons suivants :

> Automne 2022 — Présentation de recommandations à la DPI GC sur la voie à suivre.
>
> Juin 2023 — Octroi d'un modèle d'établissement des coûts et de lignes directrices; aide offerte aux ministères et à SPC pour établir les prévisions[40].

Lors de l'audience, Sony Perron a fourni la réponse suivante à une question sur le modèle d'établissement des coûts proposé :

> C'est un document qui est le fruit de la collaboration entre plusieurs ministères, sous la direction du Secrétariat du Conseil du Trésor. Il n'y a rien à cacher. Nous allons le communiquer aux ministères parce qu'il s'agit d'un outil, et je suppose que je pourrai le transmettre au Comité lorsqu'il sera prêt à être distribué[41].

Nonobstant ce qui précède, le Comité recommande :

Recommandation 4

Que, d'ici le 31 janvier 2025, le Secrétariat du Conseil du Trésor du Canada présente au Comité permanent des comptes publics de la Chambre des communes un rapport d'étape sur : A) son modèle d'établissement des coûts afin d'aider les ministères à

38 *Ibid*., paragr. 7.58.

39 SCT, Plan d'action détaillé, p. 3.

40 *Ibid*., p. 3.

41 Comité permanent des comptes publics de la Chambre des communes, *Témoignages*, 1re session, 44e législature, 30 mars 2023, réunion nº 56, 1600.

prendre des décisions éclairées au sujet de la transition vers l'infonuagique et à déterminer si des ressources et du financement additionnels sont nécessaires; B) la façon dont il aide les ministères à évaluer le financement de fonctionnement à long terme dont ils ont besoin et appuie leur accès au financement pour qu'ils puissent s'acquitter de leurs responsabilités en constante évolution à l'égard des activités liées à l'infonuagique, notamment la protection des renseignements de nature délicate.

Absence de critères environnementaux dans le processus d'approvisionnement en services infonuagiques

Le SCT et SPAC avaient élaboré des lignes directrices et de la formation pour aider les agentes et agents de négociation des contrats à intégrer les considérations environnementales dans le processus d'approvisionnement en services. De plus, SPAC et SPC avaient formé leurs agentes et agents d'approvisionnement aux pratiques d'approvisionnement écologiques[42]. Toutefois, ils « n'avaient pas exigé que les fournisseurs de services infonuagiques fassent état de leur rendement environnemental ou qu'ils expliquent comment leurs services contribueraient à réduire les émissions de gaz à effet de serre du Canada[43] ».

Même si les ministères « avaient demandé aux fournisseurs de services infonuagiques de fournir des renseignements sur leurs engagements en matière d'environnement et l'état de leurs activités, ils n'avaient pas exigé de les obtenir ou n'en avaient pas confirmé l'exactitude lorsqu'ils les avaient obtenus[44] ».

Le BVG a examiné 14 contrats et arrangements en matière d'approvisionnement en services infonuagiques et a constaté qu'aucun ne comportait de clauses liées à l'environnement. Par ailleurs, le Guide des clauses et conditions uniformisées d'achat de SPAC ne contenait aucune clause environnementale relative aux services infonuagiques[45].

Bien que les ministères puissent inclure leurs propres exigences environnementales, les trois ministères sélectionnés aux fins de l'audit ont indiqué qu'ils ne rédigeaient pas leurs propres clauses contractuelles, se fiant plutôt au Guide des clauses et conditions

42 BVG, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.68.

43 *Ibid*., paragr. 7.69.

44 *Ibid*.

45 *Ibid*., paragr. 7.70.

uniformisées d'achat (pour que les clauses soient appliquées de manière uniforme dans l'ensemble des ministères)[46].

En conséquence, le BVG a recommandé que SPAC et SPC incluent « des critères environnementaux dans le cadre de l'approvisionnement en services infonuagiques afin de favoriser la durabilité des pratiques d'approvisionnement et de contribuer à l'atteinte de l'objectif de carboneutralité du Canada[47] ».

