Public Safety Canada | Sécurité publique Canada

Sécurité publique Canada
Vérification interne du cadre de contrôle de gestion des renseignements personnels

Septembre 2015

Canada

TABLE DES MATIÈRES

SOMMAIRE

Contexte

Les fonctionnaires de Sécurité publique Canada (« SP » ou le « Ministère ») fournissent des conseils et un soutien stratégiques au ministre de la Sécurité publique et de la Protection civile sur toute une gamme d'enjeux, y compris la sécurité nationale, les stratégies frontalières, la lutte contre la criminalité et la gestion des urgences. Ils mettent aussi en œuvre un certain nombre de programmes de subventions et de contributions liés à la gestion des urgences, à la sécurité nationale ainsi qu'à la sécurité des collectivités. Le Ministère coordonne également les efforts déployés par les organismes du portefeuille de la sécurité publique et contribue à orienter leurs priorités stratégiques. Les organismes du portefeuille sont, de par leur nature, plus opérationnels; cela comprend l'Agence des services frontaliers du Canada (ASFC), le Service canadien du renseignement de sécurité (SCRS), le Service correctionnel du Canada (SCC), la Commission des libérations conditionnelles du Canada (CLCC) et la Gendarmerie royale du Canada (GRC).

SP est assujetti à la *Loi sur la protection des renseignements personnels* et doit se conformer à ses exigences relatives à la gestion et à la protection des renseignements personnels. En vertu de la *Loi sur la protection des renseignements personnels,* « renseignements personnels » s'entend au sens large des « *renseignements, quels que soient leur forme et leur support, concernant un individu identifiable* ». La *Loi sur la protection des renseignements personnels* protège la vie privée de tous les citoyens canadiens et des résidents permanents contre l'utilisation ou la divulgation non autorisée des renseignements personnels dont dispose une institution gouvernementale. La *Loi sur la protection des renseignements personnels* confère aux citoyens le droit d'accéder aux renseignements détenus par le gouvernement à leur sujet. Le Secrétariat du Conseil du Trésor (SCT) a également mis en œuvre des politiques et des directives en matière de protection des renseignements personnels qui établissent des exigences supplémentaires sur la collecte et la gestion des renseignements personnels, y compris la *Politique sur la protection de la vie privée*, la *Directive sur l'évaluation des facteurs relatifs à la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée*.

Étant donné le rôle du Ministère dans la coordination des politiques et des conseils, il ne lui incombe pas de recueillir une quantité importante de renseignements personnels directement auprès du public; ainsi, un petit nombre seulement d'activités liées à la collecte et à la gestion des renseignements personnels sur les citoyens a été cerné au cours de la vérification. Parmi les renseignements personnels détenus par le Ministère, les renseignements personnels sur les employés représentent l'une des plus importantes catégories, sinon la plus grande; ces renseignements sont colligés dans le cadre de la gestion des ressources humaines.

Bien que le Ministère ne gère pas un nombre important de fichiers de renseignements personnels, les renseignements qu'il gère sont souvent de nature délicate. Une atteinte à la vie privée au sein du Ministère (p. ex. la collecte, l'utilisation, la divulgation, la conservation ou l'élimination de renseignements personnels ou, encore, l'accès non autorisé à ces renseignements) pourrait avoir de graves conséquences pour la réputation de SP ainsi que des incidences opérationnelles, comme entraver la capacité du Ministère à accéder aux données de recherche dont il a besoin. En

outre, compte tenu du rôle de coordination et de soutien du Ministère dans le portefeuille de la sécurité publique, ainsi que de son rôle de sensibilisation auprès d'autres compétences et intervenants du domaine de la sécurité publique, toute atteinte à la réputation peut avoir de graves incidences sur l'ensemble du gouvernement. De plus, une atteinte à la vie privée peut entraîner l'utilisation de ressources ministérielles pour mener une enquête à cet égard et y répondre, y compris les réponses aux demandes du Commissariat à la protection de la vie privée du Canada (CPVP) ou aux activités de vérification.

Objectif et portée de la vérification

La vérification visait à garantir de façon raisonnable que le Cadre de contrôle de gestion des renseignements personnels du Ministère est adéquat et efficace de sorte que le Ministère se conforme à la *Loi sur la protection des renseignements personnels* et aux politiques connexes tant du Secrétariat du Conseil du Trésor (SCT) que de SP.

La portée de la vérification, qui concernait la période se terminant le 30 avril 2015, était d'examiner le cadre de responsabilisation et de politique ainsi que les procédures clés et autres mesures de contrôle qui ont été mises en place pour :

- assurer la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques connexes du SCT et de SP;
- définir et communiquer les exigences dans ce domaine;
- assurer une réponse efficace et efficiente à ces exigences;
- préserver la réputation et la crédibilité du Ministère en ce qui concerne la gestion ministérielle des renseignements personnels.

En fonction de la phase de planification de la vérification, on a fait surtout porter la vérification sur l'examen du cadre de gestion de la protection de la vie privée du Ministère et son application sur certains renseignements personnels qu'il détient. Au cours de la phase de planification, les renseignements personnels détenus par le Ministère concernant autant les employés de SP que le grand public, à la fois en format électronique et papier, ont été déterminés. En fonction des activités de planification menées, des secteurs détenant des renseignements personnels ont été choisis aux fins d'un examen plus approfondi. Ce sont les suivants :

- le Secteur de la gestion des urgences et des programmes (SGUP);
- le Secteur de la sécurité communautaire et de la réduction du crime (SSCRC);
- le Secteur de la sécurité et de la cyber sécurité nationale (SSCN);
- le Secteur de la gestion ministérielle (SGM).

La portée de la vérification englobe les renseignements personnels détenus qui concernent les employés de SP et le grand public, en format électronique et papier.

Résumé des constatations

L'équipe de vérification a observé des exemples de la bonne conception des contrôles et de leur application efficace. Cette vérification a permis de relever plusieurs points forts :

- Dans l'ensemble de ses activités, le Ministère s'est assuré d'avoir en place des pratiques appropriées de « gestion des incidents » en cas d'atteinte à la vie privée, notamment par l'élaboration et la mise en œuvre de politiques et de processus en matière de gestion des atteintes à la vie privée. Il convient également de noter qu'en ce qui concerne les atteintes à la vie privée portées à l'attention de la Division de l'accès à l'information et de la protection des renseignements personnels (AIPRP), l'équipe de vérification a constaté qu'elles ont été traitées et suivies de façon appropriée.
- Une politique et des processus visant la conduite des évaluations des facteurs relatifs à la vie privée (EFVP) ont été mis en œuvre et les évaluations passées en revue ont été réalisées et gérées de façon appropriée.
- Le Ministère a défini la délégation des pouvoirs relativement à la *Loi sur la protection des renseignements personnels* et les rôles et les responsabilités de la Division de l'AIPRP sont clairement établis pour les activités menées au sein de la division.
- On a constaté que deux postes ont récemment été pourvus (en septembre 2014) au sein de la Division de l'AIPRP afin que l'on puisse se concentrer davantage à l'élaboration et à la mise en œuvre de politiques et d'activités de formation et de sensibilisation en matière d'accès à l'information et de protection des renseignements personnels, composante essentielle des programmes de protection des renseignements personnels.
- Les employés du Ministère à qui l'on a parlé durant la vérification ont démontré qu'ils comprenaient l'importance de protéger les renseignements personnels.

Dans le cadre de gestion de la protection de la vie privée (CGPVP) existant, la vérification a permis de constater que certains domaines, où les pratiques et les processus ont fait l'objet d'examen, pouvaient être améliorés pour réduire le risque d'une atteinte à la vie privée, comme cela est résumé ci-dessous :

<u>Cadre de gestion de la protection de la vie privée (CGPVP) du Ministère</u>

Bien que le Ministère dispose d'un cadre de gestion de la vie privée (CGPVP), ce cadre continue à évoluer et à mûrir et certaines lacunes ont été observées tout au long de la vérification. De manière générale, la vérification a permis de noter que la Division de l'AIPRP n'a pas été bien intégrée dans les processus opérationnels du Ministère et que les rôles et les responsabilités de cette division concernant la protection des renseignements personnels par rapport à d'autres domaines fonctionnels n'étaient pas clairement définis ou officiellement établis. Par conséquent, la Division de l'AIPRP n'a pas été consultée sur un certain nombre de domaines pour lesquels sa contribution aurait été appropriée, y compris l'élaboration d'ententes sur l'échange d'information qui contiennent des renseignements personnels. En outre, des préoccupations ont été soulevées du fait que certains programmes ou domaines fonctionnels pouvaient ne pas reconnaître la Division de l'AIPRP en tant que premier point de contact pour les questions liées à la protection de la vie privée et consulter plutôt d'autres groupes (p. ex. les services juridiques ou de sécurité) du Ministère, voire consulter directement le CPVP.

