Gouvernement du Canada
Government of Canada
Canada

Rapport final de l'examen

Examen du cadre de gestion de la protection des renseignements personnels de Travaux publics et Services gouvernementaux Canada

Travaux publics et Services gouvernementaux Canada

Bureau de la vérification et de l'évaluation

Le 31 mars 2016

Table des matières

Introduction

1. La présente mission figurait dans le Plan de vérification et d'évaluation axé sur les risques pour 2014-2018 de Travaux publics and Services gouvernementaux Canada (TPSGC).

Contexte

2. La *Loi sur le ministère des Travaux publics et des Services gouvernementaux* désigne Travaux publics et Services gouvernementaux Canada (TPSGC) comme un organisme de services communs chargé de fournir aux ministères, aux conseils et aux organismes fédéraux des services à l'appui de leurs programmes. Pour exécuter son mandat, TPSGC recueille, conserve et utilise des renseignements personnels dans l'administration de ses services et programmes.

3. La *Loi sur la protection des renseignements personnels* et le *Règlement sur la protection des renseignements personnels* constituent le cadre juridique régissant la collecte, la conservation, l'utilisation et la divulgation des renseignements personnels, et ils s'appliquent aux institutions du gouvernement fédéral. De plus, la Loi accorde aux personnes (c.-à-d. aux citoyens canadiens et aux résidents permanents) le droit d'accéder aux renseignements personnels qui les concernent et qui relèvent des institutions gouvernementales fédérales et de demander à ce que des corrections y soient apportées.

4. La *Loi sur la protection des renseignements personnels* définit les renseignements personnels comme étant « les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable». Il peut s'agir de renseignements concernant le nom, l'adresse, la race, la scolarité, l'origine nationale ou ethnique, la religion, l'âge, la situation de famille, l'historique criminel ou financier, les antécédents professionnels ou le numéro d'identification personnel (c.-à-d. numéro d'assurance sociale) d'une personne.

5. Un cadre de gestion de la protection des renseignements personnels constitue la façon dont un organisme fédéral organise ses activités au moyen de structures, de politiques, de systèmes et de procédures pour attribuer les responsabilités en matière de protection des renseignements personnels, coordonner les travaux dans le domaine, gérer les risques qui menacent ces renseignements et assurer le respect de la *Loi sur la protection des renseignements personnels*. La *Politique sur la protection de la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée* précisent les exigences que les institutions fédérales doivent respecter à l'égard des pratiques de gestion saines, y compris des politiques et des protocoles, des responsabilités claires, de la sensibilisation à la vie privée ainsi que du contrôle de la conformité et de la production de rapports. Selon la *Politique sur la protection de la vie privée*, « les responsables d'institutions fédérales sont chargés de l'application efficace, bien coordonnée et proactive de la *Loi sur la protection des renseignements personnels* et du *Règlement sur la protection des renseignements personnels* au sein de leurs institutions ».

6. À l'article 3 de la *Loi sur la protection des renseignements personnels*, le ministre est désigné comme le responsable de l'institution fédérale aux fins de l'application de la Loi. Au sein de TPSGC, le sous-ministre adjoint de la Direction générale des politiques, de la planification et des communications agit à titre de chef de la direction générale responsable de la protection des renseignements personnels. La Direction de l'accès à l'information et de la protection des renseignements personnels (DAIPRP), ci-après la « DAIPRP », au sein de Direction générale des politiques, de la planification et des communications, administre les dispositions de la *Loi sur la protection des renseignements personnels*

pour TPSGC, y compris le Bureau de la traduction et le Bureau de l'ombudsman de l'approvisionnement. La DAIPRP est chargée d'assurer le respect des politiques, des procédures et des lignes directrices, et de promouvoir la L*oi sur la protection des renseignements personnels*.

7. La Direction générale de la surveillance (DGS) et les Services juridiques jouent également des rôles dans la gestion de la protection des renseignements personnels du Ministère.

    - La DGS, par l'intermédiaire du directeur et de l'agent délégué de la sécurité ministérielle, participe avec le coordonnateur de l'accès à l'information et de la protection des renseignements personnels (AIPRP), c.-à-d. le directeur de la DAIPRP, à un processus coopératif pour garantir une divulgation, une intervention et une enquête en temps voulu à l'égard de toute infraction ou de tout manquement soupçonné ou réel à la sécurité ou de toute atteinte soupçonnée ou réelle à la vie privée qui a été signalée par des employés du Ministère et les personnes embauchées dans le cadre d'un contrat pour TPSGC.

    - Les responsabilités de l'avocat général principal comprennent: fournir des interprétations et des conseils juridiques à l'égard de la *Loi sur la protection des renseignements personnels*; informer la DAIPRP si, à son avis, la disposition d'exclusion du Cabinet s'applique dans le contexte des consultations pour des documents pouvant contenir des renseignements confidentiels du Cabinet conformément à l'article 70 de la *Loi sur la protection des renseignements personnels*; assurer la liaison entre la DAIPRP et le Bureau du contentieux du ministère de la Justice lors des procédures judiciaires.

<u>Pratiques relatives à la protection des renseignements personnels</u>

8. Alors que la DAIPRP coordonne la gestion du cadre de protection des renseignements personnels de TPSGC, les directions générales et leurs gestionnaires de programme sont responsables des contrôles en ce qui concerne la collecte, l'utilisation et la divulgation de renseignements personnels. Les directions générales doivent donc mettre en œuvre des pratiques de gestion saines relativement au traitement de ce type de renseignements. Le chapitre *Info Source*[1] 2014 de TPSGC indique que le Ministère compte 26 fichiers de renseignements personnels[2]. Les fichiers de renseignements personnels sont liés à des activités comme l'administration de la paie et des pensions, les services d'imagerie documentaire pour la Sécurité de la vieillesse et le Régime de pensions du Canada, les dépôts et les paiements du Receveur général, le Registre sur les marchandises contrôlées et les attestations de sécurité industrielle, l'inscription des fournisseurs et le Programme d'évaluation de l'intégrité, le Programme de gestion des biens saisis et le Programme des services de voyage partagés. Les propriétaires opérationnels des fichiers de renseignements personnels sont responsables du traitement approprié des renseignements personnels, ce qui comprend la collecte, l'utilisation, la divulgation, la protection, la conservation et l'élimination de ceux-ci.

9. Tous les employés ont des responsabilités en vertu de la *Loi sur la protection des renseignements personnels* pour ce qui est de la gestion et de la manipulation des renseignements personnels. La *Politique*

[1] *Info Source* est une série de publications sur les programmes d'accès à l'information et de protection des renseignements personnels du gouvernement du Canada. Son but premier est d'aider les personnes à exercer les droits qui leur sont conférés par la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*.
[2] *Info Source* : Sources de renseignements du gouvernement fédéral et sur les fonctionnaires fédéraux 2014 : http://www.tpsgc-pwgsc.gc.ca/aiprp-atip/ressources-resources/infosource2014-fra.html#a3.11

sur le programme d'accès à l'information et de protection des renseignements personnels (002) s'applique donc à tous les employés du Ministère, y compris les organismes de services spéciaux et le Bureau de l'ombudsman de l'approvisionnement. Les responsabilités des employés comprennent : recueillir, protéger, utiliser, divulguer, conserver et éliminer les renseignements personnels conformément aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*, au *Règlement sur la protection des renseignements personnels* et aux politiques et directives du Conseil du Trésor (CT) s'y rattachant; signaler rapidement toute infraction soupçonnée ou réelle à la sécurité concernant des renseignements personnels (c.-à-d. une atteinte à la vie privée) au directeur, Sécurité ministérielle; informer rapidement la DAIPRP des exigences nouvelles ou révisées pour recueillir, utiliser ou divulguer des renseignements personnels à des fins autres que celles prévues initialement; et fournir à la DAIPRP des descriptions complètes, à jour et exactes de leurs organisations, programmes et activités, ainsi que des fonds de renseignements opérationnels et personnels qu'ils détiennent, aux fins d'inclusion dans le chapitre de TPSGC d'*Info Sourc*e : *Sources de renseignements du gouvernement fédéral et sur les fonctionnaires fédéraux*.

Surveillance et établissement de rapports

10. La *Loi sur la protection des renseignements personnels* exige que les institutions fédérales préparent un rapport annuel sur l'administration de la Loi à l'intention du Parlement. En outre, les responsables des institutions gouvernementales sont tenus de définir et de décrire leurs fichiers de renseignements personnels et de les rendre publics dans *Info Source*.

