Commissariat
à la protection de
la vie privée du Canada

Rapport spécial au Parlement

Conclusions en vertu de la *Loi sur la protection des renseignements personnels*

Enquête sur la perte d'un disque dur à Emploi et Développement social Canada

Le 25 mars 2014

Commissariat à la protection de la privée du Canada
30, rue Victoria
Gatineau (Quebec)
K1A 1H3

IP54-56/2014F-PDF
978-0-660-21870-0

Suivez nous sur Twitter : @PriveePrivacy

Table des matières

Enquête sur la perte d'un disque dur à Emploi et Développement social Canada

Plainte déposée en vertu de la *Loi sur la protection des renseignements personnels*

Introduction

1. Le présent rapport de conclusions porte sur une plainte émanant de la commissaire contre Emploi et Développement social Canada (EDSC), anciennement Ressources humaines et Développement des compétences Canada (RHDCC), relativement à la perte d'un disque dur externe (l'« incident ») contenant les renseignements personnels de 583 000 bénéficiaires de prêts d'études canadiens et de 250 employés d'EDSC.

Contexte

2. Le 17 décembre 2012, EDSC a avisé verbalement le Commissariat de l'incident. Par la suite, le 7 janvier 2013, EDSC a envoyé un avis écrit officiel.

3. L'avis écrit d'EDSC indiquait que le disque dur externe contenait des renseignements personnels datant de 2000 à 2006 et se rapportant à des bénéficiaires de prêts d'études canadiens; dont le numéro d'assurance sociale (NAS), le prénom, le nom, la date de naissance, l'adresse domiciliaire et le numéro de téléphone. EDSC a par la suite informé le Commissariat que le disque dur externe contenait aussi des renseignements sur le solde des prêts d'études. Il contenait en outre des renseignements sur des employés provenant d'une chaîne téléphonique liée au Plan de continuité des opérations : prénom; nom; adresse personnelle; numéro de téléphone à la maison et/ou numéro de téléphone cellulaire.

4. Après avoir reçu l'avis d'EDSC, nous avons déterminé que des motifs raisonnables justifiaient une plainte émanant de la commissaire à l'égard du Ministère dans le but d'établir s'il y avait eu infraction à la *Loi sur la protection des renseignements personnels.*

5. Le Commissariat à la protection de la vie privée du Canada (le « Commissariat ») a donc entamé une plainte contre EDSC le 11 janvier 2013 en vertu du paragraphe 29(3) de la *Loi sur la protection des renseignements personnels* (la « *Loi* »).

6. L'enquête du Commissariat portait sur l'incident, et plus particulièrement sur le respect des dispositions de la *Loi* concernant le retrait, l'usage et la communication des renseignements personnels.

Méthodologie

7. Au cours de l'enquête, nous avons examiné les circonstances entourant l'incident, de même que le cadre stratégique d'EDSC, afin de déterminer le degré de conformité aux politiques fédérales s'appliquant à la protection de la vie privée, ainsi que pour déterminer si les politiques et procédures du Ministère qui étaient en place au moment de l'incident étaient suffisantes et avaient été mises en œuvre de façon efficace.

8. À cette fin, nous avons examiné les observations formulées par EDSC relativement à l'incident, et notre enquête comportait des entrevues avec des employés clés dont nous savions qu'ils avaient eu accès au disque dur externe perdu, ainsi qu'une visite de l'unité du Programme canadien de prêts aux étudiants (PCPE) et des rencontres avec des représentants du Ministère.

Résumé des faits

9. Le PCPE favorise l'accès à l'enseignement postsecondaire pour les étudiants qui démontrent un besoin financier en réduisant les obstacles monétaires et en veillant à ce que les Canadiennes et les Canadiens aient la possibilité d'acquérir les connaissances et les compétences dont ils ont besoin pour jouer un rôle actif dans l'économie et la société. Compte tenu de ces objectifs, le PCPE offre un éventail de programmes et services d'aide financière aux étudiants, notamment des prêts d'études pour les étudiants à temps plein et à temps partiel, des bourses non remboursables, et des mesures d'aide au remboursement à l'intention des emprunteurs qui éprouvent des difficultés à rembourser leurs prêts.