Dans certains secteurs de programme qui ont fait l'objet de la vérification, les renseignements personnels étaient recueillis et gérés sans qu'une EFVP ne soit menée ou sans qu'une évaluation formelle ne soit effectuée pour déterminer si une EFVP était requise.

La vérification a révélé qu'il n'y avait pas de processus et de mesures en place pour effectuer l'évaluation et mesurer l'efficacité de la mise en œuvre du CGPVP du Ministère. De plus, bien qu'il y ait eu un suivi régulier des activités liées à la protection des renseignements et aux atteintes à la vie privée, ce suivi n'a pas été officialisé.

Par ailleurs, le plan de formation provisoire de la Division de l'AIPRP pourrait être amélioré grâce à un meilleur ciblage de la formation envisagée vers les secteurs de programme comportant des risques précis ou plus élevés et qui recueillent ou gèrent des renseignements personnels.

Contrôles liés à la gestion des renseignements personnels

Même si aucun problème important n'a été observé quant à la façon dont les renseignements personnels ont été recueillis, utilisés et divulgués dans les secteurs inclus dans la portée de la vérification, les processus liés à la façon dont les renseignements personnels sont gérés par les secteurs de programme n'ont généralement pas été formellement documentés. Sans lignes directrices et processus documentés de manière officielle quant à la gestion des renseignements personnels, il y a un risque que les pratiques appropriées ne soient pas respectées, surtout s'il y a des changements de personnel dans les secteurs qui gèrent les renseignements personnels. En outre, des procédures d'exploitation formelles et normalisées sont essentielles pour démontrer aux intervenants et au CPVP que des processus appropriés ont été établis et qu'ils sont en place pour soutenir le Ministère s'il se produisait une atteinte à la vie privée.

De plus, il a été noté que certains domaines fonctionnels ont établi des périodes de conservation très longues ou indéfinies pour les fichiers contenant des renseignements personnels.

Protection des renseignements personnels

En se fondant sur le travail de vérification effectué, on constate que les principaux référentiels de fichiers contenant des renseignements personnels au sein de SP sont le Système de gestion des dossiers, des documents et de l'information (SGDDI), PeopleSoft, le lecteur réseau, les dispositifs de stockage portatifs et les classeurs sécurisés. Les classeurs sécurisés et l'accès à PeopleSoft font l'objet d'un contrôle efficace; cependant, la vérification a révélé des faiblesses dans les contrôles de l'accès au SGDDI et aux dossiers du réseau. En outre, il a été noté que la fonction de gestion de l'information n'est pas apte à surveiller officiellement les incidents lorsque l'accès accordé est excessif. Restreindre l'accès aux renseignements personnels aux personnes qui nécessitent un accès dans le cadre de leurs fonctions contribue à atténuer le risque d'une atteinte à la vie privée.

Opinion du vérificateur

Au Ministère, des problèmes de moyenne importance se posent en ce qui concerne la pertinence et l'efficacité du cadre de contrôle de gestion des renseignements personnels et du respect de la *Loi sur la protection des renseignements personnels* et des politiques connexes du SCT et de SP. Néanmoins, des améliorations pourraient être apportées au cadre afin de mieux cerner les risques et d'assurer un suivi approprié pour prévenir et détecter les activités non conformes.

La vérification et le rapport qui en découle ont été réalisés à l'intention de la direction de SP. L'utilisation du rapport à d'autres fins pourrait ne pas être appropriée.

Énoncé d'assurance et de conformité

Cette vérification est conforme aux Normes relatives à la vérification interne au sein du gouvernement du Canada, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité.

Selon mon jugement professionnel en tant que dirigeant principal de la vérification, des procédures de vérification suffisantes et appropriées ont été suivies et des éléments de preuve recueillis pour confirmer l'exactitude des opinions formulées et contenues dans ce rapport. L'opinion repose sur une comparaison des conditions, telles qu'elles se présentaient au moment de la vérification, avec des critères de vérification préalablement établis et approuvés par la gestion. Elle ne s'applique qu'à l'entité examinée.

Recommandations

1. Le sous-ministre adjoint du Secteur des affaires du Portefeuille et des communications devrait élaborer et mettre en œuvre un plan formel, comprenant des échéanciers et des responsabilités, afin de combler les lacunes décelées dans le CGPVP du Ministère. Le plan devrait prévoir ce qui suit :
    a. Définir les rôles et les responsabilités relatifs à la protection des renseignements personnels des secteurs fonctionnels ainsi que l'intégration des considérations liées à la protection des renseignements personnels dans les processus opérationnels.
    b. Officialiser le processus de mise à jour des entrées des fichiers de renseignements personnels (FRP) et examiner ces derniers pour s'assurer que les fonds de renseignements personnels utilisés à des fins administratives au sein du Ministère ont des entrées de FRP correspondantes dans Info Source. La Division de l'AIPRP devrait d'abord entreprendre un processus plus approfondi de mise à jour des FRP pour s'assurer que le répertoire de tous les renseignements personnels détenus par le Ministère est bien documenté. Cela devrait également tenir compte des renseignements personnels utilisés à des fins non administratives.
    c. Établir des politiques et des lignes directrices ministérielles qui énoncent les exigences relatives à la protection des renseignements personnels pour l'élaboration d'ententes sur l'échange d'information et d'ententes de contribution.
    d. Passer en revue et exécuter le plan de formation de manière à cibler une formation axée sur des secteurs de programme comportant des risques précis ou plus élevés et qui gèrent

des renseignements personnels et mettre ce plan en œuvre en temps opportun. La Division de l'AIPRP devrait coordonner la formation prévue avec la formation de base offerte par l'École de la fonction publique du Canada. Dans le cadre de la formation, il convient de rappeler que les secteurs de programme qui gèrent des renseignements personnels devraient consulter la Division de l'AIPRP et envisager la nécessité d'effectuer une EFVP. En outre, les secteurs de programme qui font la collecte et la gestion des renseignements personnels sans avoir effectué une EFVP, selon la vérification, devraient soit effectuer une EFVP ou justifier le fait de ne pas mener une telle évaluation.

e. Établir un programme de surveillance dont les paramètres de rendement permettraient d'évaluer et de mesurer la réussite du programme de protection des renseignements personnels et de présenter régulièrement à la haute direction (p. ex. trimestriellement au comité de gestion ministériel) des données particulières sur l'état des questions clés en matière de protection des renseignements personnels.

2. Chaque sous-ministre adjoint devrait documenter officiellement les processus pour la collecte, l'utilisation et la divulgation des renseignements personnels dans les secteurs de programme qui gèrent des renseignements personnels. Cela devrait inclure des lignes directrices claires relativement à l'utilisation des renseignements personnels afin qu'il y ait une compréhension cohérente de ce qui constitue une gestion et une protection acceptables des renseignements personnels.

3. Chaque sous-ministre adjoint, le cas échéant, devrait revoir les périodes de conservation des renseignements personnels afin de déterminer si la durée est raisonnable et de veiller à ce que les calendriers soient mis à jour au besoin.

4. Chaque sous-ministre adjoint, en collaboration avec le Secteur de la gestion ministérielle, le cas échéant, devrait revoir les paramètres d'accès par défaut des documents dans le SGDDI qui contiennent des renseignements personnels. Cela devrait inclure la mise en œuvre d'activités de surveillance relatives aux droits d'accès au SGDDI et un processus de suivi et d'atténuation lorsque des droits d'accès excessifs sont accordés pour des documents contenant des renseignements personnels.

5. Chaque sous-ministre adjoint, en collaboration avec le Secteur de la gestion ministérielle, le cas échéant, devrait examiner les cas où les secteurs de programme stockent des renseignements personnels sur les lecteurs réseau ministériels dans le but de :
   a. déterminer si l'utilisation du lecteur réseau pour le stockage des renseignements personnels est appropriée;
   b. vérifier l'accès et s'assurer qu'il est limité aux seules personnes qui ont besoin d'accéder à ces renseignements;
   c. En fonction de la nature délicate des renseignements personnels, déterminer si des mesures de contrôle supplémentaires doivent être mises en œuvre (p. ex. le chiffrement de fichiers) étant donné que les administrateurs de réseau peuvent accéder aux renseignements personnels stockés sur les lecteurs réseau, y compris les administrateurs de réseau de Services partagés Canada (SPC).