11. La non-conformité à la *Politique sur la protection de la vie privée* ainsi qu'à ses directives et normes pourrait avoir des conséquences variées. Par exemple, le Secrétariat du Conseil du Trésor (SCT) du Canada exigera que les institutions gouvernementales non conformes fournissent, dans leur rapport annuel au Parlement, des renseignements supplémentaires concernant l'élaboration et la mise en œuvre de stratégies visant la conformité.

Objectif de l'examen

Objectif

12. Le présent examen visait à déterminer si TPSGC disposait d'un cadre efficace en matière de protection des renseignements personnels, qui comprenaient une structure de gouvernance; des politiques, des procédures, et de la formation; une évaluation des incidences et des risques en matière de protection des renseignements personnels; ainsi que des mécanismes d'enquête, d'établissement de rapports et de surveillance, en vue d'assurer la conformité avec les politiques du CT et du Ministère ainsi qu'avec les directives et exigences connexes prévues aux termes de la *Loi sur la protection des renseignements personnels*.

Étendue

13. L'étendue de l'étape de la planification et de l'étude préliminaire visait les responsabilités en matière de gestion de la protection des renseignements personnels de la DAIPRP (Direction générale des politiques, de la planification et des communications) et la Direction de la sécurité ministérielle (Direction générale de la surveillance), y compris la manière dont les risques associés au cadre de gestion de la protection des renseignements personnels du Ministère sont gérés.

14. L'examen du cadre de gestion de la protection des renseignements personnels de TPSGC n'a pas porté sur l'exactitude des procédures en place pour répondre aux demandes en vertu de la *Loi sur la protection des renseignements personnels*. Ces procédures sont semblables à celles utilisées pour appuyer le traitement rapide des demandes d'accès à l'information. Il a été déterminé que les résultats de l'étape de planification et de l'étude préliminaire pour ce secteur présentent un risque faible. L'examen exclut également les technologies qui appuient les programmes et les services de TPSGC, car l'infrastructure de la technologie d'information est fournie par une autre institution gouvernementale (c.-à-d. Services partagés Canada) et certains éléments de la gestion de l'information et de la technologie de l'information étaient visés par des vérifications internes et externes précédentes (par exemple (p. ex.), 2009-713 : Vérification des renseignements classifiés traités par voie électronique).

Énoncé de conformité

15. Le présent examen est conforme aux normes de vérification interne du gouvernement du Canada, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité.

16. Un examen fournit un niveau modéré d'assurance en concevant des procédures de sorte que le risque d'une conclusion inappropriée étant tirée sur la base des procédures d'examen en cours d'exécution est réduit à un niveau modéré. Ces procédures sont normalement limitées à une demande de renseignements, des procédures analytiques et des discussions. Ce risque est réduit à un niveau modéré lorsque la preuve obtenue nous permet de conclure que l'objet est plausible dans les circonstances.

Observations

17. Les observations visent à fournir, selon les renseignements recueillis pendant l'examen, une évaluation préliminaire de la situation existante par rapport à l'étendue et aux objectifs de l'examen en date du 30 septembre 2015. Ces renseignements, avec l'évaluation des risques, seront la source d'information primaire pour justifier de ne pas aller de l'avant avec une vérification exhaustive.

18. L'évaluation des risques a permis de conclure qu'une vérification exhaustive n'apporterait pas, pour le moment, de valeur ajoutée au Ministère. La directrice générale, Services ministériels et accès à l'information, a avisé le Bureau de la vérification et de l'évaluation que TPSGC a embauché une ressource externe (expert-conseil) pour obtenir des conseils sur la mise en œuvre de la nouvelle *Loi antiterroriste de 2015* (aussi connu sous le nom de projet de *Loi C-51*) et sur ses répercussions sur la protection des renseignements personnels. La directrice générale a indiqué que certaines des constatations comprises dans le présent rapport ont été portées à son attention, tout particulièrement celles liées à la gouvernance et la responsabilisation. Dans le cadre de ses observations préliminaires, l'expert-conseil a recommandé la création d'un poste de chef de la protection des renseignements personnels pour superviser l'administration de la *Loi sur la protection des renseignements personnels* à TPSGC. Le chef de la protection des renseignements personnels et un comité de gouvernance au niveau directeur général (c.-à-d. le Comité de surveillance de la protection des renseignements personnels) ont été créés pour appuyer la gestion de la protection des renseignements personnels. Les travaux réalisés à ce jour apportent ainsi une valeur ajoutée au Ministère sans qu'il soit nécessaire de réaliser une vérification exhaustive.

19. Étant donné les travaux entrepris jusqu'à présent par le Bureau de première responsabilité pour atténuer les risques à la vie privée ciblés, le Bureau de la vérification et de l'évaluation reportera la réalisation

d'une mission détaillée concernant le cadre de gestion de la protection des renseignements personnels de TPSGC. Un nombre d'observations ciblé pendant l'examen devrait retenir l'attention de la gestion. L'objectif du rapport est d'officiellement communiquer ces constatations à la haute direction afin d'améliorer le cadre actuel de gestion de la protection des renseignements personnels de TPSGC.

Gouvernance, responsabilisation, rôles et responsabilités

La Direction générale des politiques, de la planification et des communications prend des mesures pour renforcer la responsabilisation et les structures de gouvernance

20. Pour respecter les obligations établies en vertu de la *Loi sur la protection des renseignements personnels*, les responsabilités relatives au respect de la Loi doivent être bien définies et communiquées. Prévoyant les répercussions de la nouvelle *Loi antiterroriste de 2015* (aussi connu sous le nom de projet de loi *C-51*) sur la gestion et la protection des renseignements personnels, TPSGC a récemment mis en œuvre une nouvelle structure de gouvernance pour superviser l'administration de la *Loi sur la protection des renseignements personnels.*

21. Établi en juin 2015, le poste de chef de la protection des renseignements personnels est occupé par la directrice générale, Services ministériels et accès à l'information de la Direction générale des politiques, de la planification et des communications (DGPPC). Le chef de la protection des renseignements personnels est responsable de toute l'orientation stratégique globale et du respect à la *Loi sur la protection des renseignements personnels*, en plus de détenir le mandat relatif à la supervision de la protection de la vie privée pour le Ministère. chef de la protection des renseignements personnels est responsable de ce qui suit :

    - superviser et examiner les décisions concernant les ententes de partage d'information avec les autres institutions dans le cadre de *Loi sur la communication d'information ayant trait à la sécurité du Canada*, les évaluations des facteurs relatifs à la vie privée (EFVP) et la formulation de recommandations destinées au sous-ministre

    - surveiller les évaluations des menaces et des risques à la vie privée et la résolution des atteintes à la vie privée, une responsabilité partagée avec le dirigeant principal de l'information et l'agent de sécurité du Ministère

    - assurer la liaison avec le Commissariat à la protection de la vie privée au sujet de questions liées à la protection des renseignements personnels; et

    - fournir des renseignements, des séances de sensibilisation et de la formation pour la collecte, l'utilisation, la divulgation, la conservation et l'élimination des renseignements personnels; et défendre les droits liés à la protection de la vie privée auprès de la haute direction

22. TPSGC a également établi le Comité de surveillance de la protection des renseignements personnels pour appuyer le chef de la protection des renseignements personnels dans la supervision des efforts de conformité du Ministère et fournir une orientation stratégique globale en matière de protection des renseignements personnels et une approche de gestion des risques à l'échelle de l'organisation. Toutefois, les membres du Comité ne se sont pas encore réunis. Présidé par le chef de la protection des renseignements personnels, le Comité de niveau directeur général comprendra des représentants

de la Direction générale de la comptabilité, de la gestion bancaire et de la rémunération, de la Direction générale de la surveillance, de la Direction générale des approvisionnements, de la Direction générale du dirigeant principal de l'information et de la Direction générale de ressources humaines.

23. Le chef de la protection des renseignements personnels et le Comité de surveillance de la protection des renseignements personnels seront appuyés par le coordonnateur de l'AIPRP du Ministère, qui est responsable de fournir du soutien technique et stratégique au chef de la protection des renseignements personnels. Le coordonnateur de l'AIPRP et le personnel de la DAIPRP assureront également la fonction de secrétariat du Comité de surveillance de la protection des renseignements personnels. La DAIPRP est également chargée d'établir et de diriger toutes les activités du Ministère qui ont trait à la gestion du programme ministériel d'AIPRP, conformément aux instruments de délégation de TPSGC s'y rattachant et aux dispositions des lois, des règlements, des directives, des politiques et des lignes directrices.