10. L'enquête a confirmé que, le 5 novembre 2012, un employé de l'unité du PCPE a voulu prendre un disque dur externe dans un classeur et a constaté qu'il ne s'y trouvait pas.

11. Selon les observations d'EDSC, le disque dur était conservé dans un classeur pouvant être verrouillé et qui se trouvait dans le cubicule de cet employé. Le disque dur était dans une enveloppe dissimulée sous d'autres dossiers.

12. EDSC a indiqué que le disque dur externe était un disque Seagate GoFlex de 1 téraoctet (To). Il n'était pas protégé par un mot de passe et l'information qu'il contenait n'était pas chiffrée. Le numéro de série du disque dur demeure inconnu.

13. Selon EDSC, le disque dur externe était utilisé pour stocker une copie de secours de données contenues sur le lecteur T du réseau du Ministère en prévision de leur migration prochaine vers le lecteur U. La migration des données a été exécutée par la Direction générale de l'innovation, de l'information et de la technologie (DGIIT) le 12 octobre 2012.

14. EDSC a confirmé que la DGIIT n'avait rien à voir avec la sauvegarde des données sur le disque dur puisque, techniquement parlant, cela n'était pas nécessaire en vue de la migration des données. Le PCPE s'est servi du disque dur comme mesure d'atténuation du risque en cas de perte ou de suppression des fichiers par inadvertance pendant la migration.

15. À titre d'information, EDSC a confirmé que le projet de migration des données avait été lancé en 2011 par la Division du soutien des programmes opérationnels (DSPO). La DSPO est devenue la Division de l'intégrité du programme et de la responsabilisation (IPR) à l'automne 2011. La Division de l'IPR appuie le PCPE en dirigeant les activités de planification, la production de rapports, la gestion du portefeuille, la responsabilisation, l'intégrité et la conformité du programme. Elle fournit aussi des services administratifs au PCPE, ce qui comprend la gestion des ressources humaines, des finances, de l'information, de la sécurité et des locaux.

16. Après un examen approfondi des fichiers et dossiers conservés sur le réseau du Ministère et visés par le projet de migration, EDSC a informé le Commissariat que la perte du disque dur externe avait mis en péril la confidentialité des renseignements contenus dans les fichiers de données suivants, chacun d'eux étant décrit plus en détail ci-dessous :

    - fichiers se rapportant aux sondages sur la satisfaction de la clientèle;
    - fichiers renfermant des rapports d'enquête;
    - fichiers contenant des données financières, le plan d'activités et des renseignements sur les ressources humaines du PCPE;
    - fichiers renfermant de l'information sur la planification de la continuité des opérations.

17. Malgré ce qui précède, comme le disque dur a disparu, EDSC affirme qu'il est impossible de savoir avec certitude quels renseignements avaient effectivement été sauvegardés sur ce disque.

Sondages sur la satisfaction de la clientèle

18. Le PCPE effectue chaque année un sondage pour connaître le degré de satisfaction des utilisateurs à l'égard de ses services. Le sondage s'adresse aux emprunteurs qui sont encore aux études et à ceux qui remboursent leurs prêts. Il sert aussi à mesurer la satisfaction à l'égard des services du Centre de service national de prêts aux étudiants (CSNPE), et il aide le PCPE à mieux connaître la population cliente. La Division de l'IPR réalise le sondage sur la satisfaction de la clientèle pour le compte du PCPE.