Réponse de la direction

La direction accepte les recommandations de la vérification interne et travaillera en collaboration pour élaborer et mettre en œuvre des protocoles et des pratiques applicables visant à gérer efficacement et adéquatement les renseignements personnels dans le but de s'assurer que le Ministère se conforme à la *Loi sur la protection des renseignements personnels* ainsi que les politiques connexes tant du Secrétariat du Conseil du Trésor que de Sécurité publique Canada.

Les principales mesures devant être prises par la direction pour donner suite aux recommandations et aux constatations découlant de la vérification, de même que leur calendrier, se trouvent dans la section du rapport intitulée Constatations, recommandations et réactions de la direction.

Signature de la dirigeante principale de la vérification

_____

Membres de l'équipe de vérification

Rosemary Stephenson
Denis Gorman
Deborah Duhn
Avec l'aide de ressources externes

Remerciements

L'équipe de la Vérification interne tient à remercier toutes les personnes ayant apporté aide et conseils au cours de la vérification.

1. INTRODUCTION

1.1 Contexte

Les fonctionnaires de Sécurité publique Canada (« SP » ou le « Ministère ») fournissent des conseils et un soutien stratégiques au ministre de la Sécurité publique et de la Protection civile sur toute une gamme d'enjeux, y compris la sécurité nationale, les stratégies frontalières, la lutte contre la criminalité et la gestion des urgences. Le Ministère offre également un certain nombre de programmes de subventions et de contributions liées à la gestion des urgences, à la sécurité nationale et à la sécurité de la collectivité, même si ceux-ci sont généralement liés à la fourniture de ressources aux organismes gouvernementaux, à d'autres compétences ou organismes et non directement à des personnes. Le Ministère coordonne aussi les efforts déployés par les organismes du portefeuille de la sécurité publique et il fournit une orientation quant à leurs priorités stratégiques.

SP a déterminé que la gestion des renseignements personnels était un domaine qui devait faire l'objet d'une vérification en 2014-2015. La haute direction doit avoir l'assurance que le cadre de contrôle de gestion des renseignements personnels (p. ex. le cadre de gestion de la protection de la vie privée) est conçu de manière appropriée et fonctionne efficacement. Étant donné le rôle du Ministère dans la coordination des politiques et des conseils, il ne recueille pas une quantité importante de renseignements personnels directement auprès du public; ainsi, un petit nombre seulement d'activités liées à la collecte et à la gestion des renseignements personnels sur les citoyens a été cerné au cours de la vérification (voir la section 1.6 pour obtenir plus de détails sur les renseignements détenus par le Ministère). Cependant, les renseignements qu'il gère sont souvent de nature délicate. La vérification a révélé que les renseignements sur les employés représentent l'une des plus importantes catégories, sinon la plus grande, de renseignements personnels détenus par le Ministère.

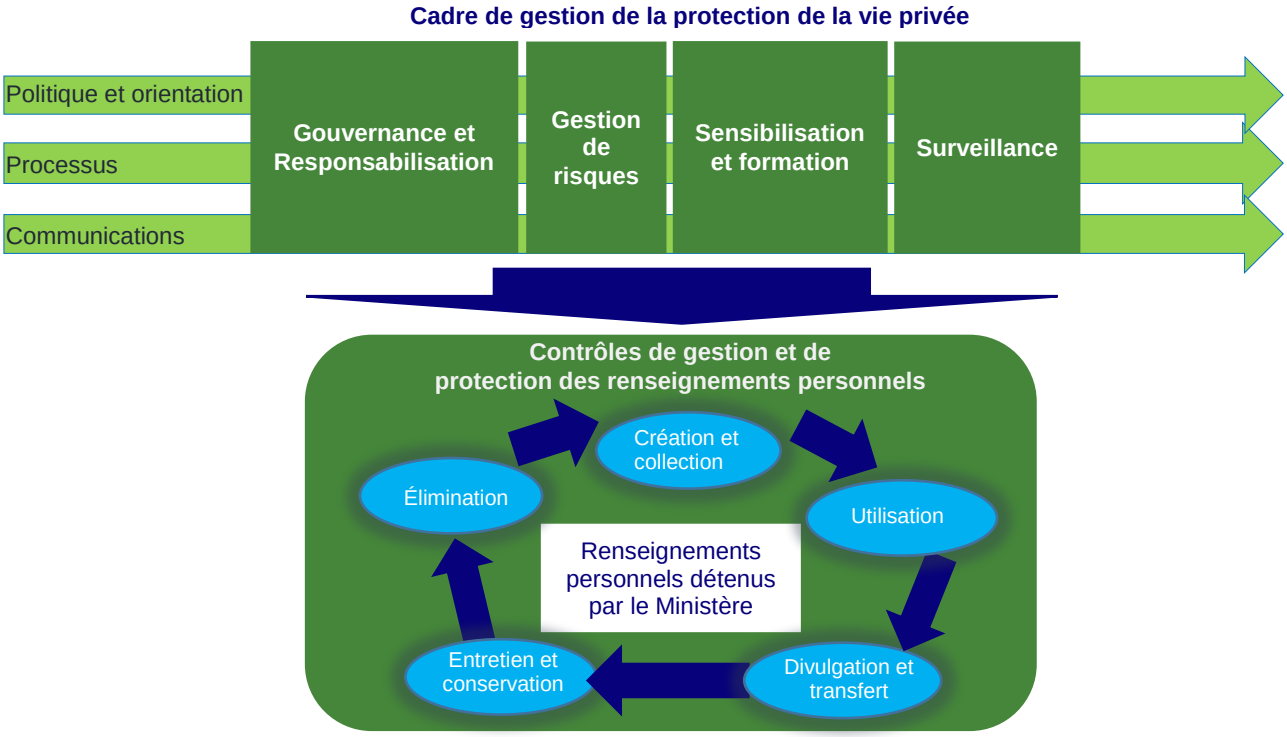
Par cadre de gestion de la protection de la vie privée (CGPVP), le commissaire à la protection de la vie privée du Canada (Commissariat) entend « *la manière dont chaque institution est organisée, à l'aide de structures, de politiques, de systèmes et de procédures, pour déléguer les responsabilités, coordonner les activités et gérer les risques relatifs à la vie privée, ainsi que pour assurer la conformité à la Loi sur la protection des renseignements personnels.* » Le CGPVP a pour but d'établir un consensus sur un ensemble de principes liés à la protection des renseignements personnels afin de guider la gestion des renseignements personnels au sein du Ministère. Le CGPVP reconnaît que des questions nouvelles ou uniques en matière de protection de la vie privée se posent régulièrement et le Ministère ne peut pas élaborer des politiques pour chaque problème potentiel à cet égard; une série massive de politiques ne serait pas non plus désirable ni viable. Ainsi, le CGPVP établit un cadre commun permettant, d'une part, de définir de meilleures pratiques de protection de la vie privée et, d'autre part, de déterminer et d'atténuer les risques potentiels à cet égard.

Bien que les éléments nécessaires pour soutenir un CGPVP puissent être classés de différentes façons, aux fins de cette vérification, ils ont été regroupés en quatre composantes principales :

- Gouvernance et responsabilisation – Définir les rôles et les responsabilités en matière de protection de la vie privée à l'échelle du Ministère

- Gestion des risques – Évaluation et gestion des risques liés à la protection de la vie privée grâce à l'élaboration et à l'actualisation de conseils appropriés ainsi que des processus de gestion des risques tels que les évaluations des facteurs relatifs à la vie privée (EFVP) et la gestion des atteintes à la vie privée
- Rayonnement et formation – S'assurer que les employés et les intervenants comprennent bien leurs droits et obligations en matière de vie privée à l'aide d'activités de formation et de sensibilisation et du maintien de bonnes relations avec les intervenants externes tels que le CPVP
- Surveillance – Mettre en œuvre des mécanismes de contrôle et de surveillance pour assurer la conformité avec les obligations du Ministère en matière de protection de la vie privée

Vous trouverez ci-dessous un exemple illustrant le cadre de gestion de la protection de la vie privée préalablement mentionné.



