Audit du BVG sur la lutte contre la cybercriminalité

À propos de l'audit
L'objectif de l'audit est de déterminer si la GRC et certaines entités fédérales sélectionnées avaient la capacité et les moyens d'appliquer efficacement les lois contre les activités de cybercriminalité pour assurer la sécurité des Canadiens.

Le rapport contenait huit recommandations, dont sept s'adressaient à la GRC.

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	**Secteur responsable**	**Réponse ministérielle**	**Produit(s) livrable(s) spécifique(s) (Description/dates)**	**Date d'achèvement finale prévue**	**Mise à jour sur la mise en œuvre**
7.20 Le Centre national de coordination en cybercriminalité de la GRC devrait établir des procédures pour cerner les avis aux victimes les plus urgents et s'assurer qu'ils sont envoyés en premier. Le Centre devrait définir des attentes officielles sur la rapidité avec laquelle les avis aux victimes doivent être envoyés, évaluer le rendement par rapport à ces normes et veiller au respect de celles-ci.	RCMP Centre national de coordination de la cybercriminalité (CNC3)	**Recommandation acceptée.** Bien que la plupart des avis aux victimes hautement prioritaires soient suivis dans les 24 heures, le Centre national de coordination de la cybercriminalité (CNC3) de la GRC établira et officialisera des procédures normalisées pour définir le niveau de priorité pour les avis aux victimes. Le CNC3 appliquera une norme de service officielle et un processus d'établissement des priorités pour les avis aux victimes d'ici septembre 2024. Ce calendrier s'aligne sur la mise en œuvre complète prévue de la Solution nationale en matière de cybercriminalité, qui comprendra de nouvelles capacités pour mesurer	D'ici le 30 mai 2025, le CNC3 prévoit mettre en œuvre toutes les fonctionnalités de base de la Solution nationale en matière de cybercriminalité, qui comprendra de nouvelles fonctionnalités, caractéristiques et règles de validation opérationnelles du système pour les avis aux cybervictimes. La mise en œuvre complète de la Solution nationale en matière de cybercriminalité renforcera donc la capacité du CNC3 de produire les avis aux victimes hautement prioritaires (urgents) et d'en faire le suivi. Grâce à la mise en œuvre complète de la Solution nationale en matière de cybercriminalité et en fonction de ses procédures opérationnelles et de sa norme de service définie, le CNC3 prévoit produire les avis aux victimes dans les 24 heures, l'objectif de rendement étant de respecter cette norme de service dans au moins 95 % des cas.	**30 mai 2025**	Le CNC3 a élaboré des procédures opérationnelles réglementaires sur les avis aux victimes, notamment l'établissement des priorités, les normes de service et les méthodes provisoires pour mesurer les activités liées aux avis aux victimes. Le CNC3 a également peaufiné ses procédures quant à la formation des employés sur les activités internes relatives aux avis aux victimes, y compris les activités officielles pour l'analyse primaire et secondaire et la validation des avis aux victimes par l'ensemble des employés au CNC3 chargés de la réception et de la supervision. Le CNC3 dispose maintenant de procédures opérationnelles réglementaires pour déterminer le

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	**Secteur responsable**	**Réponse ministérielle**	**Produit(s) livrable(s) spécifique(s) (Description/dates)**	**Date d'achèvement finale prévue**	**Mise à jour sur la mise en œuvre**
		systématiquement les activités opérationnelles du CNC3. Les procédures de notification aux victimes du CNC3 continuent d'évoluer depuis sa capacité opérationnelle initiale en 2020. Ces avis sont maintenant un élément essentiel des efforts du CNC3 et des organismes canadiens d'application de la loi visant à réduire les préjudices de la cybercriminalité pour les organisations canadiennes. Les partenaires du CNC3 et des organismes canadiens d'application de la loi ont participé aux opérations internationales d'application de la loi visant à envoyer des avis aux cybervictimes, comme le démantèlement de l'infrastructure de rançongiciel du groupe Hive en 2023. Ces efforts ont permis d'empêcher des paiements relatifs à des rançongiels ou de les atténuer, et contribuent à protéger l'économie du Canada contre les rançongiciels et autres cyberintrusions.	Responsables : directeur général, Centre national de coordination en cybercriminalité (CNC3) et Centre antifraude du Canada (CAFC)		niveau de priorité des avis aux victimes. Les avis aux victimes hautement prioritaires (urgents) comprennent une norme de service prévoyant un délai d'exécution de 24 heures et un objectif de rendement consistant à respecter cette norme de service dans au moins 95 % des cas. Les avis aux victimes hautement prioritaires (urgents) portent notamment sur les attaques en temps réel et imminentes par rançongiciels ainsi que sur d'autres cyberattaques contre des organisations et des actifs canadiens. Dans ce contexte, le CNC3 s'engage à informer les services de police canadiens compétents (c.-à-d. ceux du lieu où est établie l'organisation victime) dans un délai de 24 heures. Depuis janvier 2024, le CNC3 a avisé les victimes dans un délai de 24 heures dans environ 80 % des cas, avec des résultats de rendement atteignant 93 % à 96 % en juillet 2024 et août 2024. Le CNC3 continuera de peaufiner et d'améliorer sa capacité de produire des avis aux victimes et de mesurer les