24. Les responsabilités au titre de la *Loi sur la protection des renseignements personnels* ont également été déléguées par le biais d'une ordonnance de délégation de pouvoirs (instrument), conformément à l'article 73 de la Loi. Enfin, les rôles et les responsabilités des autres directions générales et des autres employés du Ministère en ce qui a trait à l'application de la *Loi sur la protection des renseignements personnels* sont indiqués dans la *Politique sur le programme d'accès à l'information et de protection des renseignements personnels* du Ministère (002).

25. À la suite de la réalisation de notre examen, nous avons appris que plusieurs mesures ont été prises pour faire progresser ces initiatives. Une ébauche du cadre de référence soulignant le mandat du Comité, la composition des membres, les activités ainsi que les rôles et les responsabilités a récemment été préparée. L'ébauche du cadre de référence et le plan de travail du nouveau Comité devaient être soumis à l'approbation du Comité de gestion de la direction le 8 février 2016. Le chef de la protection des renseignements personnels doit également faire rapport de ses activités aux membres du Comité de gestion de la direction une fois par an. Le premier rapport devrait être présenté au Comité de gestion de la direction dans l'exercice 2016-2017.

26. En outre, la DAIPRP étudie la possibilité de mettre en place une nouvelle structure organisationnelle qui lui permettrait de créer deux programmes liés, mais distincts (c.-à-d. le Programme d'accès à l'information et le Programme de protection des renseignements personnels). Cette nouvelle structure organisationnelle permettra d'affecter du personnel spécialisé au Programme de protection des renseignements personnels du Ministère. Les rôles et les responsabilités des employés affectés aux enjeux en matière de protection des renseignements personnels comprendront notamment: le traitement des demandes de protection des renseignements personnels; l'élaboration d'évaluations des facteurs relatifs à la vie privée; l'établissement et le maintien d'ententes de partage de renseignements; et la réalisation d'évaluations périodiques des risques relatifs à la protection des renseignements personnels.

Politiques et procédures

Les procédures et les lignes directrices visant la collecte, l'utilisation et la divulgation de renseignements personnels ne sont pas officialisées d'une manière qui permet d'assurer que les renseignements personnels sont gérés adéquatement durant leur cycle de vie

27. Les politiques, les procédures et les lignes directrices permettent aux employés de s'acquitter de façon appropriée de leurs responsabilités en matière de protection des renseignements personnels. De telles politiques et procédures doivent être mises à la disposition des employés, et structurées de manière à comprendre suffisamment de détails permettant de bien comprendre la manière dont une organisation gère la protection de la vie privée. Les organisations visées par la *Loi sur la protection des renseignements personnels* doivent établir et consigner les politiques internes concernant les obligations au titre de la Loi.

28. TPSGC a mis en place ses propres politiques pour la gestion, l'administration et l'application de la *Loi sur la protection des renseignements personnels.* La *Politique sur le programme d'accès à l'information et de protection des renseignements personnels* du Ministère présente la délégation de pouvoirs et les définitions, ainsi que les rôles et les responsabilités de tous les intervenants au sein de TPSGC. Le Ministère a également mis en œuvre une suite de politiques de gestion de l'information et de la sécurité qui comprennent des dispositions relatives à la protection de la vie privée. Cela comprend *Protection des renseignements personnels et particuliers au travail ministériel, Gestion des documents et des fonds de renseignements, Gestion des formulaires, Signalement des infractions à la sécurité et des manquements à la sécurité réels ou soupçonnés, Programme de sécurité du Ministère et Gestion de l'information*. Ces politiques sont disponibles sur le site Intranet du Ministère à titre de référence pour tous les employés.
29. Toutefois, les politiques relatives à la protection de la vie privée du Ministère ne traitent pas de certains aspects clés de la gestion des renseignements personnels, notamment la collecte, l'utilisation et la divulgation de ces derniers, y compris les exigences relatives au consentement et aux avis. De plus, TPSGC n'a pas officiellement établi des protocoles relatifs à la protection de la vie privée, notamment en ce qui a trait à la collecte, à utilisation et à divulgation des renseignements personnels à des fins non administrative (c.-à-d., utilisation des renseignements personnels à une fin qui n'est pas liée à un processus décisionnel ayant des répercussions directes sur une personne, p. ex., à des fins de recherche ou de statistique), comme l'exige la *Politique sur la protection de la vie privée* du SCT.

30. La DAIPRP a établi un certain nombre de directives et de protocoles pour remédier aux lacunes susmentionnées, notamment la *Directive sur les pratiques relatives à la protection de la vie privée, Directive visant l'usage non administratif des renseignements personnels* et le *Protocole sur les usages non administratifs des renseignements personnels*. Ces politiques et protocoles visent à s'assurer que la collecte, l'utilisation ou la divulgation de renseignements personnels respectent les dispositions de la *Loi sur la protection des renseignements personnels* ainsi que les politiques et les directives du SCT relatives à la protection de la vie privée. Les directives et le protocole connexe ne sont pas encore définitifs.

31. L'absence de principes directeurs relatifs à la collecte, à l'utilisation et à la divulgation de renseignements personnels pourrait donner lieu à des approches incohérentes quant à la gestion des renseignements personnels au sein du Ministère. Apporter des améliorations aux politiques de protection des renseignements personnels pour donner suite aux enjeux susmentionnés en matière de protection des renseignements personnels pourrait assurer une pratique plus uniforme au sein de TPSGC et une gestion adéquate des renseignements personnels.

Capacité, formation et sensibilisation

Aucune formation officielle n'est offerte aux employés pour leur transmettre les connaissances nécessaires pour respecter les obligations en matière de protection des renseignements personnels

32. Un cadre sain de gestion de la protection des renseignements personnels nécessite que tous les employés d'une organisation connaissent leurs obligations en matière de protection des renseignements personnels et qu'ils soient prêts à les respecter. Les séances de formation et d'information sont des mécanismes importants pour assurer la conformité avec la *Loi sur la protection des renseignements personnels* et la réalisation de ses objectifs. Conformément à la *Politique du CT sur la protection de la vie privée*, les administrateurs généraux et leurs délégués doivent s'assurer que tous les employés connaissent leurs obligations juridiques au titre de la *Loi sur la protection des renseignements personnels*, ainsi qu'aux politiques et aux procédures du Ministère et du CT. Actuellement, cette responsabilité incombe au coordonnateur de l'AIPRP (c.-à-d. directeur, AIPRP); elle sera transférée chef de la protection des renseignements personnels une fois le poste entièrement mis en œuvre.

33. Une formation sur la sensibilisation à la sécurité et à la protection de la vie privée est offerte dans le cadre du Programme d'accueil et d'orientation de TPSGC pour les nouveaux employés et de la formation obligatoire sur la sensibilisation à la sécurité pour tous les fonctionnaires. Le cours d'orientation en ligne (3959) du Programme d'accueil et d'orientation de TPSGC et le cours de sensibilisation à la sécurité en ligne (A230) traitent de manière limitée du traitement et de la protection des renseignements personnels. En outre, les secteurs de programme offrent aux employés ayant des responsabilités en matière de gestion de renseignements personnels des cours de formation sur la protection de la vie privée propre à leurs activités.

34. Un certain nombre d'initiatives relatives à la protection de la vie privée ont été mises en œuvre pour tenir les employés du Ministère au fait des questions relatives à la protection des renseignements personnels. Celles-ci comprennent la publication de deux séries d'articles dans le bulletin *Dans le coup* inutilités *« L'AIPRP et vous »*, entre février 2011 et mai 2012. Deux des articles décrivent certaines caractéristiques de la *Loi sur la protection des renseignements personnels* et des politiques et les directives du CT en matière de protection de la vie privée. La sensibilisation est également assurée par la Direction de la sécurité ministérielle par le biais d'articles diffusés dans le bulletin *Dans le coup*, du Réseau des agents de sécurité d'unité et de la Semaine de sensibilisation à la sécurité, qui a lieu chaque année à l'administration centrale et dans les régions.