19. EDSC a indiqué que certains renseignements contenus sur le disque dur provenaient de fichiers associés aux sondages sur la satisfaction de la clientèle du PCPE effectués en 2004-2005, 2005-2006 et 2006-2007. Par la suite, EDSC a confirmé que certains des emprunteurs concernés avaient participé aux sondages réalisés au cours d'autres exercices que ceux qui avaient été indiqués initialement, c'est-à-dire jusqu'à l'année du décaissement 2012 inclusivement.

20. En plus des sept types de renseignements personnels décrits par EDSC dans l'avis envoyé au Commissariat, les fichiers concernant les sondages sur la satisfaction de la clientèle pourraient aussi avoir contenu les champs d'information suivants se rapportant aux emprunteurs :

> Numéro de certificat de prêt; numéro d'identification du prêt; catégorie de prêt (emprunteur qui est encore aux études ou qui rembourse son prêt); contact direct ou non entre l'emprunteur et le fournisseur de services; nom de l'établissement d'enseignement fréquenté par l'emprunteur; sexe; langue et état civil de l'emprunteur; province ayant accordé le prêt; type de prêt (p. ex. prêt pour études à temps partiel); années d'études; date de fin des études; taux d'intérêt du prêt; type d'intérêt du prêt; date de l'émission du prêt; date du décaissement; montant du versement du prêt fédéral; date de consolidation du prêt étudiant; emprunteur actif (emprunteur ayant envoyé un contrat de consolidation) ou passif (emprunteur n'ayant pas soumis de contrat de consolidation); type de prêt (p. ex. prêt direct pour études à temps plein, prêt direct pour études à temps partiel, prêt intégré); indicateur de défaillance (indique si l'emprunteur est défaillant); date de la défaillance; indicateur de remboursement intégral; solde impayé du prêt; numéro de télécopieur.

21. EDSC affirme que les champs d'information n'étaient pas tous remplis pour chacun des emprunteurs. Les renseignements personnels des personnes touchées se retrouvaient dans différents fichiers de données sur le disque dur, et le nombre de champs d'information variait d'un fichier à l'autre.

Rapports d'enquête

22. Nous avons confirmé que les « rapports d'enquête » décrits par EDSC, et qui faisaient partie de l'information contenue sur le disque dur, font référence aux enquêtes administratives effectuées pour déterminer l'admissibilité d'un certain nombre d'étudiants au PCPE, c'est-à-dire aux prêts, aux bourses et à l'aide au remboursement.

23. EDSC affirme que les éléments de données suivants figuraient dans une série de documents de travail qui énuméraient les personnes dont l'admissibilité était vérifiée : nom, adresse, NAS et date de naissance du client, et montant du prêt.

24. Notre examen nous a permis de confirmer que les rapports d'enquête sauvegardés sur le disque dur pourraient aussi avoir contenu les champs d'information suivants :

> Numéro du prêt d'études canadien; montant payé (y compris l'intérêt); montant du capital uniquement qui a été payé, et état (ce champ indique si le prêt a été remboursé en entier; s'il n'y a aucun mouvement sur le compte; si le dossier de prêt a été transféré aux services juridiques pour qu'une action au civil soit entreprise; si l'emprunteur a déclaré faillite ou est décédé; ou si le prêt est réglé).

25. EDSC affirme que les champs n'étaient pas tous remplis pour chacun des 583 000 emprunteurs touchés par l'incident, car ce ne sont pas tous les emprunteurs qui avaient fait l'objet d'une enquête pour déterminer leur admissibilité au Programme.

Information financière, et information liée au plan d'activité et aux RH du PCPE

26. Notre enquête a confirmé que cette information concerne les documents portant sur les activités liées aux finances et au plan de travail du PCPE qui sont entreprises tous les ans pour affecter les ressources du Programme et répartir le travail au cours d'un exercice donné. Ces fichiers ne contenaient donc aucun renseignement personnel.