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
					activités connexes. Les principales activités à venir comprennent la mise en œuvre complète de la Solution nationale en matière de cybercriminalité, qui inclura de nouvelles fonctionnalités et caractéristiques du système qui permettront de produire avec plus d'exactitude des avis aux victimes et d'en faire le suivi.
7.24 Le Centre national de coordination en cybercriminalité de la GRC devrait veiller à ce que toutes les demandes d'assistance provenant de partenaires nationaux et internationaux soient dûment documentées et achevées, de sorte que toute l'information nécessaire soit transmise dans le cadre de la réponse. Le Centre devrait communiquer les demandes, s'il y a lieu, à toutes les organisations concernées par la demande.	RCMP Centre national de coordination de la cybercriminalité (CNC3)	**Recommandation acceptée.** Le Centre national de coordination contre la cybercriminalité (CNC3) de la GRC veillera à ce que toutes les demandes d'aide reçues des partenaires nationaux et internationaux de l'application de la loi soient entièrement consignées et complétées, et à ce que le CNC3 communique l'information, au besoin, aux organisations concernées. Depuis sa capacité opérationnelle initiale en 2020, le CNC3 a amélioré sa capacité à coordonner et à communiquer l'information avec les partenaires, tout en respectant le consentement de l'auteur et d'autres exigences en matière de communication de renseignements. Le CNC3 demande	D'ici le 30 mai 2025, le CNC3 prévoit mettre en œuvre toutes les fonctionnalités de base de la Solution nationale en matière de cybercriminalité, qui comprendra de nouvelles fonctionnalités, caractéristiques et règles de validation opérationnelles du système pour documenter et traiter les demandes d'assistance provenant des partenaires nationaux et internationaux du domaine de l'application de la loi. En particulier, la Solution nationale en matière de cybercriminalité comprendra des capacités complètes de suivi des audits pour les demandes opérationnelles et des capacités améliorées de partage d'information. Le CNC3 continuera de modifier et de mettre à jour ses procédures opérationnelles réglementaires et ses activités de formation des employés pour qu'elles soient harmonisées avec les nouvelles capacités et caractéristiques offertes	**30 mai 2025**	Le CNC3 a peaufiné ses procédures opérationnelles réglementaires pour mieux répondre aux demandes d'assistance provenant des partenaires nationaux et internationaux, notamment en améliorant la formation et le mentorat des nouveaux analystes et superviseurs du CNC3 chargés de traiter ces demandes. Le CNC3 continue de recevoir un volume élevé de demandes d'assistance provenant de partenaires chargés de l'application de la loi. Le programme reçoit annuellement environ 1 500 demandes d'assistance, dont environ 50 % proviennent de partenaires internationaux chargés de l'application de la loi. Dans de nombreux cas, ces demandes sont très complexes et

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
		également à ses partenaires de lui faire part de leurs commentaires sur ses services, notamment dans le cadre de sondages annuels. D'après les résultats des sondages, la plupart des partenaires actifs sont satisfaits ou très satisfaits des services du CNC3. D'ici septembre 2024 et après la mise en œuvre intégrale de la Solution nationale en matière de cybercriminalité (SNC), le CNC3 sera mieux outillé pour répondre pleinement aux besoins de ses partenaires nationaux et internationaux de l'application de la loi, notamment grâce à des capacités de suivi des audits plus complètes pour donner suite aux demandes opérationnelles et à des capacités de communication d'informations renforcées.	par la Solution nationale en matière de cybercriminalité. Responsables : directeur général, Centre national de coordination en cybercriminalité (CNC3) et Centre antifraude du Canada (CAFC)		peuvent inclure des enquêtes très pointues et de longue haleine sur la cybercriminalité ainsi que des opérations conjointes avec des partenaires. Le travail nécessaire pour évaluer les demandes et déterminer les protocoles appropriés en matière de partage d'information exige des décisions au cas par cas, y compris des procédures de traitement (protocole des feux de circulation) et des règles applicables aux tiers pour le partage d'information, en fonction des paramètres et des conditions établis par le partenaire national ou international chargé de l'application de la loi qui fournit les informations. Le CNC3 continuera de renforcer ses procédures de traitement des demandes d'assistance provenant de partenaires nationaux et internationaux. Ces améliorations comprendront la mise en œuvre complète de la Solution nationale en matière de cybercriminalité (prévue pour le 30 mai 2025), y compris de nouvelles capacités du système pour le suivi et le traitement des demandes d'assistance.