35. Enfin, la DAIPRP a offert des séances de formation et de sensibilisation sur la *Loi sur l'accès à l'information et* la *Loi sur la protection des renseignements personnels* et les responsabilités connexes aux gestionnaires et aux employés du Ministère. Par exemple, 15 séances ont été offertes à 195 gestionnaires et employés de tous les niveaux de toutes les directions générales du Ministère pendant l'exercice 2013-2014, selon le rapport annuel concernant l'administration de la *Loi sur la protection des renseignements personnels*. Toutefois, en examinant les documents des séances, nous avons constaté que celles-ci mettaient plutôt l'accent sur le processus des demandes d'accès à l'information plutôt que sur la protection de la vie privée ainsi que sur la gestion et la protection des renseignements personnels.

36. Malgré ce qui précède, les employés interviewés au sein de la DAIPRP et de la DSM ont indiqué que TPSGC n'offrait pas assez de formation sur la protection des renseignements personnels et qu'il n'y avait pas de programme robuste de sensibilisation à cet effet. Il pourrait être possible d'améliorer le régime de formation et de sensibilisation du Ministère sur la protection de la vie privée pour aider à assurer la

conformité avec les obligations en matière de protection des renseignements personnels. Former les employés permettrait de s'assurer qu'ils disposent des connaissances et des compétences nécessaires pour gérer les renseignements personnels conformément à la *Loi sur la protection des renseignements personnels* et se conformer entièrement aux politiques et aux exigences connexes du Ministère et du gouvernement du Canada.

37. Après la réalisation de notre examen, le sous-ministre a publié un article dans le bulletin *De la part du SM et du SMD* afin de rappeler aux employés le rôle qu'ils doivent jouer dans la protection des renseignements de nature délicate dans le milieu de travail.

Gestion des risques

Les processus de gestion des risques associés à des activités ou des programmes, qu'ils soient nouveaux ou modifiés de manière importante, ne sont pas officialisés

38. La *Directive du CT sur l'évaluation des facteurs relatifs à la vie privée* (avril 2010) offre des lignes directrices aux institutions fédérales en ce qui a trait au respect de l'administration des évaluations des facteurs relatifs à la vie privée (EFVP). L'EFVP permet de bien définir, d'évaluer et de réduire au minimum les répercussions sur la vie privée avant la mise en œuvre d'une activité ou d'un programme, qu'ils soient nouveaux ou modifiés de manière importante, touchant aux renseignements personnels. Pour respecter la Directive, les ministères doivent avoir mis en place des mécanismes pour cibler et examiner les activités et les programmes, nouveaux ou modifiés de manière importante, qui ont des répercussions sur la gestion des renseignements personnels.

39. Nous avons déterminé que les processus visant à aider les gestionnaires de programme à évaluer les répercussions qu'auront des activités ou des programmes, nouveaux ou modifiés de manière importante, sur la vie privée d'une personne et sur la gestion des risques associés, n'ont pas encore été officialisés. TPSGC a établi une *Directive ministérielle sur l'évaluation des facteurs relatifs à la vie privée*, qui vise à fournir aux employés de l'orientation pour assumer leurs responsabilités juridiques et stratégiques en ce qui a trait à la vie privée pour les programmes et les activités qui nécessitent la collecte, la création, la conservation, l'utilisation ou la divulgation de renseignements personnels. Le Ministère a également établi un modèle d'évaluation du protocole relatif à la vie privée. Ce modèle vise à aider les employés à cerner tout risque potentiel en matière de protection de la vie privée associé à l'utilisation de renseignements personnels à des fins non administratives par TPSGC et à formuler des stratégies pour atténuer ces risques. Toutefois, la *Directive sur l'évaluation des facteurs relatifs à la vie privée* et le modèle d'évaluation du protocole relatif à la vie privée ne sont pas encore définitifs.

40. Bien qu'il n'y ait pas de processus officiels en place pour l'établissement et l'approbation d'EFVP, la gestion de la DAIPRP a indiqué que les évaluations des facteurs relatifs à la vie privée sont réalisées lorsque cela est jugé nécessaire. Les employés des secteurs de programme consultent habituellement les employés de la DAIPRP pour obtenir de l'aide lorsqu'ils proposent de nouvelles activités ou de nouveaux programmes, ou lorsqu'ils modifient de manière importante des activités et des programmes existants, pour déterminer si une EFVP est requise. Pendant cet exercice consultatif, la DAIPRP recommande la réalisation d'une évaluation des facteurs relatifs à la vie privée lorsque cela s'avère nécessaire. Toutefois, il y a des enjeux concernant l'application de ce processus, car il est long, fastidieux et inefficace.

41. Bien qu'une évaluation des facteurs relatifs à la vie privée puisse être effectuée lorsque cela s'avère nécessaire, il faut établir un processus officiel qui permettra des évaluations en temps plus opportun, avec des responsabilités clairement définies pour évaluer les risques potentiels relatifs à la vie privée lorsque de nouvelles activités ou de nouveaux programmes sont mis en œuvre, conformément à la *Directive sur l'évaluation des facteurs relatifs à la vie privée* du CT. Jusqu'à ce que cela soit mis en œuvre, les processus pour les EFVP peuvent varier grandement à l'échelle des directions générales, et il est possible que des risques ne soient pas cernés et atténués.

42. Après notre examen, nous avons appris que la DAIPRP participera davantage à l'établissement des évaluations des facteurs relatifs à la vie privée. Les représentants de la DAIPRP ont indiqué qu'ils assumeront la responsabilité de rédiger les EFVP en collaboration avec les employés des secteurs de programme. Ceux-ci valideront les renseignements compris dans le document provisoire avant son approbation. En outre, le Comité de surveillance de la protection des renseignements personnels (c.-à-d. le chef de la protection des renseignements personnels) prévoit établir un plan cernant les risques à la vie privée associés aux nouvelles activités et aux nouveaux programmes du Ministère. Le président du Comité (c.-à-d. le chef de la protection des renseignements personnels) a demandé aux membres de dresser une liste de toutes les initiatives et de tous les programmes qui nécessiteront une EFVP au cours du prochain exercice. La liste servira à créer un tableau principal, lequel sera la base des travaux du Comité pour cerner les risques à la vie privée associés à des activités ou à des programmes, qu'ils soient nouveaux ou modifiés de manière importante.

Il n'y a pas de processus pour gérer les renseignements personnels partagés avec des tiers

43. En vertu de la *Loi sur la protection des renseignements personnels*, les institutions qui transfèrent des renseignements personnels à des tiers ou qui en partagent à des fins de traitement demeurent responsable de ceux-ci. La Loi, ainsi que les politiques et les directives connexes du CT, exige que les ministères: établissent des ententes ou des accords concernant le partage de ce type de renseignements; définissent la mesure dans laquelle ces renseignements sont diffusés; et cernent les contrôles en place pour protéger les renseignements personnels.

44. TPSGC communique des renseignements personnels aux institutions de sécurité du gouvernement et aux organismes chargés de l'application de la loi afin d'émettre des attestations de sécurité, de mener des enquêtes sur la sécurité nationale et d'assumer d'autres fonctions d'enquête décrites à l'alinéa 8(2)(e) de la *Loi sur la protection des renseignements personnels.*

45. Nous avons trouvé peu de preuves de procédures en place pour s'assurer que les renseignements communiqués aux tiers sont protégés et traités conformément aux exigences de la *Loi sur la protection des renseignements personnels.* Les renseignements recueillis lors de l'examen des documents indiquent qu'il y a certaines ententes de partage d'information en place, mais que le Ministère ne répertorie pas celles-ci, et ne mène pas une revue périodique pour les mettre à jour. En outre, bien que des clauses relatives à la sécurité soient couramment comprises dans les contrats, il n'est pas clair si ces derniers comprennent les clauses appropriées en matière de protection des renseignements personnels.

46. En ce qui concerne les renseignements personnels partagés avec les entrepreneurs et les fournisseurs de services, le Ministère, par le biais de ses Programmes et services d'intégrité / Programme de sécurité des contrats, a établi des mécanismes pour protéger les renseignements de nature délicate et les biens du gouvernement canadien et des gouvernements étrangers confiés à des entreprises du secteur privé par

l'entremise de marchés du gouvernement. Les mécanismes comprennent : l'évaluation des risques et l'octroi des demandes d'attestation de sécurité aux entreprises à leurs employés; les inspections de sécurité des entreprises du secteur privé et leurs employés; et, la négociation et l'administration des ententes industrielles internationales bilatérales.