Planification de la continuité des opérations et renseignements personnels des employés

27. Comme il est indiqué dans le troisième paragraphe du présent rapport, EDSC a signalé au Commissariat que le disque dur externe contenait également des renseignements sur les employés qui provenaient de la chaîne téléphonique du Plan de continuité des opérations.

28. Nous avons confirmé que la « chaîne téléphonique » sert à communiquer avec les employés dans les situations d'urgence qui les obligent à interrompre leur travail, comme la fermeture d'un édifice. La chaîne téléphonique est un document évolutif. Elle est mise à jour régulièrement pour que l'information soit exacte et pour tenir compte des changements dans le personnel.

29. EDSC a confirmé que 250 employés de la Direction générale de l'apprentissage étaient touchés par cet incident. L'information contenue dans la chaîne téléphonique comprend le prénom, le nom, l'adresse personnelle et le numéro de téléphone à la maison de l'employé et, dans certains cas, son numéro de cellulaire.

Mesures prises par EDSC à la suite de l'incident

30. Dans le cadre des observations présentées au Commissariat, EDSC a fourni un rapport détaillé sur la chronologie des mesures prises à la suite de l'incident et des précisions sur les recherches effectuées dans les locaux de l'organisation et dans l'édifice, les réunions organisées avec les employés, les communiqués adressés au personnel, les entrevues préliminaires réalisées avec l'employé qui a signalé la disparition du disque dur et avec d'autres employés dont on savait qu'ils avaient eu accès au disque dur, ainsi que les mesures prises par la DGIIT pour repérer, scanner et analyser les disques durs externes qui se trouvaient dans l'édifice et à d'autres endroits dans la région de la capitale nationale.

31. Nous attirons l'attention sur les dates suivantes mentionnées dans les observations d'EDSC :

    - Le 5 novembre 2012, le gestionnaire de l'employé a été informé de la disparition du disque dur et des recherches ont été entreprises.

- Le 22 novembre 2012, le directeur du PCPE a été informé de l'incident, et d'autres recherches ont été entreprises, y compris des communications avec l'ensemble du personnel.

- Le 26 novembre 2012, le directeur du PCPE a été informé du contenu du disque dur externe et a avisé la haute direction qu'un incident était survenu et que la confidentialité des renseignements personnels pouvait être en péril.

- Le 29 novembre 2012, le rapport d'incident relatif à la sécurité a été approuvé par le directeur du PCPE. Le bureau régional de sécurité a mené d'autres recherches dans l'aire des locaux et l'édifice et a interrogé l'employé qui avait signalé l'incident ainsi que trois anciens employés.

- Le 6 décembre 2012, après un examen approfondi des fichiers et des dossiers qui avaient été sauvegardés sur le disque dur externe, EDSC a déterminé que les renseignements personnels compromis concernaient plus de 500 000 clients.

32. Le 4 janvier 2013, l'Unité des enquêtes spéciales d'EDSC, qui relève de la Direction de l'intégrité interne et de la sécurité, a été chargée de mener une enquête interne officielle afin d'établir les circonstances entourant la perte du disque dur. L'enquête interne a donné lieu à un rapport daté du 27 février 2013 et à un addenda au rapport daté du 9 avril 2013.

33. EDSC a indiqué que, dans le cadre de l'enquête interne, des entrevues avaient été menées avec quatre employés de l'unité du PCPE qui avaient fait partie du groupe de travail créé pour le projet de migration des données. Il a été déterminé que ces employés avaient eu le disque dur en leur possession aux fins du projet de migration, ou qu'ils savaient où il était conservé.

34. De plus, les ordinateurs de ces quatre employés ont été soumis à une analyse informatico-judiciaire pour déterminer si un disque dur externe y avait été branché.

35. Des rencontres ont également eu lieu avec 15 employés travaillant dans le secteur où le disque dur avait été déclaré manquant, y compris deux employés qui travaillent actuellement dans d'autres ministères fédéraux.