Dans son Plan d'action détaillé, SPC a indiqué que des critères environnementaux « seront inclus dans les stratégies de SPAC et de SPC et intégrés dans les modèles de contrat infonuagique normalisés en cours d'élaboration pour l'approvisionnement en services infonuagiques à l'échelle du gouvernement du Canada[48] ». Il a également présenté les jalons suivants :

> Élaborer des critères environnementaux cotés à inclure dans les appels d'offres concurrentiels en infonuagique. (31 août 2022)
>
> Commencer à inclure des critères environnementaux dans les processus d'appels d'offres concurrentiels en vertu de l'accord-cadre sur l'infonuagique de SPC. (29 septembre 2022)
>
> Rédiger une ébauche de modèle normalisé de contrat en infonuagique qui comprend les conditions relatives à la durabilité pour les fournisseurs de services infonuagiques. (29 septembre 2022)
>
> Consulter l'industrie au sujet du modèle normalisé des modalités en matière d'infonuagique, y compris les conditions relatives à la durabilité. Mettre les modèles normalisés à jour pour donner suite à la consultation. (31 mars 2023)
>
> Élaborer les clauses contractuelles résultantes liées aux objectifs de réduction des GES, après consultation de l'industrie. Incorporer ces clauses dans les appels d'offres de SPAC et de SPC, ainsi qu'au modèle normalisé de contrat en infonuagique. (31 mars 2023)[49]

46 *Ibid*., paragr. 7.71.

47 *Ibid*., paragr. 7.72.

48 Services partagés Canada, Plan d'action détaillé, p. 1.

49 *Ibid*., p. 1 et 2.

Enfin, les jalons suivants ont été établis dans le Plan d'action de SPAC :

> **Principal jalon provisoire A (31 mars 2023) :**
>
> Actualisation de l'arrangement en matière d'approvisionnement (AMA) pour les logiciels-services de SPAC en y apportant des modifications tenant compte des priorités du gouvernement du Canada pour l'élimination complète des GES, comme suit :
>
> - Mise à jour des informations environnementales recueillies.
> - Possibilité pour les clients d'inclure des critères environnementaux dans les appels d'offres lancés dans le cadre de l'AMA.
> - Intégration de clauses contractuelles résultantes liées aux objectifs de réduction des GES.
>
> **Principal jalon provisoire B (terminé) :**
>
> En collaboration avec SPC, élaboration et publication, pour les agents d'approvisionnement, d'un modèle standard de contrats de services infonuagiques comprenant des conditions de durabilité applicables aux fournisseurs de services infonuagiques[50].

Lors de l'audience, Sony Perron a répondu ceci lorsqu'on lui a demandé si l'on avait donné suite à cette recommandation :

> Services partagés Canada ainsi que Services publics et Approvisionnement Canada se sont engagés à travailler avec l'industrie pour déterminer quelle est la meilleure façon d'exiger, dans les soumissions qui seront présentées pour des services infonuagiques, l'information nécessaire pour évaluer l'impact environnemental des propositions de services. Les consultations sont terminées et, dans quelques semaines, en avril, les critères seront intégrés dans les véhicules contractuels que nous avons pour les appels d'offres compétitifs[51].

Costas Theophilos, directeur général, Gestion des produits et des services infonuagiques, Services partagés Canada, a ajouté ceci au sujet des critères à prendre en compte :

---

50 Services publics et Approvisionnement Canada, Plan d'action de SPAC, p. 1.

51 Comité permanent des comptes publics de la Chambre des communes, *Témoignages*, 1re session, 44e législature, 30 mars 2023, réunion nº 56, 1700.

> En ce qui concerne l'exactitude des renseignements qui sont fournis, des entreprises comme Google rendent publics leurs engagements en matière d'émissions de gaz à effet de serre pour leurs activités. Sept des huit fournisseurs avec lesquels nous traitons concernant l'infonuagique à Services partagés Canada ont atteint ou dépassé ces objectifs. Nous assurons le suivi auprès du huitième[52].