47. Des mécanismes servant à gérer les renseignements personnels communiqués à des tiers (p. ex., des entrepreneurs, des prestataires de services et d'autres institutions gouvernementales) pourraient aider à assurer que ces renseignements sont traités, par les tiers, conformément à de saines pratiques de protection des renseignements personnels. Le manque de contrôles sur les renseignements personnels communiqués à des tiers pourrait entraîner: des pratiques non uniformes à l'échelle du Ministère en ce qui a trait au partage des renseignements personnel; le non-respect des obligations relatives à la protection des renseignements personnels lorsque les fonctions ou les services d'une organisation sont réalisés par des tiers dans le cadre de contrat ou lorsque des renseignements personnels sont divulgués à d'autres institutions gouvernementales; et le non-respect des exigences en matière de notification et d'établissement de rapports à l'intention du Parlement et du commissaire à la protection de la vie privée.

48. Le Secrétariat du Conseil du Trésor a préparé, en collaboration avec l'Institut des services axés sur les citoyens (ISAC), le document *Ententes d'échange de renseignements personnels entre gouvernements — Lignes directrices sur les pratiques exemplaires,* qui offre des conseils utiles et des stratégies pour réduire les risques à la vie privée dans les ententes de partage de renseignements. Les lignes directrices comprennent des modèles pour aider les organisations fédérales à établir de telles ententes. Le SCT a également diffusé un autre document d'orientation qui s'applique aux contrats et aux ententes de services avec des tiers qui touchent à des renseignements personnels, intitulé *Prise en compte de la protection des renseignements personnels avant de conclure un marché.* Ces documents sont pertinents et applicables aux pratiques d'échange des renseignements personnels et pourraient être utilisés par TPSGC pour établir des contrôles sur les renseignements personnels traités par des tiers.

49. Nous n'avons pas examiné en détail les pratiques d'échange de renseignements personnels de TPSGC dans la présente étape de l'examen. D'autres directions générales et secteurs du Ministère communiquent des renseignements dans le cadre de l'administration des programmes, notamment l'administration des pensions fédérales, du régime d'avantages sociaux des employés et du programme des marchandises contrôlées. Dans ces cas-là, des renseignements personnels peuvent être communiqués à des institutions gouvernementales à des fins de vérifications de la couverture de la pension (p. ex., Emploi et Développement social Canada, Défense nationale, Gendarmerie royale du Canada) ou à des administrateurs des régimes d'assurance du secteur privé (comme la Sun Life et Great-West) aux fins de prestations. Des preuves supplémentaires seront recueillies pendant la vérification des pratiques relatives à la protection des renseignements personnels de TPSGC pour confirmer qu'il y a des mesures en place pour s'assurer que le Ministère continue de respecter ses obligations en vertu de la Loi lorsqu'il sous-traite à des tiers une fonction d'exécution de programmes ou de prestation de services.

Surveillance et établissement de rapports

Il y a des mécanismes pour signaler des atteintes à la vie privée et enquêter sur celles-ci

50. Conformément aux *Lignes directrices sur les atteintes à la vie privée* du CT, « une atteinte à la vie privée suppose la collecte, l'usage, la communication, la conservation ou le retrait inapproprié ou non autorisé de renseignements personnels. Une atteinte à la vie privée peut survenir au sein d'une institution ou à l'extérieur, et être le résultat d'erreurs de bonne foi ou d'actes malveillants commis par des employés,

des tiers, des partenaires ou des intrus. » Conformément à la *Directive sur les pratiques relatives à la vie privée* du CT, les institutions gouvernementales sont responsables de mettre en œuvre un plan afin de réagir aux atteintes à la vie privée qui pourraient survenir.

51. Conformément à la *Directive sur les pratiques relatives à la vie privée* du CT, TPSGC a établi en juin 2015 le *Protocole sur les atteintes à la vie privée*. Le Protocole vise à aider le Ministère à répondre aux incidents de consultation ou de communication inadéquate ou non autorisée de renseignements personnels d'une manière efficace et coordonnée. Le Ministère a adopté une approche collaborative, dans le cadre de laquelle des employés de la DAIPRP et de la DSM collaborent pour enquêter sur les atteintes à la vie privée. D'autres intervenants ministériels (p. ex., le Secteur des communications et la Direction de la sécurité de la technologie de l'information) pourraient y participer, au besoin. Les procédures et les outils pour répondre à une atteinte à la vie privée sont précisés dans le *Protocole sur les atteintes à la vie privée* de TPSGC. Nous avons examiné le Protocole et déterminé qu'il respecte les recommandations sur le signalement des atteintes établies par le SCT. Plus particulièrement, le Protocole définit les rôles et les responsabilités dans le cas d'une atteinte et offre de l'orientation pour assurer une résolution rapide, y compris les étapes clés suivantes : 1) détection et signalement; 2) évaluation complète; 3) avis; 4) mesures d'atténuation et correctives.

52. La Direction générale de la surveillance (c.-à-d., la Direction de la sécurité ministérielle et la Secteur de la sécurité industrielle) a également établi des procédures internes pour s'assurer qu'en cas d'incident de sécurité relatif à des renseignements personnels, les employés touchés connaissent leurs rôles et leurs responsabilités et peuvent atténuer les répercussions d'un accès non autorisé à des biens ou à renseignements personnels et protégés. Les procédures (c.-à-d., i) Procédures normalisées d'opération pour les enquêtes sur les atteintes à la vie privée; et ii) traitement des incidents de sécurité visant des renseignements personnels mal acheminés) sont fondées sur le *Protocole sur les atteintes à la vie privée* de TPSGC et contiennent des renseignements sur les mesures à prendre lorsque survient une atteinte à la vie privée et sur les façons de les prévenir.

53. La Direction de la sécurité ministérielle (DSM) établit également les indicateurs de rendement pour les enquêtes sur les cas d'atteinte à la sécurité qui pourraient entraîner des atteintes à la vie privée. Une enquête sur une atteinte à la vie privée réelle ou soupçonnée doit être terminée et close dans les 90 jours civils suivant la signalisation de l'incident à l'unité des enquêtes sur la sécurité de la DSM. L'équipe de l'examen a appris que la DSM éprouve des difficultés à enquêter sur les atteintes à la vie privée. En raison de la sensibilisation accrue des employés, le nombre de signalements d'atteintes alléguées a augmenté au cours de la dernière année. La DSM n'a pas été en mesure de respecter l'échéance de 90 jours. Toutefois, par le passé, la DSM a dépassé sa cible (85 %) avec 90 % à 95 % des enquêtes terminées dans un délai de 90 jours. Maintenant, les enquêteurs ne sont en mesure que de terminer 70 % des enquêtes dans les 90 jours suivants. Étant donné ces circonstances, la DSM a indiqué qu'à l'avenir, les atteintes feront l'objet d'une enquête au cas par cas, et la priorité sera accordée aux atteintes substantielles.

54. Bien que les atteintes à la vie privée fassent l'objet d'une enquête, il n'est pas clair si des mesures correctives sont mises en place pour réduire le risque de récurrence. Sans surveillance pour s'assurer que des mesures correctives sont mises en œuvre, il y a un risque que les atteintes se reproduisent. L'équipe de l'examen n'a pas examiné les pratiques des secteurs de programmes, et par conséquent, nous ne pouvons pas confirmer si les recommandations découlant des enquêtes sur les atteintes sont bien mises en œuvre. La vérification prévue des pratiques de protection des renseignements personnels visera les

mesures correctives mises en œuvre par les employés des secteurs de programmes à la suite d'une enquête.

55. Les statistiques fournies par l'agent de sécurité du Ministère et le coordonnateur de l'AIPRP démontrent qu'entre le 1er avril 2013 et le 30 novembre 2015, il y a eu 151 atteintes à la vie privée alléguées (soupçonnées) signalées à l'agent de sécurité du Ministère. De celles-ci, 123 ont été jugées fondées (voir le Tableau 1 pour obtenir de plus amples renseignements).

Tableau 1 : Nombre d'atteintes à la vie privée alléguées et réelles par année

Année	Alléguées	Réelles
2013-2014	**19**	**12**
2014-2015	**36**	**24**
2015-2016 *(1)*	**96**	**87**
Total	**151**	**123**

(1) Les chiffres sont fondés sur la période du 1er avril au 30 novembre 2015 (il s'agit de la période visée lorsqu'on fait référence aux statistiques sur les atteintes à la vie privée pendant l'exercice 2015-2016 dans le présent rapport)

56. Les erreurs administratives représentent 90 % de toutes les atteintes à la vie privée réelles du 1er avril 2013 au 30 novembre 2015. Les autres atteintes à la vie privée visaient les catégories perte, divulgation, protection et vol. Le Tableau 2 présente une ventilation des catégories des atteintes à la vie privée. L'annexe A définit les catégories d'atteintes.