36. EDSC a confirmé que le secteur du PCPE est contrôlé par un système de carte d'accès, et que les registres d'accès au secteur ont été examinés dans le cadre de son enquête.

37. Une recherche à l'échelle du Canada a également été menée sur le réseau ministériel d'EDSC pour vérifier si un disque dur externe correspondant à la marque et au modèle du disque dur disparu avait été branché sur l'un de ses ordinateurs.

38. L'enquête interne d'EDSC a permis d'établir les faits suivants :

    - La sauvegarde initiale de l'information en cause sur le disque dur externe a été effectuée en 2011 à la Division du soutien des programmes opérationnels.

- Entre janvier et août 2012, le disque dur a été utilisé de temps à autre par le groupe de travail de l'unité du PCPE pour sauvegarder l'information contenue sur le lecteur T. EDSC a établi que les membres du groupe de travail n'avaient supprimé aucun fichier sur le disque dur.

- L'analyse informatico-judiciaire a confirmé qu'un disque dur externe de la même marque et du même modèle (Seagate GoFlex) que le disque dur perdu avait été branché en juin 2012 à l'un des ordinateurs analysés. EDSC a indiqué que, selon la prépondérance des probabilités, il s'agissait probablement du disque dur externe perdu (et de son numéro de série correspondant).

- En ce qui concerne deux des ordinateurs analysés, l'analyse informatique n'a débouché sur aucune conclusion : l'ordinateur d'un employé a été remplacé en octobre 2012 et envoyé aux surplus; et une nouvelle image a été installée sur l'autre ordinateur en décembre 2012, ce qui a effacé tous les éléments de preuve pouvant indiquer qu'un disque dur y avait été branché.

- EDSC n'a trouvé aucune trace indiquant qu'un disque dur externe Seagate GoFlex avait été branché au quatrième ordinateur analysé durant l'enquête interne.

- EDSC a également confirmé que pendant certaines périodes (se mesurant en semaines) le disque dur n'était pas conservé dans un classeur verrouillé. Même lorsqu'il était rangé dans le classeur, celui-ci n'était pas toujours verrouillé et d'autres employés participant au projet de migration des données savaient où se trouvaient les clés.

- Le disque dur externe a été vu pour la dernière fois par un employé en août 2012 et, comme il a été mentionné précédemment, on s'est rendu compte qu'il avait disparu le 5 novembre 2012.

- Le registre d'accès couvrant la période allant du mois d'août 2012 au mois de novembre 2012 a révélé que plus de 200 employés avaient eu accès à la zone contrôlée du PCPE. La vérification d'EDSC a confirmé que toutes ces personnes étaient autorisées à entrer dans cette zone.

- Après avoir mené de multiples recherches dans l'édifice où se trouvent les bureaux du PCPE, EDSC n'a trouvé aucun signe d'introduction par effraction dans l'immeuble ou de tentatives de forcer la serrure du classeur dans lequel était conservé le disque dur.

- L'information contenue sur le disque dur n'était pas chiffrée et n'était pas protégée par un mot de passe.

- Les procédures décrites dans le Manuel des politiques et méthodes de sécurité d'EDSC pour le traitement de l'information contenue sur le disque dur externe (Protégé B) n'ont pas été suivies en ce qui concerne le stockage (lorsqu'un support amovible est utilisé pour stocker de l'information sensible, le support doit être conservé dans un coffre de sécurité approuvé) et le chiffrement (l'information sensible doit être chiffrée).

39. Le 11 janvier 2013, EDSC a affiché une déclaration publique sur son site Web concernant la perte du disque dur externe. Le Ministère fournissait des renseignements contextuels et une chronologie des événements liés à l'incident.

40. EDSC affirme que, pour atténuer les répercussions de la perte du disque dur sur les clients concernés, il a lancé sur son site Web une campagne d'information publique comprenant des communiqués, des annonces publiques et des renseignements spéciaux. De plus, EDSC a mis en place une ligne d'information gratuite pour permettre aux Canadiennes et aux Canadiens de vérifier s'ils sont touchés par l'incident et d'obtenir des renseignements supplémentaires. Ce service a été offert à partir du 14 janvier 2013.