Une atteinte à la vie privée (que ce soit par la collecte, l'utilisation, la divulgation, la conservation ou l'élimination de renseignements personnels ou un accès non autorisé à ces renseignements) pourrait avoir de graves conséquences pour la réputation de SP ainsi que des incidences opérationnelles, comme entraver la capacité du Ministère à accéder à des données de recherche dont il a besoin. En outre, compte tenu du rôle de coordination et de soutien du Ministère dans le portefeuille de la sécurité publique, ainsi que de son rôle de sensibilisation auprès d'autres compétences et intervenants du domaine de la sécurité publique, toute atteinte à la réputation peut avoir de graves incidences sur l'ensemble du gouvernement. De plus, une atteinte à la vie privée peut entraîner l'utilisation de ressources ministérielles pour mener une enquête à cet égard et y répondre, y compris les réponses aux demandes du CPVP ou ses activités de vérification.

1.2 Cadre législatif

SP est assujetti à la *Loi sur la protection des renseignements personnels* et doit se conformer à ses exigences relatives à la gestion et à la protection des renseignements personnels. En vertu de la *Loi sur la protection des renseignements personnels*, « renseignements personnels » s'entend au sens large des « *renseignements, quels que soient leur forme et leur support, concernant un individu identifiable* ». La *Loi sur la protection des renseignements personnels* protège la vie privée de tous les citoyens canadiens et des résidents permanents contre l'utilisation ou la divulgation non autorisée des renseignements personnels dont dispose une institution gouvernementale. La *Loi sur la protection des renseignements personnels* confère aux citoyens le droit d'accéder aux renseignements détenus par le gouvernement. Le Secrétariat du Conseil du Trésor (SCT) a également mis en œuvre des politiques et des directives en matière de protection des renseignements personnels qui prévoient des exigences supplémentaires pour la collecte et la gestion des renseignements personnels, y compris la *Politique sur la protection de la vie privée*, la *Directive sur l'évaluation des facteurs relatifs à la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée*.

1.3 Rôles et responsabilités

La *Loi sur la protection des renseignements personnels* énonce plusieurs pouvoirs et fonctions qui sont attribués au chef d'une institution gouvernementale, par exemple ceux liés à la réponse aux demandes ou aux communications liées aux renseignements personnels en vertu de l'article 8(2) de la *Loi*. Conformément à la *Loi sur la protection des renseignements personnels*, « *Le responsable d'une institution fédérale peut, par arrêté, déléguer certaines de ses attributions à des cadres ou employés de l'institution.* » Même si les délégués sont tenus pour responsables des décisions qu'ils prennent, la responsabilité ultime incombe toujours au chef de l'institution fédérale. SP a établi une délégation de pouvoirs en vertu de l'article 73 de la *Loi sur la protection des renseignements personnels* décrivant les rôles et les responsabilités qui ont été délégués, entre autres, au directeur de l'accès à l'information et de la protection des renseignements personnels (AIPRP) et de la Division des services exécutifs et au gestionnaire de l'AIPRP.

Outre les tâches administratives telles qu'elles sont décrites dans la *Loi sur la protection des renseignements personnels*, la Division de l'AIPRP est responsable de s'assurer de l'établissement d'un CGPVP au sein du Ministère. Parmi les instruments nécessaires devant être mis en œuvre par la Division de l'AIPRP pour soutenir les composantes du CGPVP mentionnées ci-dessus, mentionnons les politiques, les directives, les processus tels que les EFVP et la gestion des atteintes à la vie privée ainsi que les communications au personnel et à d'autres intervenants internes et externes. Bon nombre des composantes liées aux politiques, aux processus et aux communications sont également exigées par le SCT, comme le stipulent la *Politique sur la protection de la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée.*

La Division de l'AIPRP, situé au sein du Secteur des affaires du Portefeuille et des communications, est composée de dix membres du personnel dont le gestionnaire de l'AIPRP,

deux conseillers principaux, cinq analystes, un analyste subalterne et un agent administratif. Deux postes ont été récemment pourvus (en septembre 2014) au sein de la Division de l'AIPRP pour former l'Unité des politiques, de la protection des renseignements et de la formation.

En 2013-2014, la Division de l'AIPRP a reçu environ 465 demandes d'accès à l'information et 68 demandes de communication de renseignements personnels. Outre le fait de répondre aux demandes formulées en vertu de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*, la Division de l'AIPRP fournit les services suivants au Ministère, comme indiqué dans le *Rapport annuel au Parlement sur l'administration de la Loi sur la protection des renseignements personnels 2013-2014* :

- traiter les consultations reçues d'autres établissements;
- offrir des conseils et une orientation aux employés et aux cadres supérieurs en ce qui concerne les questions liées à l'AIPRP;
- produire les rapports annuels déposés au Parlement;
- donner des séances de sensibilisation sur l'AIPRP aux employés du Ministère;
- coordonner la mise à jour régulière des manuels d'Info Source;
- passer en revue les documents ministériels, comme les vérifications et les évaluations, avant leur divulgation proactive sur le site Web du Ministère;
- élaborer des procédures ministérielles pour le traitement des demandes liées à l'AIPRP;
- maintenir la salle de lecture du Ministère consacrée à l'AIPRP;
- participer aux tribunes réunissant les membres de la collectivité de l'AIPRP, comme les réunions et les groupes de travail de la collectivité de l'AIPRP relevant du SCT.

Les rôles, les responsabilités et les obligations liés à la protection de la vie privée définis de manière formelle, mais hors de la Division de l'AIPRP, sont moins formalisés. L'équipe de vérification a appris que cela était dû aux contraintes liées aux ressources de la Division de l'AIPRP, contraintes qui ont limité l'élaboration et la mise en œuvre de directives et de séances de formation sur la protection de la vie privée au sein du Ministère. Il convient de mentionner que même s'il incombe principalement à la Division de l'AIPRP de fournir des politiques, de la formation et des outils habilitants pour assurer la conformité avec la *Loi sur la protection des renseignements personnels*, chaque employé a l'ultime responsabilité de veiller à ce que les renseignements personnels sous sa garde ou son contrôle soient gérés conformément aux exigences de la *Loi sur la protection des renseignements personnels*.

1.4 Objectif de la vérification

La vérification visait à garantir de façon raisonnable que le cadre de contrôle de gestion des renseignements personnels du Ministère est adéquat et efficace de sorte que le Ministère se conforme à la *Loi sur la protection des renseignements personnels* et aux politiques connexes tant du Secrétariat du Conseil du Trésor (SCT) que de SP.

1.5 Portée

La portée de la vérification, qui concernait la période se terminant le 30 avril 2015, était d'examiner le cadre de responsabilisation et de politique ainsi que les procédures clés et autres mesures de contrôle qui ont été mises en place pour :

- assurer la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques connexes du SCT et de SP;
- définir et communiquer les exigences dans ce domaine;
- assurer une réponse efficace et efficiente à ces exigences;
- préserver la réputation et la crédibilité du Ministère en ce qui concerne la gestion ministérielle des renseignements personnels.

La portée de la vérification comprenait à la fois un examen du cadre de gestion de la protection de la vie privée de SP ainsi que de la façon dont ce cadre a été appliqué pour sélectionner les renseignements personnels recueillis et gérés par SP. Au cours de la phase de planification, les renseignements personnels détenus par le Ministère concernant autant les employés de SP que le grand public, à la fois en format électronique et papier, ont été déterminés. En fonction des activités de planification menées, des secteurs détenant des renseignements personnels ont été choisis aux fins d'un examen plus approfondi devant avoir lieu au cours de la phase d'exécution :

- le Secteur de la gestion des urgences et des programmes (SGUP), qui comprend la **Division des programmes** du Centre national de prévention du crime. Par l'intermédiaire de cette division, SP fournit des fonds pour l'évaluation d'initiatives menées par des tiers en vue de réduire la criminalité.
- le Secteur de la sécurité communautaire et de la réduction du crime (SSCRC) qui comprend la **Division de la recherche** de la Direction générale de la recherche, des affaires intergouvernementales et des politiques horizontales. Par l'intermédiaire de cette division, SP effectue des recherches liées à la sécurité communautaire et à la criminalité, y compris la collecte de renseignements personnels auprès d'autres compétences canadiennes qui souhaitent participer à la recherche.
- le Secteur de la sécurité communautaire et de la lutte contre le crime (SSCLCC), qui comprend la **Division des affaires correctionnelles et de la justice pénale** de la Direction générale des affaires correctionnelles et de la justice pénale (DGACJP). Par l'intermédiaire de cette division, SP reçoit des fichiers provenant des organismes du portefeuille pour lesquels SP effectue une analyse visant à fournir une recommandation au ministre de la Sécurité publique concernant des domaines tels que les demandes de transfèrement international des délinquants.
- Le Secteur de la sécurité et de la cyber sécurité nationale (SSCN), qui comprend le **Centre canadien de réponse aux incidents cybernétiques (CCRIC),** recueille des renseignements sur les menaces à la cyber sécurité; les incidents y sont regroupés et gérés.
- Le Secteur de la gestion ministérielle (SGM), qui comprend la **Direction des ressources humaines (RH)**, recueille et gère les renseignements concernant les employés.