Tableau 2 : Atteintes à la vie privée réelles par catégorie

Catégorie	2013-2014	2014-2015	2015-2016	Total	Pourcentage (%)
Accès					
Erreur administrative	10	20	81	111	90
Collecte					
Divulgation	1	1	4	6	5
Perte	1	1	1	3	2
Protection		1	1	2	2
Vol		1		1	1
Utilisation					
Autre : cyberattaques					
Total	**12**	**24**	**87**	**123**	**100**

57. Le nombre d'atteintes à la vie privée réelles par direction générale du 1er avril 2013 au 30 novembre 2015 est indiqué dans le Tableau 3. Les deux directions générales ayant le plus grand nombre d'atteintes sont la Direction générale de la comptabilité, de la gestion bancaire et de la rémunération et la Direction générale de la surveillance. Ces résultats peuvent être dus au fait que ces directions générales traitent un grand volume de renseignements personnels étant donné la nature de leurs activités et programmes.

Tableau 3 : Nombre d'atteintes à la vie privée réelles par direction générale dans la région de la capitale nationale (du 1er avril 2013 au 30 novembre 2015)

Direction générale	2013-2014	2014-2015	2015-2016	Total	Pourcentage (%)
Comptabilité, gestion bancaire et rémunération	8	20	32	**60**	**49**
Approvisionnements					
Dirigeant principal de l'information					
Surveillance	1	1	48	**50**	**41**
Finances et administration					
Ressources humaines		1	2	**3**	**3**
Services intégrés		1	1	**2**	**2**
Services juridiques					
Cité parlementaire	1			**1**	**1**
Politiques, planification et communications	1		4	**5**	**4**
Biens immobiliers					
Bureau de la traduction					
Total	**11**	**23**	**87**	**121**	**100**

Bien que Travaux publics et Services gouvernementaux Canada respecte les exigences obligatoires en matière de production de rapports du Secrétariat du Conseil du Trésor sur l'administration de la *Loi sur la protection des renseignements personnels*, le Ministère pourrait profiter d'une surveillance continue pour s'assurer que les politiques et les procédures applicables sont bien mises en œuvre et adoptées uniformément à l'échelle de l'organisation

58. La surveillance et l'établissement de rapports permettent aux organisations assujetties à la *Loi sur la protection des renseignements personnels* de déterminer si elles respectent les exigences des politiques et des directives en place pour appuyer une administration appropriée de la Loi. Elles permettent également de s'assurer que la haute direction est mise au courant régulièrement du bon fonctionnement, ou non, du cadre de gestion de la protection des renseignements personnels. Les administrateurs généraux ou leurs délégués sont chargés de surveiller la conformité à la *Politique sur la protection de la vie privée* du CT en ce qui a trait à l'administration de la *Loi sur la protection des renseignements personnels*. En outre, les ministères doivent produire, chaque année, un rapport aux termes de l'article 72 de la Loi sur la façon dont ils administrent celle-ci.

59. Conformément aux exigences de la *Politique sur la protection de la vie privée*, TPSGC prépare un rapport annuel sur l'administration de la Loi qu'il dépose au Parlement. Le plus récent rapport disponible, le *Rapport annuel 2013-2014 sur la Loi sur la protection des renseignements personnels*, fournit des renseignements sur le nombre d'atteintes substantielles à la vie privée signalées à la DAIPRP ou à la Direction de la sécurité ministérielle, les statistiques pluriannuelles, l'interprétation et l'explication des tendances sur les demandes reçues en vertu de la Loi. Le rapport souligne également les évaluations des facteurs relatifs à la vie privée effectuées et les fichiers de renseignements personnels (nouveaux ou

révisés) inscrits pendant l'exercice financier. Toutefois, le rapport ne comprend pas des renseignements sur la surveillance quotidienne, les enjeux relatifs à la vie privée identifiés au cours de l'exercice ou sur les risques associés aux activités du Ministère et sur la réponse à ces derniers.

60. Le sous-ministre adjoint de la Direction générale des politiques, de la planification et des communications (SMD de la DGPPC), l'administrateur général de la DGPPC responsable de la protection des renseignements personnels, a également eu recours aux comités de la direction (c.-à-d. le Comité de gestion de la direction, ou CGD) pour aviser la haute direction des questions de protection des renseignements personnels au sein de TPSGC. Les exposés présentés aux membres des comités traitaient des risques à la vie privée et des mesures proposées pour renforcer le cadre de gestion de la protection des renseignements personnels du Ministère.

61. Bien que l'examen des enjeux relatifs à la vie privée par les comités de la direction permette de s'assurer que les gestionnaires disposent de mécanismes pour surveiller de manière continue les préoccupations relatives à la protection des renseignements personnels, rien n'indique que les membres des comités examinent les mesures correctives ou les mesures prises pour les traiter, ou qu'ils en effectuent le suivi. Par exemple, dans l'exposé intitulé *Cadre de protection des renseignements personnels de TPSGC – zones de risques* qui a été présenté au CGD le 13 février 2013, on soulignait les risques liés à la protection des renseignements personnels du sein du Ministère et on proposait des mesures pour renforcer le cadre de gestion de la protection des renseignements personnels de l'organisation. À la suite de cet exposé, le sous-ministre a demandé que les équipes de gestion des directions générales et des régions évaluent régulièrement leurs vulnérabilités sur le plan des dossiers de nature délicate, de l'accès et de la transmission/le traitement des données, ainsi que des mesures relatives à la gestion de l'information. Lors de la présentation de l'exposé le 13 février 2013, le sous-ministre adjoint responsable de la protection des renseignements personnels a proposé, à titre de mesure pour renforcer le cadre de gestion de la protection des renseignements personnels de TPSGC, d'établir un plan d'action de la gestion et de faire le point sur sa mise en œuvre aux membres du Comité dans un délai de 12 mois. Toutefois, aucune mesure corrective n'a été adoptée comme prévu pour traiter les risques à la vie privée et les lacunes. La DAIPRP a indiqué qu'il a été décidé plus tard que les enjeux cernés dans l'exposé ne représentaient pas une préoccupation majeure pour le Ministère, et, par conséquent, un plan d'action de la gestion n'était pas requis. Toutefois, nous n'avons pas été en mesure d'obtenir toute preuve relative à cette décision.

62. Le Rapport annuel sur la *Loi sur la protection des renseignements personnels* est le seul outil officiel de suivi et de rapport utilisé pour évaluer la gestion et l'administration de la *Loi sur la protection des renseignements personnels* au sein de TPSGC et en faire état. Nous croyons qu'il est possible de renforcer les mécanismes de surveillance. À cette fin, le Ministère pourrait déterminer si ses mécanismes de surveillance existants sont appropriés étant donné la portée et la complexité de son mandat et des risques associés aux renseignements personnels administrés.

Conclusions

63. Dans l'ensemble, l'examen a permis de démontrer que, bien que certains éléments d'un cadre exhaustif de gestion de la protection des renseignements personnels sont en cours d'être mis en place, il y a encore des lacunes et des occasions d'amélioration relativement au cadre en question pour garantir le respect des politiques et des directrices connexes du Ministère et du SCT ainsi que les exigences au titre de la *Loi sur la protection des renseignements personnels*.

64. Une nouvelle structure de gouvernance, avec la nomination d'un chef de la protection des renseignements personnels et la création du Comité de surveillance de la protection des renseignements personnels, a été mise en œuvre pour fournir une approche coordonnée et uniforme à la gestion des renseignements personnels à l'échelle du Ministère. *Le Protocole sur les atteintes à la vie privée* de TPSGC a été établi pour répondre aux incidents de divulgation ou d'accès non autorisé ou inapproprié de renseignements personnels d'une manière coordonnée et efficace.