41. Entre le 28 janvier 2013 et le 1er février 2013, EDSC a envoyé des lettres d'avis aux clients pour lesquels il possédait des coordonnées à jour. EDSC a informé les clients touchés des renseignements personnels dont la confidentialité était mise en péril par la perte du disque dur externe : numéro d'assurance sociale (NAS); prénom; nom; date de naissance; adresse personnelle; numéro de téléphone; solde du prêt étudiant.

42. Dans ses observations au Commissariat, EDSC affirme que, dans le but d'informer les personnes touchées aussi clairement et rapidement que possible, les fichiers et champs d'information ont été analysés et regroupés sous les sept catégories de renseignements personnels indiquées plus haut.

43. Dans les lettres d'avis envoyées aux clients touchés, EDSC offrait également une protection du crédit par le biais d'une entente avec Equifax.

44. EDSC a confirmé avoir conclu un contrat avec Equifax pour offrir aux clients touchés, avec leur consentement, des services gratuits de protection du crédit et de l'identité. Cette offre a été annoncée publiquement par EDSC le 25 janvier 2013.

45. Par la suite, soit le 7 juin 2013, EDSC a conclu un contrat avec l'agence d'évaluation du crédit TransUnion Canada pour offrir aux clients touchés par l'incident des services additionnels de protection du crédit. EDSC a fait cette offre publiquement le 28 juin 2013, en indiquant que les personnes qui avaient déjà consenti à recevoir les services d'Equifax recevraient automatiquement les services de TransUnion Canada.

46. La note demeurera au dossier de crédit de TransUnion et d'Equifax pendant six ans à moins que la personne touchée ne décide de la faire enlever. Elle indiquera aux organismes de crédit que les données peuvent avoir été compromises, et les prêteurs prendront alors des mesures supplémentaires pour vérifier l'identité de la personne avant de lui faire crédit, ou de lui ouvrir ou de lui permettre d'utiliser un compte.

47. EDSC a également confirmé que, à partir du 21 janvier 2013, une note avait été jointe au dossier de NAS des personnes touchées dans le Registre d'assurance sociale. Cette note indique que le NAS a fait l'objet d'un incident (perte). Elle précise que les agents de Service Canada doivent suivre un processus d'authentification renforcé avant d'émettre une autre carte d'assurance sociale ou de modifier des renseignements dans le dossier de NAS. Le processus d'authentification exige que l'agent pose une série de questions supplémentaires et demande une photo d'identification pour vérifier l'identité de la personne. De plus, les transactions relatives aux NAS concernés dans le Registre d'assurance sociale sont examinées régulièrement et Service Canada avisera immédiatement les personnes concernées de tout sujet de préoccupation.

48. La fonction de surveillance a débuté le 21 janvier 2013, mais EDSC a expliqué qu'il avait effectué une analyse rétroactive de toutes les transactions liées aux NAS pendant la période du 5 novembre 2012 au 18 janvier 2013 et qu'aucune anomalie n'avait été constatée. Les transactions dans le Registre d'assurance sociale qui concernent les NAS visés par l'incident continuent d'être examinées régulièrement. EDSC a indiqué que, jusqu'à maintenant, aucune anomalie n'avait été détectée.

49. EDSC a pris des dispositions pour que les NAS soient surveillés jusqu'à la fin de janvier 2015. Un indicateur continuera d'être associé aux NAS en cause et, comme il a été expliqué précédemment, les personnes qui demanderont un changement à un NAS touché par l'incident devront se soumettre à un processus d'authentification renforcé.