Les renseignements personnels traités au bureau du ministre ont été exclus de la portée de la vérification.

Pour plus de détails sur les critères précis de la vérification, voir l'annexe A.

1.6 Évaluation des risques

L'évaluation des risques effectuée pendant la phase de planification de la vérification a servi de fondement à l'établissement de la portée et des critères de la vérification. Les risques potentiels ont été déterminés comme suit :

1. Il y a un risque que le niveau de participation des secteurs opérationnel et fonctionnel à l'égard de l'AIPRP soit faible dans tout le Ministère, par exemple en qui concerne la participation de l'AIPRP à l'élaboration des EFVP, des protocoles d'entente (PE) et des FRP pour assurer l'application uniforme des pratiques appropriées relatives à la protection de la vie privée et le respect de la *Loi sur la protection des renseignements personnels* et des exigences du SCT.

2. Il y a un risque que les politiques et procédures, ainsi que la formation et la sensibilisation appropriées, soit insuffisantes en ce qui a trait à la gestion des renseignements personnels, lequel pourrait mener à une gestion inadéquate ou incohérente des renseignements personnels au sein du Ministère.

3. Il y a un risque qu'un secteur de programme, pour remplir son mandat, recueille des renseignements personnels non requis provenant de l'extérieur.

4. Il y a un risque que l'accès aux renseignements personnels qui sont conservés dans des référentiels tels que le SGDDI soit excessif.

5. Il y a un risque d'utilisation ou de divulgation inappropriée de renseignements personnels liés à des fichiers reçus par SP pour effectuer des analyses dans le but de fournir une recommandation au ministre.

6. Il y a le risque que les renseignements sur les employés ne soient pas utilisés de manière appropriée, à l'interne, au Ministère.

7. Il y a le risque de ne pas disposer de normes de conservation et d'élimination bien définies concernant les renseignements personnels liés à des fichiers reçus par SP pour effectuer des analyses dans le but de fournir une recommandation au ministre ainsi que les renseignements personnels recueillis au moyen des activités de cyber sécurité.

1.7 Opinion du vérificateur

Au Ministère, des problèmes de moyenne importance se posent en ce qui concerne la pertinence et l'efficacité du cadre de contrôle de gestion des renseignements personnels et du respect de la *Loi sur la protection des renseignements personnels* et des politiques connexes du SCT et de SP. Néanmoins, des améliorations pourraient être apportées au cadre afin de mieux cerner les risques et d'assurer un suivi approprié pour prévenir et détecter les activités non conformes.

1.8 Énoncé d'assurance et de conformité

Cette vérification est conforme aux Normes relatives à la vérification interne au sein du gouvernement du Canada, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité.

Selon mon jugement professionnel en tant que dirigeant principal de la vérification, des procédures de vérification suffisantes et appropriées ont été suivies et des éléments de preuve recueillis pour confirmer l'exactitude des opinions formulées et contenues dans ce rapport. L'opinion repose sur une comparaison des conditions telles qu'elles se présentaient au moment de la vérification, avec des critères de vérification préalablement établis et approuvés par la gestion. Elle ne s'applique qu'à l'entité examinée.

2. CONSTATATIONS, RECOMMANDATIONS ET RÉACTIONS DE LA DIRECTION

Tout au long des travaux de vérification, l'équipe a relevé plusieurs exemples de méthodes utilisées pour assurer la conception adéquate et l'application efficace des mesures de contrôle. Cette initiative a permis de faire plusieurs constatations positives. Des exemples figurent ci-dessous :

- Le Ministère a affirmé qu'il avait mis en place des pratiques appropriées en matière de « gestion des incidents » en cas d'atteinte à la vie privée. Plus précisément, le Ministère a élaboré et mis en œuvre des politiques et des processus en matière de gestion des atteintes à la vie privée. La vérification a permis de confirmer que les atteintes à la vie privée portées à l'attention de la Division de l'AIPRP ont été traitées et suivies de façon appropriée.
- Une politique et des processus visant la conduite des évaluations des facteurs relatifs à la vie privée (EFVP) ont été mis en œuvre et les évaluations passées en revue dans le cadre de la vérification ont été réalisées et gérées de façon appropriée.
- Le Ministère a défini la délégation des pouvoirs relativement à la *Loi sur la protection des renseignements personnels* et les rôles et les responsabilités sont clairement définis au sein de la Division de l'AIPRP.
- Deux postes ont été récemment pourvus (en septembre 2014) au sein de la Division de l'AIPRP afin que l'on puisse se concentrer davantage à l'élaboration et à la mise en œuvre de politiques et d'activités de formation.
- Grâce à des tests par échantillonnage visant à déterminer l'accès qui ont été menés au cours de la vérification, il a été noté que l'accès aux renseignements personnels dans PeopleSoft était bien contrôlé. En outre, dans les secteurs sélectionnés pour la vérification, l'accès à des documents papier contenant des renseignements personnels était bien contrôlé.
- Les employés du Ministère à qui l'on a parlé durant la vérification ont démontré qu'ils comprenaient l'importance de protéger les renseignements personnels.

L'équipe de vérification a également noté des éléments à améliorer dans le CGPVP existant et, en particulier, en ce qui a trait aux pratiques et aux processus de gestion des secteurs individuels. Ces éléments sont expliqués en détail dans les constatations ci-dessous.

2.1 Cadre de gestion de la protection de la vie privée du Ministère

Les vérificateurs s'attendaient à ce qu'un CGPVP détaillé et efficace ait été mis en place au sein du Ministère et qu'il soit harmonisé avec les exigences de la *Loi sur la protection des renseignements personnels* de même qu'avec les exigences de la politique du SCT et de SP. Même si le CGPVP de SP évolue et continue à mûrir, des lacunes ont été observées.

Gouvernance et responsabilisation

Le Ministère a défini la délégation des pouvoirs appropriée relativement à la *Loi sur la protection des renseignements personnels.* Bien que les rôles et les responsabilités au sein de la Division de l'AIPRP aient été clairement définis et communiqués, les descriptions de travail pour certains postes dans la Division de l'AIPRP sont obsolètes et doivent être mises à jour, initiative qui devrait être traitée dans le cadre de l'Initiative de développement de la collectivité de l'AIPRP du gouvernement du Canada qui a pour but de créer des descriptions de travail génériques.

Même si les rôles et les responsabilités liés aux activités menées par la Division de l'AIPRP sont clairement établis, les rôles et les responsabilités de la Division de l'AIPRP concernant la protection des renseignements personnels par rapport à d'autres domaines fonctionnels n'étaient pas aussi clairement définis ou officiellement établis. Par conséquent, la Division de l'AIPRP n'a pas été consultée sur un certain nombre de domaines pour lesquels sa contribution aurait été appropriée. En outre, des préoccupations ont été soulevées du fait que certains programmes ou domaines fonctionnels pouvaient ne pas reconnaître la Division de l'AIPRP en tant que premier point de contact pour les questions liées à la protection de la vie privée et consulter plutôt d'autres groupes (p. ex. les services juridiques ou de sécurité) du Ministère, voire consulter directement le CPVP. Parmi les exemples où les rôles et les responsabilités exigeraient d'être davantage précisés et formalisés, citons :

- Les secteurs de programme ne semblent pas toujours être conscients de la nécessité de consulter la Division de l'AIPRP sur des questions telles que les incidences des ententes et des contrats mis en place ou en ce qui concerne les divulgations faites dans l'intérêt public (consultant souvent les services juridiques plutôt que la Division de l'AIPRP). En raison de cet état de choses, et à titre d'exemple, la Division de l'AIPRP n'a pas un point de vue ministériel quant aux protocoles d'entente conclus entre le Ministère et d'autres entités. En outre, en ce qui a trait aux protocoles d'entente en place liés à l'échange d'information, ces derniers ne sont pas élaborés de manière cohérente et aucun processus officiel n'exige la participation de la Division.
- Les secteurs de programme ne consultent pas toujours la Division de l'AIPRP concernant l'élaboration ou l'inclusion d'une certaine forme de texte sur la protection de la vie privée dans les ententes de contribution. Par exemple, le Ministère fournit du financement à des tiers lié à leurs programmes de prévention de la criminalité et aux recherches qui visent à évaluer l'efficacité de ces programmes. Le Ministère a limité la quantité de renseignements personnels reçus par l'intermédiaire de ces ententes de contribution aux renseignements provenant du sommaire des résultats (sans les renseignements personnels). Malgré cela, les ententes de contribution ne définissent pas clairement les responsabilités des bénéficiaires en ce qui a trait aux renseignements personnels, ni leur contrôle et leur garde.
- Un processus visant à traiter les atteintes à la vie privée a été mis en œuvre au Ministère et la vérification a révélé que les atteintes à la vie privée signalées à la Division de l'AIPRP ont