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
					Le calendrier de mise en œuvre complète de la SNC a été modifié en raison de la complexité du système et des exigences des utilisateurs.
7.30 La Police fédérale de la GRC devrait adopter un processus de triage uniforme géré de manière centralisée de sorte que les ressources spécialisées dans les enquêtes sur la cybercriminalité soient affectées aux enquêtes sur les cybercrimes les plus graves.		**Recommandation acceptée.** La GRC reconnaît qu'il faut redoubler d'efforts à cette fin. L'équipe de la Police fédérale chargée de la Cybercriminalité (EC) a commencé la mise en œuvre d'un processus de surveillance du respect de l'utilisation de l'Outil de triage des incidents (OTI) pour tous les nouveaux dossiers. L'OTI, lancé dans l'ensemble de la Police fédérale en 2020, est conçu pour guider les enquêteurs au fil d'un processus d'évaluation normalisé et complet, tout en repérant les obstacles possibles tels que le manque de ressources ou d'expertise. Un processus de surveillance structuré au sein des secteurs de programme permettra de veiller à la conformité et à ce que les ressources soient concentrées sur les enquêtes les plus importantes, tout en recueillant des données clés pour éclairer la prise de décision et la responsabilisation.	**<u>Résultat prévu :</u> Accent accru du Programme de cybercriminalité de la Police fédérale (PCPF) sur les cybercrimes les plus graves touchant le Canada.** Ce résultat sera atteint grâce aux activités suivantes : • Le PCPF a commencé à utiliser l'Outil de triage des incidents (OTI) pour tous les nouveaux dossiers (c.-à-d. les incidents). L'OTI vise à orienter les ressources et les opérations vers les menaces criminelles prioritaires relevant du mandat de la Police fédérale. Il assure l'uniformité à l'échelle nationale et fournit des orientations pour la prise de décision. • Les sections d'enquête de la Police fédérale doivent saisir l'OTI pour chaque nouvel incident créé dans le Système d'incidents et de rapports de police (SIRP), le système de gestion des dossiers de la GRC. • Le PCPF collaborera avec les équipes d'enquête sur la cybercriminalité de la	Outil de triage des incidents Mai 2025 Cadre de gouvernance du PCPF - Mars 2026	Le PCPF continue de surveiller l'utilisation de l'Outil de triage des incidents pour les nouveaux dossiers d'enquête de la Police fédérale et d'en assurer la conformité. La surveillance de l'utilisation de l'Outil de triage des incidents pour les nouveaux dossiers d'enquête de la Police fédérale relève également de la responsabilité des Enquêtes criminelles régionales, qui examinent les dossiers/incidents et font rapport aux chefs régionaux de la Police fédérale. Cette mesure a été prise afin de concentrer tous les efforts sur les priorités nationales de la Police fédérale, de recentrer toutes les ressources de la Police fédérale sur ses opérations et de soutenir la capacité d'intervention rapide et l'affectation des ressources. Le Plan de gestion des résultats du PCPF a été approuvé par le directeur général, Programme de cybercriminalité de la Police fédérale, en juillet 2024. Le Plan de gestion des résultats a été distribué à l'échelle du programme, y compris aux équipes d'enquête sur la

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
		En outre, l'EC a élaboré un plan d'action qui sera mis en œuvre par les équipes d'enquête sur la cybercriminalité partout au Canada afin de garantir le respect du mandat de la Police fédérale. Elle est convaincue qu'avec un mandat clair, un modèle de gouvernance défini et une meilleure coordination des activités de ces équipes, les résultats correspondront au mandat de la Police fédérale et se concentreront sur les menaces les plus graves.	Police fédérale pour surveiller régulièrement la conformité en ce qui concerne l'utilisation des outils de collecte de données et des mécanismes de signalement, incluant l'utilisation de l'Outil de triage des incidents, et utilisera ces informations pour orienter l'amélioration continue de ces outils ou mécanismes. • FOYER est un système d'interface utilisé par la Police fédérale, conçu pour combler les écarts entre les divers systèmes de données. Ce système vise à accroître l'uniformité et à augmenter la capacité du Groupe de soutien en matière de connaissance de la situation d'analyser justement les données opérationnelles et d'en rendre compte. De plus, afin d'encourager l'utilisation des données de Foyer pour éclairer la prise de décisions liées aux enquêtes de la Police fédérale, le Groupe de soutien en matière de connaissance de la situation publiera une nouvelle version du tableau de bord de l'OTI d'ici la fin de 2024. • Le PCPF a élaboré un plan de gestion des résultats pour définir les principales priorités du programme, qui comprend le soutien aux équipes d'enquête du PCPF. Le Plan de gestion des résultats vise à faire		cybercriminalité. Le Plan de gestion des résultats comprend 22 initiatives axées sur la réalisation des priorités du programme. La mise en œuvre de diverses initiatives est en cours. Dans le cadre du Plan de gestion des résultats, le PCPF en est aux premières étapes de l'élaboration d'un cadre de gouvernance et d'une politique opérationnelle pour le programme. Le PCPF a examiné et clarifié son mandat afin de s'assurer qu'il s'attaque aux cybercrimes les plus graves qui touchent le Canada. Les délais prévus pour l'élaboration et la mise en œuvre complètes des mesures proposées par le PCPF de la GRC en réponse aux recommandations du BVG restent incertains en raison de la complexité des solutions individuelles.

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	**Secteur responsable**	**Réponse ministérielle**	**Produit(s) livrable(s) spécifique(s)** **(Description/dates)**	**Date d'achèvement finale prévue**	**Mise à jour sur la mise en œuvre**
			progresser les initiatives clés dans le cadre des priorités stratégiques suivantes : ○ *Confiance accrue envers le Programme de cybercriminalité de la Police fédérale et efficacité améliorée de ses enquêtes grâce à la collaboration et aux partenariats* ○ *Efficacité opérationnelle du Programme de cybercriminalité de la Police fédérale grâce à la gouvernance et la reddition de compte* ○ *Recrutement, formation et perfectionnement au sein d'un programme de cybercriminalité de la Police fédérale moderne* ○ *Culture d'équipe et promotion d'un milieu de travail inclusif au sein du Programme de cybercriminalité de la Police fédérale* • Dans le cadre du Plan de gestion des résultats, le PCPF élaborera, diffusera et mettra en œuvre un cadre de gouvernance et une politique opérationnelle bien définis afin d'accroître l'efficience, de réduire les duplications et d'assurer l'harmonisation		