50. EDSC a déclaré que le disque dur n'avait pas été retrouvé et qu'on ne savait pas si sa disparition résultait d'une erreur humaine ou d'une intention malveillante. Il précise cependant que, selon les rapports analytiques d'Equifax Canada et du Registre d'assurance sociale, il est en mesure de dire qu'à la date indiquée sur le présent rapport, rien n'indique qu'un méfait lié à la perte du disque dur a été commis.

51. EDSC a transmis le dossier à la Gendarmerie royale du Canada (GRC) le 7 janvier 2013 en vue de la tenue d'une enquête. Le 8 août 2013, la GRC a déclaré publiquement qu'elle ne procéderait pas à une enquête criminelle dans cette affaire.

52. EDSC affirme que des mesures administratives appropriées ont été prises relativement à cet incident, conformément aux Lignes directrices concernant la discipline du Secrétariat du Conseil du Trésor.

Cadre de gestion des renseignements personnels d'EDSC

53. EDSC affirme que le Ministère a entrepris un examen de son cadre de gestion des renseignements personnels en 2010, ce qui a donné lieu au lancement d'une initiative pluriannuelle pour le renouvellement de la protection des renseignements personnels.

54. En 2011-2012, EDSC a procédé à un examen de ses pratiques de gestion des renseignements personnels et ses représentants ont rencontré des intervenants clés pour discuter de l'élaboration du Plan d'action pour le renouvellement de la protection des renseignements personnels. La première phase du Plan d'action a débuté en 2011-2012 et comprenait un triage des risques en matière de vie privée et la rédaction d'un code ministériel harmonisé sur la protection des renseignements personnels, qui est entré en vigueur en mars 2013.

55. En 2012-2013, quatre grandes priorités ont été définies pour la deuxième phase du Plan d'action, dont la mise en place de plans d'action en matière de protection des renseignements personnels (dirigés par les responsables de chaque programme) pour huit des programmes législatifs d'EDSC; la réorganisation du processus ministériel d'évaluation des facteurs relatifs à la vie privée (EFVP); le lancement d'une nouvelle politique du Ministère sur la gestion de la protection des renseignements personnels; la mise en œuvre d'une stratégie renouvelée de formation et de sensibilisation en matière de protection de la vie privée.

Directives et protocoles du Ministère

56. Le 14 janvier 2013, EDSC a remis de nouvelles lignes directrices sur la sécurité de la TI à tous ses employés. La Directive concernant les périphériques de stockage USB indique que seuls les périphériques USB autorisés peuvent être utilisés sur les ordinateurs du Ministère. Cela s'applique aux disques durs portables et aux clés USB.

57. Pour assurer le respect de la Directive, on a recueilli tous les périphériques USB non chiffrés afin d'en disposer de manière appropriée et un nombre limité de périphériques chiffrés (protégés par un mot de passe ou un dispositif biométrique) sont distribués aux employés qui utilisent régulièrement de l'information protégée ou classifiée dans le cadre de leur travail. EDSC a en outre indiqué qu'il scannait régulièrement son réseau ministériel pour détecter l'utilisation de périphériques USB non autorisés.

58. EDSC a également indiqué qu'une version à jour de son Guide de classification de l'information a été diffusée à nouveau le 15 janvier 2013 pour sensibiliser les employés aux exigences liées à la protection de l'information protégée et classifiée.

59. En plus de la nouvelle directive sur les périphériques USB, EDSC procède à une évaluation des risques associés aux autres appareils mobiles afin de déterminer le risque que d'autres renseignements personnels soient perdus. À cette fin, il a temporairement désactivé la fonction permettant aux employés d'écrire sur les CD, les DVD et d'autres supports optiques, à moins qu'un besoin opérationnel légitime ne soit établi et que l'approbation soit accordée.

60. EDSC a confirmé que le travail se poursuit au Ministère pour concevoir et offrir une formation intégrée améliorée au personnel. Tous les employés devront suivre une formation obligatoire sur la protection des renseignements personnels, la sécurité, la sécurité des technologies de l'information (TI), la gestion de l'information, et les valeurs et l'éthique. L'accréditation devra être renouvelée tous les deux ans.