été gérées de manière appropriée; toutefois, les secteurs de programme peuvent ne pas toujours signaler ces atteintes à la Division de l'AIPRP, négligeant ainsi de consulter la Division afin de déterminer l'existence réelle d'une atteinte à la vie privée. Il importe de mentionner que les lignes directrices ministérielles en matière de protection de la vie privée exigent que les responsables de programme avisent l'AIPRP en cas d'atteinte à la vie privée. En outre, il n'y avait pas de processus officiel en place pour que l'information relative aux atteintes à la vie privée puisse être échangée entre l'unité des Opérations de sécurité et la Division de l'AIPRP. Les discussions menées avec l'unité des Opérations de sécurité ont permis de mettre en évidence un certain nombre d'atteintes à la vie privée qui auraient pu toucher des renseignements personnels et qui n'ont pas été signalées à la Division de l'AIPRP.

Sans une définition claire ou officielle des rôles et des responsabilités en matière de protection de la vie privée pour l'ensemble des activités du Ministère, et une plus grande précision de ce qui constitue des renseignements personnels et une atteinte à la vie privée, il y a un risque que les secteurs de programme ne comprennent pas la nécessité de consulter la Division de l'AIPRP et que des pratiques relatives à la protection de la vie privée ne soient pas mises en place. En outre, cela limite la capacité de la Division de l'AIPRP d'avoir une perspective complète sur la façon dont les renseignements personnels sont recueillis et gérés au Ministère, ce qui complique, pour la Division de l'AIPRP, la tâche de déterminer et de hiérarchiser les risques liés à la protection de la vie privée de même que les mesures requises pour leur atténuation. Par ailleurs, l'insuffisance des politiques et lignes directrices ministérielles énonçant les exigences en matière de protection de la vie privée liées aux ententes pour les ententes sur l'échange d'information augmente le risque qu'aucune forme de texte sur la protection de la vie privée ne soit incluse dans ces ententes, ou conforme à celles-ci; ainsi, les parties aux ententes pourraient ne pas bien comprendre leurs rôles et leurs responsabilités liées à la protection de la vie privée et à la sauvegarde des renseignements personnels.

Gestion des risques

Dans le cas des cinq secteurs de programme sélectionnés aux fins de la vérification, les renseignements personnels recueillis étaient gérés de manière appropriée, bien que pour deux des cinq secteurs de programme, des EFVP n'avaient pas été réalisées. Sans la conduite d'une EFVP dans les secteurs de programme qui gèrent des renseignements personnels, il y a un risque que les renseignements personnels ne soient pas gérés en conformité avec la *Loi sur la protection des renseignements personnels*. Tout au moins, les secteurs de programmes qui recueillent des renseignements personnels devraient documenter le défaut d'effectuer une EFVP et conserver une justification à cet égard.

Bien que tous les renseignements personnels importants détenus par le Ministère et cernés dans le cadre de la vérification aient été accompagnés d'une entrée correspondante dans les fichiers de renseignements personnels (FRP) dans Info Source, la vérification a révélé que certains renseignements personnels et leur usage par ces secteurs n'étaient pas décrits à l'aide d'une entrée dans les FRP, en particulier :

- les demandes d'extradition visant le retour au Canada d'un délinquant canadien qui a quitté le pays ont été envoyées par le SCC au SSCLCC aux fins d'une recommandation de l'approbation du ministre;

- les demandes de prérogative royale de clémence pour alléger la peine imposée à une personne ou la modifier ont été envoyées par la CLCC au SSCLCC.

Sans un processus officiel pour déterminer la nécessité des entrées dans le FRP, dans Info Source, ainsi que leur mise à jour, il y a un risque que tous les renseignements personnels détenus par le Ministère n'aient pas d'entrée correspondante dans le FRP, conformément aux exigences législatives.

Rayonnement et formation

La Division de l'AIPRP a fait remarquer qu'elle n'a pas été en mesure de fournir des séances de formation sur la *Loi sur la protection des renseignements personnels* et les processus du Ministère en matière de protection de la vie privée en raison de contraintes liées aux ressources. Un plan de formation provisoire a été mis au point et devrait être mis en œuvre en 2015; les objectifs de formation à court terme sont d'offrir des séances de sensibilisation à la haute direction au printemps 2015. La formation sera ensuite offerte à l'ensemble du Ministère au cours des trois prochaines années.

La vérification a permis de constater que le plan de formation provisoire de la Division de l'AIPRP peut être amélioré grâce à un meilleur ciblage de la formation envisagée à des secteurs de programme comportant des risques précis ou plus élevés et gérant des renseignements personnels afin de s'assurer que les employés qui traitent ces renseignements reçoivent une formation en matière de protection de la vie privée en temps opportun. Si une formation adéquate n'est pas offerte, les employés pourraient ne pas reconnaître les questions liées à la protection de la vie privée, ne pas comprendre la nécessité de consulter la Division de l'AIPRP pour les questions qui touchent les renseignements personnels et ne pas savoir quoi faire en cas d'atteinte à la vie privée.

Surveillance

Un processus et des mesures correspondantes n'ont pas été établis pour évaluer et mesurer l'efficacité de la mise en œuvre du CGPVP du Ministère. De plus, bien qu'il y ait eu un suivi régulier des activités liées à la protection des renseignements et aux atteintes à la vie privée, ce suivi n'a pas été officialisé. Si un suivi n'est pas effectué, le programme de protection des renseignements personnels pourrait ne pas être mis en œuvre de manière appropriée ou telle que prévue.

Recommandations

1. Le sous-ministre adjoint du Secteur des affaires du Portefeuille et des communications devrait élaborer et mettre en œuvre un plan formel, comprenant des échéanciers et des responsabilités, afin de combler les lacunes décelées dans le CGPVP du Ministère. Le plan devrait prévoir ce qui suit :
    a. Définir les rôles et les responsabilités relatifs à la protection des renseignements personnels des secteurs fonctionnels ainsi que l'intégration des considérations liées à la protection des renseignements personnels dans les processus opérationnels.

b. Établir, de façon officielle, un processus de mise à jour des entrées dans les fichiers de renseignements personnels (FRP) et examiner ces fichiers afin que tous les renseignements personnels utilisés à des fins administratives au Ministère aient une entrée correspondante dans Info Source. La Division de l'AIPRP devrait d'abord entreprendre un processus plus approfondi de mise à jour des FRP pour s'assurer que le répertoire de tous les renseignements personnels détenus par le Ministère est bien documenté. Cela devrait également tenir compte des renseignements personnels utilisés à des fins non administratives.

c. Établir des politiques et des lignes directrices ministérielles qui énoncent les exigences relatives à la protection des renseignements personnels pour l'élaboration d'ententes sur l'échange d'information et d'ententes de contribution.

d. Passer en revue et exécuter le plan de formation de manière à cibler une formation axée sur des secteurs de programme comportant des risques précis ou plus élevés et qui gèrent des renseignements personnels et mettre ce plan en œuvre en temps opportun. La Division de l'AIPRP devrait coordonner la formation prévue avec la formation de base offerte par l'École de la fonction publique du Canada. Dans le cadre de la formation, il convient de rappeler que les secteurs de programme qui gèrent des renseignements personnels devraient consulter la Division de l'AIPRP et envisager la nécessité d'effectuer une EFVP. En outre, les secteurs de programme qui font la collecte et la gestion des renseignements personnels sans avoir effectué une EFVP, selon la vérification, devraient soit effectuer une EFVP ou justifier le fait de ne pas mener une telle évaluation.

e. Établir un programme de surveillance dont les paramètres de rendement permettraient d'évaluer et de mesurer la réussite du programme de protection des renseignements personnels et de présenter régulièrement à la haute direction (p. ex. trimestriellement au comité de gestion ministériel) des données particulières sur l'état des questions clés en matière de protection des renseignements personnels.