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
			des activités opérationnelles relevant du mandat de la Police fédérale.		
7.31 La GRC devrait s'assurer que ses systèmes de gestion de l'information recueillent des données exactes et complètes qui permettent d'évaluer le rendement, d'améliorer la prise de décisions et de démontrer l'optimisation des ressources en ce qui concerne les travaux effectués par le Groupe de lutte contre la cybercriminalité de la Police fédérale.		**Recommandation acceptée.** La Police fédérale de la GRC s'engage à collaborer avec le centre de décision chargé du Système de gestion des dossiers opérationnels (SGDO) de la GRC, connu sous le nom de Système d'incidents et de rapports de police, afin d'élaborer des façons d'accroître l'exactitude et l'exhaustivité des données concernant les enquêtes en matière de cybercriminalité. Elle a également débuté à discuter avec le centre de décision afin d'explorer des façons d'améliorer les rapports au sein du SGDO. Le délai de mise en œuvre des solutions choisies dépendra de leur complexité. En plus des efforts visant à améliorer les données du SGDO, la Police fédérale continuera d'élaborer des façons d'améliorer les rapports opérationnels complets, tout en augmentant la précision des données. Plus précisément, on prévoit lancer un nouveau rapport sur l'évolution de l'enquête qui	**<u>Résultat prévu :</u> Amélioration de l'exactitude et de l'exhaustivité des dossiers et des enquêtes du PCPF.** Ce résultat sera atteint grâce aux activités suivantes : • Le PCPF, l'équipe chargée de la responsabilisation de la Police fédérale et le Groupe de soutien en matière de connaissance de la situation collaboreront avec le centre de décision du système de gestion des dossiers opérationnels de la GRC pour élaborer des moyens d'améliorer l'exactitude et l'exhaustivité des données liées aux enquêtes sur la cybercriminalité de la Police fédérale. Ils devront notamment collaborer avec d'autres secteurs de la GRC pour créer un tableau de bord sur la qualité des données relatives à la cybercriminalité qui servira à signaler les problèmes de qualité des données liés à la cybercriminalité. Le Groupe de soutien en matière de connaissance de la situation travaille également avec d'autres secteurs d'activité de la GRC pour créer un tableau	Juillet 2025 – toutes les initiatives	Le PCPF continue de participer à des processus définis afin d'améliorer l'exactitude et l'exhaustivité des enquêtes et des dossiers. La phase pilote du rapport d'évolution des enquêtes sera lancée à l'été 2024 et devrait être déployée à l'échelle de la Police fédérale à l'hiver 2024-2025. Les délais pour l'élaboration et la mise en œuvre complètes des mesures proposées par le PCPF en réponse aux recommandations du BVG restent incertains en raison de la complexité des solutions individuelles.

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
		devrait améliorer l'exhaustivité des données opérationnelles en donnant un accès aux données à toutes les étapes d'une enquête, augmentant ainsi la responsabilisation et permettant la prise de décisions fondées sur des données probantes au moyen de données à jour, exactes et complètes. Le nouveau rapport sera mis à l'essai à compter de l'été 2024 et devrait être déployé dans l'ensemble de la Police fédérale à l'hiver 2024. De plus, la Police fédérale s'engage à collaborer avec le centre de décision pour le Système d'information sur la gestion des ressources humaines de la GRC, les systèmes de rapport financiers (TEAM) et le SGDO afin de développer des indicateurs qui démontreront le rapport qualité-prix (retour sur les investissements), mettre en place des méthodologies standardisées et d'identifier les capacités actuelles et les limites reliées à ces indicateurs.	de bord sur la qualité des données sur la cybercriminalité qui servira à signaler les problèmes de qualité des données liés aux dossiers de cybercriminalité. • Le Centre canadien de la statistique juridique et de la sécurité des collectivités (CCSJSC), en collaboration avec les services de police, recueille tous les ans des données sur les actes criminels déclarés par la police dans le cadre du Programme de déclaration uniforme de la criminalité (DUC). Le Programme DUC vise à mesurer la fréquence des crimes dans la société canadienne et leurs caractéristiques. La prochaine mise à niveau du Programme DUC dans le Système d'incidents et de rapports de police comprendra également de nouvelles variables de classification de la cybercriminalité qui aideront à fournir plus de détails sur la nature des incidents de cybercriminalité (maliciels, disponibilité des systèmes et des services, collecte d'information, intrusion, divulgation de données, fraudes, contenu abusif et exploitation). Des documents de référence (guides pratiques, procédures opérationnelles réglementaires) et de la formation seront fournis aux équipes		

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
			d'enquête sur la cybercriminalité afin de garantir que ces nouvelles données soient saisies dans le système de gestion des dossiers. Une fois la mise à niveau effectuée, la conformité des données sera surveillée. Le Groupe de soutien de la connaissance de la situation prévoit également ajouter ce nouveau champ au tableau de bord sur la qualité des données sur la cybercriminalité. • Le PCPF mobilisera également l'équipe du rendement et des résultats de la Police fédérale, le Groupe de soutien en matière de connaissance de la situation, l'équipe de recherche et de méthodologie de la Police fédérale, le Groupe des ressources humaines de la GRC et les centres de décisions en ressources financières afin d'établir des indicateurs qui démontrent une optimisation des ressources et le recours à des méthodes normalisées. • Le Groupe de soutien en matière de connaissance de la situation, en collaboration avec le PCPF, continuera d'appuyer l'examen et la mise à jour des outils existants de collecte de données et de production de rapports, incluant l'OTI et le rapport sur l'évolution de l'enquête,		