65. Toutefois, il y a des lacunes importantes qui doivent être comblées et TPSGC pourrait renforcer son cadre de gestion de la protection des renseignements personnels pour s'assurer de respecter ses obligations en vertu de la *Loi sur la protection des renseignements personnels* et conformément aux politiques du Ministère et du SCT. Ce ceci comprend:

- mettre en œuvre des procédures et des lignes directrices générales sur la collecte, l'utilisation et la divulgation de renseignements personnels pour s'assurer que ces renseignements sont gérés de manière appropriée
- améliorer les connaissances et la sensibilisation à l'égard de la protection des renseignements personnels, y compris de la formation adaptée aux rôles et aux responsabilités des employés

- officialiser les processus de gestion des risques à la vie privée pour s'assurer que les risques potentiels associés à des activités ou à des programmes, nouveaux ou modifiés de façon importante, sont ciblés, surveillés et atténués

- établir des mécanismes pour partager des renseignements personnels avec des tiers pour s'assurer de respecter les obligations au titre de la *Loi sur la protection des renseignements personnels*

- évaluer si les mécanismes de surveillance sont appropriés pour la portée et complexité du mandat du Ministère et les risques associés aux renseignements personnels administrés

66. Nous n'avons pas examiné les pratiques de protection des renseignements personnels à l'échelle du Ministère, et nous n'avons pas tenté de décrire chaque élément d'un cadre de gestion de la protection des renseignements personnels. Après la fin de notre examen, la DAIPRP nous a fourni des renseignements supplémentaires sur les mesures prises pour traiter les lacunes ciblées et améliorer le cadre de gestion de la protection des renseignements personnels, plus particulièrement en ce qui a trait à la gouvernance, à la gestion des risques à la vie privée et à la gestion des atteintes. Une vérification exhaustive aurait permis de recueillir des preuves supplémentaires pour confirmer si TPSGC dispose d'un cadre efficace de gestion de la protection des renseignements personnels pour garantir la conformité aux politiques du Ministère et du CT et aux directives connexes, ainsi qu'aux exigences au titre de la *Loi sur la protection des renseignements personnels*. Toutefois, étant donné les travaux actuels entrepris par le Bureau de première responsabilité pour atténuer les risques cernés, le Bureau de la vérification et de l'évaluation reportera cette mission. Dans le cadre de son processus annuel de planification, le Bureau de la vérification et de l'évaluation étudiera la possibilité de relancer la vérification à une date ultérieure. Le présent rapport souligne nos observations dont le Ministère devra tenir compte dans ses efforts pour mettre en place un programme de gestion de la protection des renseignements personnels efficace. Le Bureau de la vérification et de l'évaluation examinera en détail les pratiques de protection des renseignements personnels des directions générales et des secteurs de programmes pendant son examen des pratiques de protection des renseignements personnels pour confirmer que les contrôles en place permettent bien de s'assurer que les employés respectent leurs obligations au titre de la *Loi sur la protection des renseignements personnels*.

Recommandation

Il est recommandé que le sous-ministre adjoint, Direction générale des politiques, de la planification et des communications, tient compte des lacunes identifiées lors du développement de leur plan d'action pour améliorer le cadre de gestion de la protection des renseignements personnels.

Réponse de la gestion

Nous avons eu l'occasion d'examiner le rapport de la Dirigeante principale de la vérification et de l'évaluation concernant l'Examen du cadre de gestion de la protection des renseignements personnels de Travaux publics et Services gouvernementaux Canada (2014-710) et nous acceptons les conclusions et recommandations qui s'y trouvent. Le rapport nous parvient au moment opportun puisque nous sommes en train de revoir notre programme de protection de la vie privée pour assurer un meilleur soutien à la haute direction ainsi qu'une approche plus proactive de la gestion des risques associés à la protection de la vie privée au sein du Ministère. Les points saillants des mesures prises à ce jour comprennent la nomination d'une dirigeante principale de la protection des renseignements personnels, la mise en place d'une structure de gouvernance robuste, et l'actualisation du processus d'évaluation des facteurs relatifs à la vie privée. Alors que nous poursuivons nos efforts de transformation, les résultats du rapport d'examen fournissent de précieuses informations afin d'assurer que nous mettions en place un programme de protection de la vie privée robuste. Les actions prévues sont décrites dans notre plan d'action de la gestion détaillé.

Plan d'action de la gestion

Le sous-ministre adjoint, Direction générale des politiques, de la planification et des communications va :

1.1. Mettre en œuvre la structure de gouvernance pour la gestion de la protection des renseignements personnels, y compris la définition et la communication des rôles et des responsabilités en matière de gestion de la protection des renseignements personnels.

- 1.1.1. Établir une fonction de chef de la protection des renseignements personnels et un comité de surveillance de la protection des renseignements personnels.
- 1.1.2. Mener une analyse de la conjoncture de l'évaluation des facteurs relatifs à la vie privée.

1.2. Publier le protocole sur les atteintes à la vie privée sur le site intranet du Ministère et le diffuser aux employés de Travaux publics et Services gouvernementaux Canada au moyen du bulletin *Dans le coup*. La Direction de l'accès à l'information et de la protection des renseignements personnels et la Direction de la sécurité ministérielle ont déjà mis en œuvre le protocole.

Le protocole décrit les rôles et les responsabilités des intervenants ministériels en cas d'atteinte à la vie privée, et la procédure détaillée pour répondre à une atteinte à la vie privée, y compris les étapes de détection et de signalement, d'évaluation, d'avis ainsi que de mesures d'atténuation et correctives.

1.3. Soumettre la nouvelle Directive sur les pratiques relatives à la protection de la vie privée à l'unité des politiques ministérielles afin d'aller de l'avant avec le processus d'approbation en conformité avec le Cadre des instruments de politique ministérielle de TPSGC (politique ministérielle 003).

La nouvelle directive définit les rôles et les responsabilités de tous les intervenants en ce qui a trait à la gestion de la protection des renseignements personnels au sein du Ministère, y compris la réalisation d'évaluations des facteurs relatifs à la vie privée pour les activités et les programmes nouveaux ou considérablement modifiés ainsi que la surveillance des plans d'action connexes, de l'échange d'information avec des tiers, etc.

1.4. Mettre au point l'ébauche du protocole relatif à la vie privée pour les utilisations non administratives des renseignements personnels et la soumettre aux membres du comité de surveillance sur la protection des renseignements personnels pour examen et commentaires, puis au Chef de la protection des renseignements personnels pour approbation.

1.5. Préparer un plan de communication, en consultation avec le Secteur des communications, pour informer les employés de TPSGC des nouveaux instruments de politique relatifs à la protection des renseignements personnels.

1.6. Élaborer et mettre en œuvre un programme de formation sur la protection des renseignements personnels ciblé et axé sur les risques pour sensibiliser davantage les employés de TPSGC à leurs obligations en matière de protection des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels* et des politiques connexes.

1.7. Mettre à jour la liste des évaluations des facteurs relatifs à la vie privée en cours et prévues, en vue de cerner les risques liés à la protection des renseignements personnels associés aux activités et aux programmes nouveaux ou considérablement modifiés.

1.8. Déposer un rapport annuel au Comité exécutif sur l'état de la protection des renseignements personnels au sein du Ministère, et saisir les occasions d'évaluer l'efficience de notre programme, gouvernance et cadre stratégique, de même que de nos mécanismes de surveillance.

Nous utiliserons divers facteurs pour déterminer les aspects comportant un risque plus élevé, comme le nombre de fichiers de renseignements personnels et de systèmes de renseignements personnels, les atteintes à la vie privée et la fréquence de l'échange d'information.

Nous mesurerons les extrants comme le nombre de séances, le nombre d'employés ayant suivi la formation, la distribution du matériel de sensibilisation et les résultats (p. ex. diminution ou augmentation du nombre d'atteintes à la vie privée).

À propos de l'Examen

Autorité

La présente mission figurait dans le Plan de vérification et d'évaluation axé sur les risques pour 2014-2018 de Travaux publics et Services gouvernementaux (TPSGC).

Objectif

Le présent examen visait à déterminer si TPSGC disposait d'un cadre efficace en matière de protection des renseignements personnels, qui comprenaient une structure de gouvernance; des politiques, des procédures et de la formation; une évaluation des incidences et des risques en matière de protection de la vie privée; ainsi que des mécanismes d'enquête, d'établissement de rapports et de surveillance, en vue d'assurer la conformité avec les politiques du CT et du Ministère ainsi qu'avec les directives et exigences connexes prévues aux termes de la *Loi sur la protection des renseignements personnels*.

Portée et approche

L'étape de la planification et de l'étude préliminaire visait les responsabilités en matière de gestion de la protection des renseignements personnels de la DAIPRP (Direction générale des politiques, de la planification et des communications) et la Direction de la surveillance ministérielle (Direction générale de la surveillance), y compris la manière dont les risques associés au cadre de gestion de la protection des renseignements personnels du Ministère sont gérés.