En conséquence, le Comité recommande :

Recommandation 5

Que, d'ici le 31 janvier 2025, Services publics et Approvisionnement Canada présente au Comité permanent des comptes publics de la Chambre des communes un rapport sur les critères environnementaux à utiliser dans le cadre de l'approvisionnement en services infonuagiques afin de favoriser la durabilité des pratiques d'approvisionnement et de contribuer à l'atteinte de l'objectif de carboneutralité du Canada.

Recommandation 6

Que, d'ici le 31 janvier 2025, Services partagés Canada présente au Comité permanent des comptes publics de la Chambre des communes un rapport indiquant les progrès réalisés relativement à l'élaboration de critères environnementaux à utiliser dans le cadre de l'approvisionnement en services infonuagiques afin de favoriser la durabilité des pratiques d'approvisionnement et de contribuer à l'atteinte de l'objectif de carboneutralité du Canada.

Autres constats en matière de sécurité

Le BVG a constaté des lacunes dans la façon dont les inspections de sécurité visant les fournisseurs de services infonuagiques étaient réalisées. Cependant, le BVG ne peut publier ces constatas parce que le faire révélerait de l'information sur des vulnérabilités et poserait un risque à la sécurité nationale. Il les a plutôt signalées directement à SPAC, accompagnées d'une recommandation concernant la communication des résultats des inspections liées à la sécurité matérielle aux parties prenantes et les réinspections liées à la sécurité matérielle[53].

52 *Ibid.*, 1710.

53 BVG, La cybersécurité des renseignements personnels dans le nuage, rapport 7 des Rapports de 2022 de la vérificatrice générale du Canada, paragr. 7.25.

CONCLUSION

Le Comité conclut que le gouvernement du Canada disposait de contrôles pour prévenir les événements de cybersécurité qui pourraient compromettre les renseignements personnels de la population canadienne stockés dans le nuage, détecter ces événements et agir en conséquence. Cependant, il ne les a pas appliqués efficacement et n'a pas établi et communiqué des rôles et des responsabilités clairs pour leur mise en œuvre.

En outre, le SCT n'a pas fourni aux ministères fédéraux de méthode de financement à long terme ou de modèle d'établissement des coûts pour les aider à mieux comprendre les coûts du passage à l'infonuagique et du fonctionnement dans le nuage. Enfin, le gouvernement fédéral n'a pas intégré de critères environnementaux à son processus d'approvisionnement en services infonuagiques, même s'il était tenu de réduire les émissions de gaz à effet de serre.

Dans le présent rapport, le Comité formule six recommandations pour aider le gouvernement du Canada à mieux gérer ses responsabilités à l'égard de la protection des renseignements personnels en ce qui a trait à l'utilisation des services infonuagiques.

ANNEXE A :
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
Bureau du vérificateur général	2023/03/30	56
Jean Goulet, directeur principal		
Andrew Hayes, sous-vérificateur général		
Gabriel Lombardi, directeur principal		
Centre de la sécurité des télécommunications	2023/03/30	56
Rajiv Gupta, dirigeant associé, Centre canadien pour la cybersécurité		
Ministère des Travaux publics et des Services gouvernementaux	2023/03/30	56
Catherine Poulin, sous-ministre adjointe, Direction générale de la surveillance		
Paul Thompson, sous-ministre		
Services partagés Canada	2023/03/30	56
Sony Perron, président		
Costas Theophilos, directeur général, Gestion des produits et des services infonuagiques		
Secrétariat du Conseil du Trésor	2023/03/30	56
Catherine Luelo, sous-ministre et dirigeante principale de l'information du canada		

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions n^{os} 56, et 138) est déposé.