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
			afin de s'assurer que ces outils répondent aux exigences du programme en matière de production de rapports et permettent de saisir avec exactitude les données opérationnelles sur la cybercriminalité. • Grâce aux outils mis en œuvre par le Groupe de soutien en matière de connaissance de la situation, comme la fonction de surveillance de Foyer, le PCPF collaborera avec les équipes d'enquête sur la cybercriminalité afin de contrôler régulièrement la conformité des outils de collecte de données et des mécanismes de signalement, et utilisera ces informations pour améliorer en permanence ces outils et mécanismes. Il est à noter que la fonction de surveillance de Foyer permet aux divisions d'être au courant de la nature des incidents en rapport avec le mandat et les priorités de la Police fédérale et d'accroître la responsabilisation à tous les niveaux en enregistrant et en surveillant les mesures d'enquêtes prises et leur incidence. • Le PCPF examinera et mettra à jour les procédures opérationnelles réglementaires et la politique opérationnelle afin d'assurer la		

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
			conformité quant à l'utilisation des outils de collecte de données et de signalement.		
7.58 La GRC devrait améliorer ses systèmes et pratiques de gestion de l'information afin d'associer systématiquement les signalements reçus par le Centre antifraude du Canada aux mesures prises. La GRC pourra ainsi suivre les progrès réalisés par rapport aux cas hautement prioritaires et de cerner les approches efficaces utilisées.	RCMP Centre antifraude du Canada (CAFC)	**Recommandation acceptée**. Le Centre antifraude du Canada (CAFC) de la GRC veillera à effectuer le suivi et à rendre compte de toutes les mesures prises pour lutter contre les fraudes et les cybercrimes qui lui sont signalés. Le signalement des cybercrimes et des fraudes est essentiel pour les organismes d'application de la loi, car il leur permet d'orienter les mesures de lutte contre ces types de crimes prolifiques et graves. Sur le plan national, les mesures d'application de la loi comprennent l'identification de nouvelles menaces de cybercriminalité, les renvois à la police locale, la collaboration avec les partenaires de l'industrie pour perturber les menaces et adopter des tactiques de prévention pour réduire la victimisation, entre autres objectifs. Lorsqu'il est possible d'agir, le CAFC mène des activités de suivi pour les	En 2025, la GRC prévoit mettre en œuvre le Système national de signalement des incidents de cybercriminalité et de fraudes. Le nouveau système améliorera et simplifiera le signalement des cybercrimes et des fraudes dont des personnes sont victimes aux organismes d'application de la loi à l'échelle nationale. De plus, d'ici le 30 mai 2025, le CNC3 prévoit mettre en œuvre toutes les fonctionnalités de base pour la Solution nationale en matière de cybercriminalité. Cela comprendra de nouvelles fonctionnalités, caractéristiques et règles de validation opérationnelle qui permettront au CAFC de faire correspondre les signalements des victimes aux mesures prises, comme la mise en place de nouvelles capacités techniques pour le suivi des cas hautement prioritaires associés aux signalements de cybercrimes et de fraudes par les victimes. Responsables : directeur général, Centre national de coordination en cybercriminalité (CNC3) et Centre antifraude du Canada (CAFC)	**30 mai 2025**	Le CAFC continue d'améliorer ses systèmes et pratiques de gestion de l'information afin de faire correspondre les signalements des victimes aux mesures prises par le CAFC. La capacité du CAFC de donner suite aux signalements des victimes dépend de plusieurs facteurs, tels que l'exhaustivité et l'exactitude des signalements et l'établissement des priorités en fonction des données personnelles ou des pertes financières indiquées dans les signalements. Au cours de l'été 2024, le CAFC a procédé à une analyse manuelle des 320 signalements de victimes ayant subi des pertes financières d'au moins 10 000 $. L'analyse a révélé que le CAFC était en mesure de donner suite à 82 % de ces signalements, notamment grâce au renvoi de cas à la police locale, à des activités de perturbation et à des activités de prévention et d'analyses du renseignement ou d'autres mesures.