N^{o}	**Plan d'action de gestion**	**Date de finalisation prévue Date**
1	Le sous-ministre adjoint du Secteur des affaires du Portefeuille et des communications veillera à : a. Rappeler que les violations touchant des renseignements personnels doivent être signalées au Bureau de l'AIPRP. Mettre en place un groupe de travail ministériel où la question de la protection de la vie privée peut être intégrée dans les processus opérationnels.	a. 21 décembre 2016 b. 21 décembre 2015

	b. Dans le cadre de l'AIPRP, les secteurs devront cerner tous les renseignements personnels qui se trouvent dans leur domaine de responsabilité à des fins administratives et non administratives, confirmer s'il existe un FRP correspondant, si ce FRP doit être mis à jour et, s'il n'y en a aucun, effectuer une EFVP pour déterminer si un FRP est nécessaire et veiller à ce que ces mises à jour et examens aient lieu dans le cadre de nos processus opérationnels courants. c. Élaborer des outils et des lignes directrices ministériels en matière de politique pour aider les employés à rédiger des protocoles d'entente, des ententes sur l'échange d'information ou des ententes de contribution lorsqu'il est question de renseignements personnels. d. L'AIPRP fournira des conseils et de la formation sur la façon de remplir les EFVP et de réviser le plan de formation en matière d'AIPRP pour mettre en évidence les domaines ciblés au Ministère. e. Ajouter, dans les prévisions hebdomadaires de l'AIPRP, des mesures de rendement. Établir une communauté de praticiens au chapitre de la protection de la vie privée avec les organismes du portefeuille pour discuter de domaines d'intérêt commun et mettre en commun les pratiques exemplaires.	c. 21 décembre 2016 d. 21 décembre 2015 pour les séances de formation ciblées sur les EFVP e. 31 janvier 2016 21 décembre 2015

2.2 Contrôles liés à la gestion des renseignements personnels

Les vérificateurs s'attendaient à ce que le Ministère gère les renseignements personnels qu'il détient en conformité avec la *Loi sur la protection des renseignements personnels* et les politiques de SP et du SCT applicables. Les vérificateurs s'attendaient aussi à ce que le Ministère ait recueilli, utilisé et divulgué, de manière appropriée, des renseignements personnels conformément à la *Loi sur la protection des renseignements personnels,* y compris le fait de détenir l'autorité appropriée pour la collecte de renseignements, en limitant la collecte à ce qui était nécessaire pour les fins déterminées et en s'assurant que l'utilisation et la divulgation de ces renseignements étaient compatibles avec leur collecte originale et limitées à ce qui était nécessaire.

Même si aucun problème important n'a été observé quant à la façon dont les renseignements personnels ont été recueillis, utilisés et divulgués dans les secteurs inclus dans la portée de la vérification, les processus liés à la façon dont les renseignements personnels sont gérés n'ont généralement pas été formellement documentés. Sans lignes directrices et processus documentés de manière officielle quant à la gestion des renseignements personnels, il y a un risque que les pratiques appropriées ne soient pas respectées, surtout s'il y a des changements de personnel

dans les secteurs qui gèrent les renseignements personnels. En outre, des procédures d'exploitation formelles et normalisées sont essentielles pour démontrer aux intervenants et au CPVP que des processus appropriés ont été établis et qu'ils sont en place pour soutenir le Ministère s'il se produisait une atteinte à la vie privée. Parmi les observations particulières liées aux pratiques informelles cernées lors de la vérification, notons les suivantes :

- Les Ressources humaines n'ont pas officiellement documenté leurs pratiques utilisées pour répondre aux demandes de rapports et générer ces rapports, y compris le fait de mentionner quelles personnes devraient avoir accès à ces rapports et les étapes et les facteurs qui devraient être pris en compte pour s'assurer des limites de l'utilisation des renseignements personnels.
- Le SSCLCC n'a pas officiellement documenté ses processus au moyen de lignes directrices ou de procédures normalisées d'opérations pour la gestion des renseignements personnels provenant d'organismes du portefeuille pour l'analyse et la formulation de recommandations au ministre (p. ex. la *Loi sur le transfèrement international des délinquants* [LTID[1]] et les divulgations de casier judiciaire).

La Division de la recherche au sein du SSCLCC mène des recherches relativement approfondies comportant des renseignements personnels de nature délicate. Des procédures d'opérations particulières n'ont pas été formellement établies pour les activités de recherche, bien que le personnel ait indiqué que des pratiques de pointe liées à la gestion des renseignements personnels à des fins de recherche ont été suivies de manière informelle (p. ex. la politique des trois Conseils). De plus, il a été indiqué qu'il n'existait pas de procédures ni de lignes directrices normalisées d'opérations sur la protection de la vie privée, notamment en concluant des protocoles d'entente, en recueillant des renseignements personnels et en jumelant ou reliant des renseignements personnels à des fins de recherche.

En outre, les secteurs de programme ont établi des périodes de conservation très longues ou indéfinies pour les fichiers contenant des renseignements personnels. Observations particulières résultant de cette vérification :

- Le SSCLCC conserve les fichiers liés à la LTID et aux divulgations des casiers judiciaires pendant dix ans. Cela comprend les dossiers relatifs à des demandes qui ont été retirées par le demandeur (pour lesquelles, par conséquent, aucune décision n'a été prise).
- La Division de la recherche au sein du SSCLCC n'a généralement pas établi formellement de périodes de conservation de documents ni éliminé de renseignements personnels sous sa garde, y compris de vastes fonds de renseignements personnels de nature délicate liés aux délinquants et aux casiers judiciaires ainsi qu'aux projets de recherche qui sont inactifs depuis un certain nombre d'années.
- Le CCRIC conserve les renseignements indirectement reçus par l'intermédiaire des recherches sur les incidents cybernétiques pendant dix ans, bien que les numéros d'assurance sociale (NAS) soient immédiatement supprimés et que l'information financière soit supprimée lorsqu'elle est présente.

[1] La *Loi sur le transfèrement international des délinquants* (LTID) permet aux délinquants de demander à purger une peine imposée à l'étranger dans leur pays de citoyenneté.

Le fait de conserver des renseignements personnels plus longtemps que nécessaire augmente le risque que ces renseignements soient utilisés ou divulgués indûment et peut être considéré comme une atteinte à la vie privée. En outre, le fait d'avoir des périodes de conservation plus longues que nécessaire augmente les coûts des ressources associées à la gestion de ces renseignements.

Recommandations

2. Chaque sous-ministre adjoint devrait documenter officiellement les processus pour la collecte, l'utilisation et la divulgation des renseignements personnels dans les secteurs de programme qui gèrent des renseignements personnels. Cela devrait inclure des lignes directrices claires relativement à l'utilisation des renseignements personnels afin qu'il y ait une compréhension cohérente de ce qui constitue une gestion et une protection acceptables des renseignements personnels.

3. Chaque sous-ministre adjoint, le cas échéant, devrait revoir les périodes de conservation des renseignements personnels afin de déterminer si la durée est raisonnable et de veiller à ce que les calendriers soient mis à jour au besoin.

N^{o}	**Plan d'action de gestion**	**Date de finalisation prévue Date**
2	Conformément au cadre établi par l'AIPRP, chaque sous-ministre adjoint : - élaborera et documentera des processus pour la collecte, l'utilisation et la divulgation des renseignements personnels dans les fichiers de renseignements personnels (FRP); - élaborera des lignes directrices relatives à l'utilisation des renseignements personnels.	31 mars 2017
3	Le sous-ministre adjoint de la Gestion ministérielle : - fournira des conseils sur la détermination de périodes de conservation raisonnables pour les documents contenant des renseignements personnels. Chaque sous-ministre adjoint, en collaboration avec le Secteur de la gestion ministérielle et l'AIPRP : - examinera et mettra à jour les périodes de conservation; - établira un calendrier pour les documents contenant des renseignements personnels lorsqu'aucune période de conservation n'a été établie.	31 mars 2017

2.3 Protection des renseignements personnels

Les vérificateurs s'attendaient à ce que des mesures de sécurité appropriées aient été mises en place pour s'assurer que les renseignements personnels étaient convenablement protégés et que leur accès était limité. En se fondant sur le travail de vérification effectué, on constate que les principaux référentiels de fichiers contenant des renseignements personnels au sein du Ministère sont le SGDDI, PeopleSoft, le lecteur réseau et les classeurs sécurisés. Même si les classeurs sécurisés et l'accès à PeopleSoft dans les secteurs sélectionnés pour la vérification faisaient l'objet d'un contrôle efficace, la vérification a révélé des faiblesses dans les contrôles de l'accès au SGDDI et aux dossiers du réseau.