Respectueusement soumis,

Le président,
John Williamson

Rapport dissident conservateur au 42e rapport du Comité permanent des comptes publics : La cybersécurité des renseignements personnels dans le nuage

44e législature

La coalition Libéral-NPD donne la priorité à la réduction idéologique des émissions de carbone plutôt qu'à la cybersécurité des Canadiens

Le Bureau de la vérificatrice générale du Canada a déposé un rapport cinglant qui montre à quel point le gouvernement du Canada ne fait pas grand-chose pour protéger la cybersécurité des Canadiens. Au lieu de remédier à ces lacunes, les libéraux ont réagi en liant les investissements nécessaires en matière de cybersécurité à la réduction des émissions de carbone.

Comme l'expliquent clairement le corps du rapport et le rapport de novembre 2022 du Bureau de la vérificatrice générale intitulé *La cybersécurité des renseignements personnels dans le nuage*, le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada, Services publics et Approvisionnements Canada et le Centre de la sécurité des télécommunications Canada n'ont pas réussi à protéger adéquatement les renseignements personnels des Canadiens en raison de l'incompétence des libéraux et du fait qu'ils n'ont pas accordé la priorité à cet enjeu urgent.

Le gouvernement du Canada devrait concentrer toutes ses ressources et ses efforts en matière de cybersécurité pour respecter ses propres règles et réglementations et surtout combler les lacunes afin que les Canadiens soient protégés. Il s'agit notamment de sécuriser les applications logicielles et les bases de données, de garantir l'application des garde-fous du nuage, ainsi que de prévenir les cyberattaques et d'y répondre.

Le gouvernement libéral ne devrait pas gaspiller les investissements et les ressources en cybersécurité dans sa quête idéologique de réduction des émissions de carbone ou d'autres gaz à effet de serre. La cybersécurité et la protection des Canadiens ne doivent pas être sacrifiées au profit des messages politiques du gouvernement libéral.

Le Bureau de la vérificatrice générale a signalé l'échec du gouvernement libéral dans la mise en œuvre de la stratégie d'adoption du nuage de 2018. Le rapport souligne également que les ministères ont du mal à comprendre leurs rôles et responsabilités, ce qui entraîne une certaine confusion en ce qui concerne les tâches liées à la cybersécurité. Cette confusion amplifie encore les risques potentiels pour la sécurité des Canadiens en raison de l'inefficacité bureaucratique et politique et de l'incompétence du gouvernement libéral. Compte tenu des retards, de la confusion et des risques potentiels pour la sécurité, il n'est pas prudent d'ajouter des tâches supplémentaires non liées.

Aucune preuve n'a été fournie pour suggérer que le fait de demander à Services publics et Approvisionnements Canada ou à Services partagés Canada de rédiger un rapport établissant un lien entre l'achat de services en nuage et la cybersécurité et l'objectif fixé pour 2050 contribuera à réduire les émissions.

Les conservateurs ne sont pas d'accord avec la mise en œuvre des recommandations 5 et 6 du rapport majoritaire, qui mettent l'accent sur la poursuite idéologique du gouvernement libéral en faveur de la neutralité nette plutôt que sur la protection des Canadiens.

Au lieu de cela, les conservateurs recommandent ce qui suit à la place des recommandations 5 et 6 :

> **Que, le Secrétariat du Conseil du Trésor du Canada prenne des mesures immédiates pour dissiper la confusion entre les ministères en ce qui concerne les rôles et les responsabilités en matière de cybersécurité et qu'il établisse enfin des mandats clairs et concis à l'intention des ministères concernés par la cybersécurité.**
>
> Et
>
> **Qu'en s'efforçant de remédier immédiatement aux défaillances signalées par la vérificatrice générale, Services publics et Approvisionnements Canada et Services partagés accordent la priorité à la protection des renseignements personnels des Canadiens et ne poursuivent pas d'objectifs sans rapport avec l'objet principal des opérations de cybersécurité.**