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
		signalements prioritaires de victimes. Le CAFC reconnaît que de nouvelles capacités techniques sont nécessaires pour améliorer le suivi systématique des signalements de victimes. En 2024, le CAFC et le CNC3 mettront en œuvre un nouveau système national de signalement des incidents de cybercriminalité et de fraude qui améliorera le signalement des victimes à l'échelle nationale à des fins d'application de la loi. Le système de signalement en ligne comprend de nouvelles capacités techniques permettant au CAFC de relier systématiquement les signalements de victimes aux activités de suivi.			Le CNC3 et le CAFC poursuivent la mise en œuvre du Système national de signalement des incidents de cybercriminalité et de fraude, qui améliorera le signalement des cybercrimes et des fraudes dont des personnes sont victimes aux organismes d'application de la loi à l'échelle nationale. La mise en œuvre complète du système est prévue à la fin de 2024. Le système comprendra de nouvelles capacités techniques liées à la Solution nationale en matière de cybercriminalité pour faire correspondre systématiquement les signalements des victimes aux mesures prises par le CAFC. La capacité du CAFC à mettre en correspondance les signalements des victimes et les mesures prises de manière systématique et évolutive sera encore améliorée lorsque la Solution nationale en matière de cybercriminalité sera pleinement mise en œuvre (prévue pour le 30 mai 2025).
7.64 La GRC devrait mener une analyse pour comprendre ses difficultés à recruter et à maintenir en poste du personnel pour les postes spécialisés en cybercriminalité. Elle devrait ensuite		**Recommandation acceptée**. La Police fédérale a élaboré une stratégie de recrutement et de développement de l'expertise en cybersécurité. La GRC s'attaquera également aux défis liés au	**<u>Résultat prévu</u> : Amélioration du recrutement par le PCPF de ressources possédant des compétences, des connaissances et de l'expérience spécialisées en matière de cybersécurité/cybercriminalité.**	Janvier 2026 – toutes les initiatives	Le PCPF continue de participer à des processus définis afin de rester une option concurrentielle et intéressante pour les ressources formées en cybersécurité. Bien que les ressources cybernétiques restent limitées, le PCPF

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
se servir des résultats de cette analyse pour orienter ses futurs efforts de recrutement et de maintien en poste en vue d'accroître sa capacité de lutte contre la cybercriminalité.		recrutement et à la rétention des employées dans le cadre des efforts futurs visant à améliorer la capacité de lutte contre la cybercriminalité au cours des deux ou trois prochaines années, notamment, dans le cadre d'initiatives de modernisation plus vastes, des gains d'efficacité dans le processus de sélection pour le Programme des enquêteurs criminels civils ainsi qu'en explorant comment des initiatives comme le Programme des policiers expérimentés peuvent aider à relever ces défis. Malgré la pénurie de cybercompétences, la GRC continue de recruter des personnes spécialisées, notamment au moyen du programme des enquêteurs criminels civils et des stages pour étudiants COOP afin d'attirer de nouveaux talents. La formation est un autre outil stratégique. Le Programme de formation de la Police fédérale fournit un guide pour tous les enquêteurs, y compris ceux du domaine de la cybercriminalité, qui a été diffusé à l'échelle nationale en janvier 2024.	Ce résultat sera atteint grâce aux activités suivantes : • Le PCPF collaborera avec des partenaires internes et externes clés afin d'élaborer et de mettre en œuvre une stratégie fédérale en matière de ressources humaines afin de mieux soutenir la mise en œuvre des programmes et d'assurer leur viabilité. • Dans le cadre de sa stratégie en matière de ressources humaines, le PCPF collaborera avec des partenaires internes et externes clés pour moderniser les initiatives de recrutement existantes et exploiter de stratégies et de plateformes de recrutement novatrices. • L'équipe du Programme des enquêteurs criminels civils travaille actuellement avec un spécialiste de la dotation pour moderniser le processus et les outils de dotation des postes d'enquêteurs criminels civils afin d'attirer et d'embaucher des employés civils possédant des compétences spécialisées pour travailler avec des policiers au sein d'équipes d'enquête intégrées. La Gestion de l'effectif de la Police fédérale fait activement la promotion des offres d'emploi d'enquêteur criminel		continue de rechercher des candidats dûment formés pour occuper des postes dans ce domaine en modernisant ses initiatives de recrutement et en mettant à jour sa stratégie en matière de ressources humaines. Le PCPF a entrepris d'examiner la possibilité de créer un programme de formation viable en matière de cybercriminalité. Le PCPF a également consulté des intervenants externes afin d'examiner des possibilités de formation. Les délais pour l'élaboration et la mise en œuvre complètes des mesures proposées par le PCPF en réponse aux recommandations du BVG restent incertains en raison de la complexité des solutions individuelles.

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
		Il tire également parti d'autres formations offertes par des partenaires externes et le Collège canadien de police de la GRC. Le CNC3 a lancé le Portail de cyberapprentissage qui fournit des ressources aux employés de la GRC à l'appui des enquêtes liées à la cybercriminalité.	civil par le biais de LinkedIn ainsi que lors d'activités de recrutement, dans le but de recruter des candidats susceptibles de contribuer à un effectif diversifié et professionnel. • Le PCPF continuera de collaborer avec les programmes de recrutement et les programmes COOP établis afin d'améliorer le recrutement de ressources possédant des compétences, des connaissances et de l'expérience spécialisées en matière de cybersécurité/cybercriminalité. **<u>Résultat prévu</u> : Formation accrue en matière de cybersécurité/cybercriminalité et développement des capacités et des compétences dans ce domaine.** Ce résultat sera atteint grâce aux activités suivantes : • Le PCPF collaborera avec les principaux intervenants pour examiner la viabilité d'un programme de formation de base approuvé en matière de cybercriminalité, comprenant des cours obligatoires et recommandés. La structure de l'effectif diversifié et les besoins des équipes d'enquête du PCPF seront pris en compte (c.-à-d. enquêteurs		

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
			membres réguliers, enquêteurs criminels civils, analystes du renseignement et ressources techniques). • Le PCPF continuera d'examiner les possibilités de formation offertes par des partenaires externes. **<u>Résultat prévu :</u> Amélioration du maintien en poste des ressources formées en cybersécurité par la Police fédérale.** Ce résultat sera atteint grâce aux activités suivantes : • Le PCPF évaluera régulièrement le maintien en poste des employés à son quartier général ainsi qu'au sein des équipes d'enquête sur la cybercriminalité, afin de mieux orienter les efforts en matière de dotation. • Le PCPF continuera de faire preuve d'innovation dans la recherche de nouvelles possibilités de formation et d'apprentissage et d'outils et de technologies cybernétiques pour appuyer les enquêtes sur la cybercriminalité.		