L'examen du cadre de gestion de la protection des renseignements personnels de TPSGC n'a pas porté sur l'exactitude des procédures en place pour répondre aux demandes en vertu de la *Loi sur la protection des renseignements personnels*. Ces procédures sont semblables à celles utilisées pour appuyer le traitement rapide des demandes d'accès à l'information. Il a été déterminé que les résultats de l'étape d'étude préliminaire pour ce secteur présentent un risque faible. L'examen exclut également les technologies qui appuient les programmes et les services de TPSGC, car l'infrastructure de la technologie d'information est fournie par une autre institution gouvernementale (c.-à-d. Services partagés Canada) et certains éléments de la gestion de l'information et de la technologie de l'information étaient visés par des vérifications internes et externes précédentes (p. ex., 2009-713 : Vérification des renseignements classifiés traités par voie électronique).

L'examen a été réalisé conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* de l'Institut des vérificateurs internes.

L'examen a été réalisé pour mieux comprendre le domaine en examinant et en analysant les politiques, les processus et les documents des secteurs, des directions générales et du Ministère fournis par la Direction de l'accès à l'information et de la protection des renseignements personnels (DAIPRP), par la Direction de la surveillance ministérielle et par la Direction de la sécurité de la technologie de l'information de la Direction générale du dirigeant principal de l'information. Des renseignements ont également été recueillis dans le cadre d'entrevues avec des directeurs, des gestionnaires et du personnel clés au sein de la Direction générale des politiques, de la planification et des communications, de la Direction générale de la surveillance et de la Direction générale du dirigeant principal de l'information.

Critères

Les critères d'évaluation ont été élaborés après la réalisation d'une évaluation des risques, et ils sont fondés sur les exigences de la *Loi sur la protection des renseignements personnels*, de la *Politique sur la protection de la vie privée* du CT et des directives et lignes directrices connexes régissant la gestion des renseignements personnels, et la *Politique ministérielle sur le programme d'accès à l'information et de protection des renseignements personnels (PM-02).*

Les critères sont les suivants :

- TPSGC dispose d'un cadre de gestion des renseignements personnels qui comprend une structure de gouvernance, des politiques et des procédures, de même qu'un programme efficace de formation et de sensibilisation à l'appui de la gestion efficace des renseignements personnels.
- Les risques à la vie privée associés aux systèmes, programmes et activités nouveaux ou modifiés de manière importante qui nécessitent l'utilisation de renseignements personnels sont cernés et atténués.
- Des mécanismes de signalement, d'examen et de résolution des atteintes à la vie privée sont élaborés et mis en œuvre. Des procédures sont mises en place pour s'assurer que les employés et les tierces parties qui causent ces manquements sont informés des politiques et des protocoles en matière de protection des renseignements personnels et des conséquences du non-respect de ces politiques.
- Des procédures et des contrôles sont établis pour assurer le respect de la *Loi sur la protection des renseignements personnels* lors de la communication de renseignements personnels à des tiers (c.-à-d. des organisations du secteur privé, des institutions du gouvernement fédéral et d'autres organisations du secteur public).
- Des procédures sont en place pour assurer un contrôle et un signalement uniforme relativement à l'administration de la *Loi sur la protection des renseignements personnels*, y compris un processus pour donner suite aux plaintes et aux contestations liées à la protection des renseignements personnels.

Fin des travaux de l'examen

Les travaux d'examen menés aux fins de cet examen ont été pour l'essentiel terminés le 30 septembre 2015.

Équipe de l'examen

L'examen a été mené par le personnel du Bureau de la vérification et de l'évaluation, sous la supervision du directeur de la vérification interne sous la direction générale de la dirigeante principale de la vérification et de l'évaluation.

L'examen a été passé en revue par la Direction de l'examen de la qualité et des activités stratégiques du Bureau de la vérification et de l'évaluation.

Annexe A : Définition des catégories d'atteintes à la vie privée[3]

1. **(Accès) Accès inapproprié à des renseignements personnels :** Lorsqu'un employé a eu accès à des renseignements personnels conservés dans des dossiers papier ou dans un système de gestion de l'information du gouvernement.

2. **Erreur administrative :** Cette catégorie comprend des incidents mineurs et vise des erreurs découlant du traitement inapproprié de correspondance ministérielle (p. ex., courriel, courrier postal, télécopies et documents papier qui ont été transmis par inadvertance au mauvais destinataire) et les demandes téléphoniques où les mauvaises mesures ont été prises pour identifier un client. Lorsqu'un incident est classé dans cette catégorie, l'une des sous-catégories suivantes doit également être indiquée :

    a. **Autre :** Des erreurs administratives ou de traitement qui ne correspondent pas à l'une des autres sous-catégories.
    b. **Courriel :** Lorsqu'un courriel comprenant des renseignements personnels est envoyé à une personne non autorisée. Cela comprend les fonctionnaires qui reçoivent des courriels à l'intention d'un autre fonctionnaire qui a un nom très similaire.
    c. **Courrier :** Lorsque la correspondance papier est envoyée par courrier postal ou par service de messagerie à une personne non autorisée, ou reçue par une telle personne. Cela comprendra les enveloppes où des documents ont été glissés par erreur, du courrier perdu et d'autres incidents dans les cas où les dossiers sont acheminés par courrier.
    d. **En personne :** Lorsque des renseignements personnels sont remis en mains propres à une personne non autorisée pendant une interaction avec un client. Cela comprend des chèques et d'autres documents émis à la mauvaise personne.
    e. **Erreur de compte :** Lorsque l'employé d'un secteur de programme met à jour par erreur les renseignements du mauvais titulaire de compte (c.-à-d. ajouter une personne à charge à un compte, changer une adresse, etc.), mais l'erreur est découverte sans que de la correspondance (sous toute forme) ne soit établie.
    f. **Mauvaise adresse :** Comprend les incidents où une personne a déménagé, mais n'a pas mis à jour son adresse consignée par le gouvernement; ainsi, la correspondance est livrée à la mauvaise adresse.
    g. **Télécopie :** Lorsqu'une télécopie comprenant des renseignements personnels est envoyée à une personne non autorisée.
    h. **Téléphone :** Des erreurs administratives relatives à l'identification ou à la vérification inadéquate d'un client.

3. **(Collecte) Collecte inappropriée de renseignements personnels :** Lorsque le gouvernement collecte inadéquatement des renseignements personnels auprès d'une personne (p. ex., sans son consentement ou sans autorisation adéquate de procéder à la collecte).

4. **(Divulgation) Divulgation inappropriée de renseignements personnels :** Comprend les divulgations verbales ou autres (p. ex., des dossiers non expurgés de manière inappropriée relatif à un litige) de renseignements personnels à une personne qui n'est pas autorisée à les obtenir.

[3] Source : Unité d'enquête privée du Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique

5. **Perte :** Incidents visant la perte de dossiers gouvernementaux comprenant des renseignements personnels. Cela comprend la perte de documents papier et de dossiers électroniques stockés dans un appareil technologique (un téléphone cellulaire, un ordinateur, une clé bus série universel (USB) ou d'autres appareils de stockage électronique) qui n'était pas crypté (p. ex. appareil personnel) et/ou non sécurisé (p. ex., pas protégé par un mot de passe).

6. **(Protection) Protection inadéquate des renseignements personnels :** Incidents où il n'y a pas eu de divulgation ou d'échange apparent de renseignements personnels, mais dans le cadre desquels un organisme gouvernemental ne s'est pas assuré qu'il y avait en place des mesures de sécurité raisonnable pour protéger les renseignements personnels.

7. **(Vol) Bien volé, y compris des dossiers papier :** Des incidents relatifs au vol de dossiers gouvernementaux comprenant des renseignements personnels. Cela comprend le vol de documents papier et de dossiers électroniques stockés dans un appareil technologique (un téléphone cellulaire, un ordinateur, une clé USB ou d'autres appareils de stockage électronique) qui n'était pas crypté (p. ex. appareil personnel) et/ou non sécurisé (p. ex., pas protégé par un mot de passe).

8. **(Utilisation) Utilisation inappropriée de renseignements personnels :** Lorsqu'un fonctionnaire ou une organisation utilise inadéquatement des renseignements personnels ou opérationnels de nature délicate.

9. **Autre — cyberattaques :** Une cyberattaque des systèmes de données par le biais de programmes malveillants (p. ex., virus automatisé), de piratage ou d'hameçonnage qui entraîne une atteinte à la vie privée. Ces activités sont habituellement menées par des acteurs non gouvernementaux.