Les fichiers contenant des renseignements personnels enregistrés dans le SGDDI ne sont pas toujours sécurisés de manière appropriée dans l'ensemble du Ministère. En menant des tests par échantillonnage au cours de la vérification, on a observé que 10 des 25 documents examinés contenant des renseignements personnels présents dans le SGDDI avaient des autorisations d'accès excessives. À titre d'exemple d'accès excessif, mentionnons le fait que des personnes n'appartenant plus à une équipe avaient toujours accès aux documents et que l'accès était indûment fourni à tous les utilisateurs du SGDDI dans le cas de certains renseignements. Par conséquent, l'accès aux documents est souvent accordé aux membres des équipes à titre individuel plutôt qu'à des groupes d'utilisateurs, ce qui augmente la probabilité d'un accès excessif aux documents du fait que lorsque les employés quittent leur poste ou changent de poste, ils continuent souvent d'avoir accès à des dossiers chronologiques. En outre, lorsqu'on a recours à un accès pour des groupes d'utilisateurs, on peut accorder l'accès à des employés qui ne devraient pas être au courant de l'information en question.

De plus, la surveillance exercée par la Direction de la gestion de l'information a permis de constater que l'accès à environ 10 000 fichiers dans le SGDDI classés comme Protégé A ou plus n'était pas restreint. Bien que le nombre ait diminué dans tous les secteurs au cours de la dernière année, il n'y a pas eu de suivi officiel concernant ces documents puisque la Direction avait surtout veillé à ce que les documents classifiés soient sauvegardés de manière appropriée dans la version classifiée du SGDDI plutôt que dans la version non classifiée.

La vérification a révélé que, dans la Division de la recherche de SSCRC, un fort volume de renseignements personnels de nature délicate était stocké sur les lecteurs réseau. Les tests ont indiqué que l'accès était excessif car un certain nombre de personnes au sein de SP avait accès à un dossier où était stockée de l'information découlant des recherches sans avoir besoin de connaître cette information. En outre, un certain nombre d'employés de Services partagés Canada (SPC) avaient accès au dossier compte tenu de leur rôle d'administrateur de systèmes; les dossiers n'étaient pas protégés par des restrictions supplémentaires telles qu'un mot de passe ou des données chiffrées. En raison de l'accès excessif, des personnes ont accès à des renseignements personnels qui ne sont pas requis dans le cadre de leurs fonctions; cet état de choses augmente le risque d'atteinte à la vie privée.

Recommandations

4. Chaque sous-ministre adjoint, en collaboration avec le Secteur de la gestion ministérielle, le cas échéant, devrait revoir les paramètres d'accès par défaut des documents dans le SGDDI

qui contiennent des renseignements personnels. Cela devrait inclure la mise en œuvre d'activités de surveillance relatives aux droits d'accès au SGDDI et un processus de suivi et d'atténuation lorsque des droits d'accès excessifs sont accordés pour des documents contenant des renseignements personnels.

5. Chaque sous-ministre adjoint, en collaboration avec le Secteur de la gestion ministérielle, le cas échéant, devrait examiner les cas où les secteurs de programme stockent des renseignements personnels sur les lecteurs réseau ministériels dans le but de :
   a. déterminer si l'utilisation du lecteur réseau pour le stockage des renseignements personnels est appropriée;
   b. vérifier l'accès et s'assurer qu'il se limite aux seules personnes qui ont besoin d'accéder à ces renseignements;
   c. en fonction de la nature délicate des renseignements personnels, déterminer si des mesures de contrôle supplémentaires doivent être mises en œuvre (p. ex. le chiffrement de fichiers) étant donné que les administrateurs de réseau peuvent accéder aux renseignements personnels stockés sur les lecteurs réseau, y compris les administrateurs de réseau de SPC.

N^{o}	**Plan d'action de gestion**	**Date de finalisation prévue** **Date**
4	Le sous-ministre adjoint du Secteur des affaires du Portefeuille et des communications recommandera systématiquement de fonder exclusivement l'accès aux documents de nature personnelle sur le besoin de savoir. Le sous-ministre adjoint de la Gestion ministérielle : - communiquera les pratiques exemplaires en matière de contrôle de l'accès au SGDDI et fera en sorte que ces pratiques exemplaires en matière de contrôle de l'accès soient prises en compte dans la formation au SGDDI; - mettra en place un processus de suivi des documents classés au-delà de Protégé A lorsque des droits d'accès excessifs ont été accordés; - fournira des conseils sur les mesures correctives à prendre lorsqu'un accès excessif a été accordé à des documents contenant des renseignements personnels. Chaque sous-ministre adjoint, en collaboration avec le Secteur de la gestion ministérielle et l'AIPRP : - élaborera un protocole visant l'accessibilité aux renseignements personnels dans le SGDDI qui comprendra la vérification de l'utilisation des	31 mars 2017

	paramètres d’accès par défaut.	
5	Le sous-ministre adjoint de la Gestion ministérielle : - fournira des conseils sur le transfert de cette information dans le SGDD; - examinera la liste des exceptions liées au lecteur partagé dans le cas des secteurs de programme qui utilisent encore des lecteurs réseau; - élaborera des ententes de tenue de documents avec chaque secteur de programme en utilisant un lecteur partagé; - établira un processus de surveillance pour assurer l’utilisation appropriée des lecteurs partagés. Chaque sous-ministre adjoint, en collaboration avec le Secteur de la gestion ministérielle : - examinera les renseignements enregistrés sur les lecteurs réseau, le cas échéant, et déterminera s’ils doivent être maintenus sur les disques partagés; - veillera à ce que les matériaux soient correctement transférés dans le SGDDI ou dans un système pour les documents classifiés, au besoin; supprimera les fichiers hors réseau et travaillera avec la technologie de l’information pour les clore définitivement; - le cas échéant, examinera les politiques relatives au réseau pour assurer une utilisation appropriée des fichiers contenant des renseignements personnels.	31 mars 2017

ANNEXE A : CRITÈRES DE VÉRIFICATION

Critères de vérification	Sous-critères de vérification
Sécurité publique Canada a mis en place un cadre de gestion de la protection de la vie privée efficace pour la gestion des renseignements personnels qui garantit la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques connexes du SCT et de SP.	1.1 **Rôles et responsabilités –** La structure de gouvernance ainsi que les rôles et les responsabilités en matière de protection de la vie privée sont établis, clairement définis, compris et documentés. 1.2 **Politiques et procédures –** Sécurité publique dispose de politiques, de guides, de manuels, de protocoles et de processus relatifs à la gestion des renseignements personnels. 1.3 **Formation, sensibilisation et communication –** Une formation et de la sensibilisation appropriées sont fournies à l'ensemble du personnel conformément avec les responsabilités de chaque poste en matière de protection de la vie privée. 1.4 **Surveillance et production de rapports –** Des mécanismes, y compris ceux portant sur l'évaluation et l'atténuation des risques liés aux atteintes à la vie privée, sont en place pour surveiller la gestion des renseignements personnels de manière efficace et préparer des rapports à cet égard. 1.5 **Ententes sur l'échange d'information et ententes avec des tiers –** Les ententes sur l'échange d'information concernant les renseignements personnels sont bien documentées, y compris les rôles et les responsabilités liés à l'utilisation et à l'élimination des renseignements personnels.
Sécurité publique Canada gère les renseignements personnels qu'il détient en conformité avec la *Loi sur la protection des renseignements personnels* et les politiques applicables de SP et du SCT.	**2.1 Collecte –** Les renseignements personnels sont recueillis conformément aux exigences de la *Loi sur la protection des renseignements personnels,* y compris l'exigence de détenir l'autorité appropriée pour la collecte de renseignements, et la collecte se limite aux renseignements nécessaires pour des fins déterminées. **2.2 Sauvegarde –** Des mesures de sécurité appropriées sont en place pour veiller à ce que les renseignements personnels soient convenablement protégés et que leur accès soit limité. **2.3 Utilisation et divulgation –** Les renseignements personnels sont utilisés et divulgués conformément aux exigences de la *Loi sur la protection des renseignements personnels,* notamment en veillant à ce que leur utilisation et leur divulgation soient conformes avec l'intention de leur collecte

	originale et se limitent aux renseignements nécessaires. **2.4 Conservation et élimination –** Des mécanismes sont en place pour s'assurer que les renseignements personnels sont conservés et éliminés de façon adéquate et conformément aux calendriers de conservation et d'élimination approuvés.