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
7.69 La GRC devrait veiller à régler les problèmes associés à la mise en adéquation des fonctionnalités de la Solution nationale en matière de cybercriminalité avec les besoins des utilisatrices et des utilisateurs afin que le projet respecte l'ensemble des exigences énoncées. Elle devrait aussi mettre en œuvre des réponses efficaces aux risques et des plans d'urgence pour que le projet soit réalisé dans le respect du budget et du calendrier révisé.	RCMP Centre national de coordination de la cybercriminalité (CNC3)	**Recommandation acceptée**. La GRC veillera à ce que les difficultés liées à la Solution nationale en matière de cybercriminalité soient atténuées et à ce que les besoins des utilisateurs correspondent aux exigences du système d'ici mars 2025. La Solution est une importante initiative technologique qui permettra à la GRC et à la communauté canadienne de l'application de la loi de disposer de capacités nouvelles pour appuyer les enquêtes entre plusieurs administrations sur la cybercriminalité. La Solution nationale en matière de cybercriminalité, lancée au début de la pandémie de COVID-19, est une initiative complexe qui comprend de nouvelles approches en matière d'approvisionnement et de système pour la GRC. La mise en œuvre de la nouvelle Solution connaît des difficultés et des retards. Pour atténuer les risques, la GRC a demandé un examen indépendant de celle-ci. Bien que l'examen ait cité la	D'ici le 30 mai 2025, le CNC3 prévoit mettre en œuvre toutes les fonctionnalités de base de la Solution nationale en matière de lutte contre la cybercriminalité. Il s'agit d'un projet complexe, qui comprend un grand nombre de nouvelles caractéristiques novatrices visant à permettre aux organismes canadiens d'application de la loi de lutter contre la cybercriminalité. Malgré les relations de travail étroites entre la GRC, le fournisseur de la Solution nationale en matière de cybercriminalité et Services publics et Approvisionnement Canada (autorité contractante), le projet comporte des risques inhérents compte tenu de la portée et de l'ampleur des activités. La GRC continuera de mettre en œuvre des stratégies d'atténuation des risques et d'intervention pour gérer les risques liés au projet. Cela étant dit, les retards futurs relativement à la Solution nationale en matière de cybercriminalité demeurent un risque actif et étroitement surveillé. De plus, la lutte contre la cybercriminalité dans un contexte d'application de la loi exige des stratégies et des approches évolutives pour suivre le rythme du milieu criminel et des avancées technologiques. Compte tenu de cette complexité, la GRC prévoit que la Solution nationale en matière de cybercriminalité	**30 mai 2025 / En cours**	La GRC continue de travailler en étroite collaboration avec ses partenaires chargés de l'application de la loi pour veiller à ce que la Solution nationale en matière de cybercriminalité réponde aux besoins des utilisateurs. À ce jour, la GRC a intégré certains partenaires chargés de l'application de la loi aux niveaux fédéral, provincial et municipal au Canada afin qu'ils aient accès à la Solution nationale en matière de cybercriminalité, l'utilisent, et contribuent à son développement et à sa mise en œuvre continus. La GRC a également amélioré la communication avec le fournisseur de la Solution nationale en matière de cybercriminalité, notamment en lui transmettant régulièrement les commentaires des utilisateurs (p. ex. sur les caractéristiques et les fonctionnalités du système). La GRC continue également de collaborer étroitement avec le fournisseur de la Solution nationale en matière de cybercriminalité et Services publics et Approvisionnement Canada (autorité contractante) pour surveiller et évaluer de près les risques liés au projet associés

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
		Solution comme une initiative phare avec de bonnes pratiques, elle contenait des recommandations sur les contraintes en matière de ressources, l'assurance de la prestation des systèmes, les besoins des utilisateurs et les activités de transfert des connaissances. La GRC mettra en œuvre ces recommandations afin d'atténuer les risques liés à la mise en œuvre continue de la Solution nationale en matière de cybercriminalité et continuera de travailler en collaboration avec les partenaires pour s'assurer que la Solution répond aux besoins des partenaires et qu'elle s'harmonise avec les politiques du gouvernement du Canada en matière de services numériques axés sur l'utilisateur, et ce, dès maintenant et jusqu'au 31 mars 2025.	fera l'objet d'itérations futures et continues et que des changements seront apportés au système afin de suivre l'évolution des besoins des organismes canadiens d'application de la loi. La GRC continuera de travailler en étroite collaboration avec le fournisseur de la Solution nationale en matière de cybercriminalité, ses partenaires fédéraux et les utilisateurs. Tout changement éventuel au calendrier du projet et à la portée des activités tiendra pleinement compte des stratégies d'atténuation des risques et des besoins des utilisateurs afin de garantir que la mise en œuvre complète de la Solution nationale en matière de cybercriminalité soit aussi optimale que possible. Responsables : directeur général, Centre national de coordination en cybercriminalité (CNC3) et Centre antifraude du Canada (CAFC)		à la Solution. Activités de surveillance et de gouvernance du projet, y compris la mobilisation du comité directeur du projet, les réunions bimensuelles et ponctuelles, les activités liées au sprint de développement du projet et du système, entre autres mesures.
7.78 Sécurité publique Canada, la GRC, le Centre de la sécurité des télécommunications Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes devraient collaborer pour veiller à ce que les cybercrimes signalés par les	RCMP Centre national de coordination de la cybercriminalité (CNC3)	**Recommandation acceptée.** La GRC continuera de travailler avec ses partenaires fédéraux pour s'assurer que les cybercrimes signalés sont acheminés vers les organismes fédéraux appropriés. Elle reconnaît que les signalements des victimes	En 2025, la GRC prévoit mettre en œuvre le Système national de signalement des incidents de cybercriminalité et de fraude. Le nouveau système améliorera et simplifiera le signalement des cybercrimes et des fraudes dont des personnes sont victimes aux organismes d'application de la loi à l'échelle nationale.	**31 mars 2026 / permanent**	La GRC continue de collaborer étroitement avec ses partenaires fédéraux afin d'améliorer le partage d'information et de simplifier le processus de signalement des cybercrimes et des fraudes au Canada, notamment par les particuliers, les

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	Secteur responsable	Réponse ministérielle	Produit(s) livrable(s) spécifique(s) (Description/dates)	Date d'achèvement finale prévue	Mise à jour sur la mise en œuvre
particuliers et les entreprises canadiennes soient acheminés à l'organisation dotée du mandat en la matière.		sont essentiels pour lutter contre la cybercriminalité et que de nombreux incidents ne sont pas signalés aux autorités policières. La GRC continue de mener des activités de sensibilisation auprès d'organismes du secteur privé, de groupes vulnérables et d'autres communautés afin d'améliorer le signalement et d'encourager le rôle des organismes d'application de la loi dans les plans d'intervention en cas d'incidents cybernétiques. La mise en œuvre du nouveau Système national de signalement des incidents de cybercriminalité et de fraude en 2024 permettra également aux victimes de signaler plus facilement les incidents aux organisations d'application de la loi sur le plan national. La GRC reconnaît également qu'il faut redoubler d'efforts pour harmoniser les activités opérationnelles dans la collectivité fédérale en matière d'intervention en cas de cyberincident, ainsi que pour trouver des façons de simplifier et de rationaliser la	De plus, d'ici le 30 mai 2025, le CNC3 prévoit mettre en œuvre toutes les fonctionnalités de base de la Solution nationale en matière de cybercriminalité. La GRC continuera de travailler en étroite collaboration avec les partenaires fédéraux pour améliorer davantage l'acheminement des signalements des victimes vers les partenaires fédéraux appropriés, en plus d'examiner des façons de simplifier le processus de signalement des cybervictimes dans l'ensemble du gouvernement. La GRC considère qu'il s'agit d'une activité permanente, étant donné que les mesures fédérales de lutte contre la cybercriminalité devront constamment évoluer pour répondre aux besoins des particuliers, des entreprises et des organismes canadiens victimes de cybercrimes. La GRC reconnaît les efforts déployés par le Centre canadien pour la cybersécurité (CCCS) afin d'examiner des stratégies sur le plan politique, technique et des communications pour améliorer l'acheminement des signalements de cybercriminalité vers l'organisme fédéral compétent. La GRC continuera de travailler avec le CCCS et d'autres partenaires fédéraux au cours des deux prochaines années et par la suite pour améliorer la façon dont les signalements de cybercriminalité sont traités à l'échelle nationale.		entreprises et d'autres organisations victimes. Pour la GRC, le Système national de signalement des incidents de cybercriminalité et de fraude du NC3 et du CAFC, dont la mise en œuvre complète est prévue pour la fin de 2024, constitue une étape importante dans ce contexte. La GRC prévoit que le nouveau système recevra 100 000 signalements ou plus de la part de victimes de cybercriminalité et de fraude. Le CNC3 et le CAFC continuent également de collaborer étroitement avec le Centre canadien pour la cybersécurité et d'autres partenaires fédéraux afin d'assurer cohérence et la clarté des messages transmis aux Canadiens sur le signalement d'incident de cybercriminalité par les victimes et les moyens de signaler les cybercrimes et les fraudes au gouvernement du Canada, en plus de les signaler aux services de police locaux au Canada.

Recommandation du BVG (N° du paragraphe seulement jusqu'au dépôt le 4 juin)	**Secteur responsable**	**Réponse ministérielle**	**Produit(s) livrable(s) spécifique(s)** **(Description/dates)**	**Date d'achèvement finale prévue**	**Mise à jour sur la mise en œuvre**
		manière dont les organisations qui représentent les victimes et les particuliers signalent les incidents et reçoivent le soutien de la GRC et de ses partenaires fédéraux. La GRC continuera de travailler en étroite collaboration avec ses partenaires fédéraux en vue d'améliorer les services de signalement et d'intervention offerts aux victimes de cybercriminalité.	Responsables : directeur général, Centre national de coordination en cybercriminalité (CNC3) et Centre antifraude du Canada (CAFC)		