61. Le Ministère met aussi en œuvre un plan de mobilisation visant à faire participer les employés à l'intendance de l'information. Pour appuyer ce plan, EDSC a mis en service un portail sur l'intendance de l'information en août 2013. Le site fournit aux employés de l'information sur la gestion et la protection des renseignements du Ministère et sur d'autres questions : protection de la vie privée; sécurité; sécurité des TI; gestion de l'information; valeurs et éthique.

Application

62. Pour rendre notre décision, nous avons pris en considération les articles 3, 6, 7 et 8 de la *Loi*.

63. Selon l'article 3 de la *Loi*, les renseignements personnels sont des renseignements, quels que soient leur forme et leur support, qui concernent un individu identifiable, notamment les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille; les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières; tout numéro identificateur; ses empreintes digitales, son groupe sanguin; ses opinions personnelles, etc.

64. Selon le paragraphe 6(3) de la *Loi*, une institution fédérale doit procéder au retrait des renseignements personnels qui relèvent d'elle conformément aux règlements et aux instructions ou directives applicables du ministre désigné.

65. L'article 7*a*) de la *Loi* stipule que, à défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins.

66. La *Loi* prévoit que les renseignements personnels ne peuvent être communiqués qu'avec le consentement de la personne concernée — paragraphe 8(1) — ou conformément à l'une des catégories de communication autorisée décrites au paragraphe 8(2) de la *Loi*.

Analyse

67. Les renseignements personnels contenus sur le disque dur égaré — par exemple, le nom, l'adresse, la date de naissance, le NAS — sont manifestement des renseignements personnels selon la définition indiquée à l'article 3 de la *Loi sur la protection des renseignements personnels.*

68. Après avoir analysé les politiques d'EDSC, plus précisément le Manuel des politiques et méthodes de sécurité (juin 2005), la Politique ministérielle sur la gestion de la sécurité en technologie de l'information (décembre 2010) et la Politique ministérielle sur la protection des renseignements personnels (dernière mise à jour en octobre 2009), nous sommes convaincus que ces politiques satisfont aux exigences des politiques et lignes directrices du Secrétariat du Conseil du Trésor (SCT) en la matière, notamment la Politique sur la sécurité du gouvernement, la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) et la Norme opérationnelle sur la sécurité matérielle (NOSM).

69. Nous sommes convaincus que, au moment de l'incident, EDSC avait des politiques qui satisfaisaient aux exigences du gouvernement du Canada en ce qui a trait à la protection des renseignements personnels.

70. Malgré ce qui précède, notre enquête a mis en lumière plusieurs faiblesses dans le contrôle exercé par EDSC sur les renseignements personnels contenus sur le disque dur perdu. À notre avis, le Ministère n'a pas réussi à transposer ses propres politiques en matière de protection de la vie privée et de sécurité en pratiques opérationnelles judicieuses.

71. Pour faciliter la consultation, nous avons structuré notre analyse en fonction des quatre types de mesures de contrôle qui, selon le Commissariat, fournissent une protection contre les atteintes à la sécurité des renseignements personnels – ce que nous appelons les quatre piliers d'une saine gestion de la protection des renseignements personnels.

72. Ces piliers se fondent sur la Directive sur les pratiques relatives à la protection de la vie privée et la Politique sur la sécurité du gouvernement du SCT. Il s'agit plus précisément des :

    I. contrôles physiques;
    II. contrôles techniques;
    III. contrôles administratifs;
    IV. contrôles de sécurité du personnel.

I. Contrôles physiques

73. Les contrôles de la sécurité physique sont essentiels pour garantir que l'information (y compris les renseignements personnels), les biens et les services gouvernementaux sont protégés contre toute compromission. Cela comprend la mise en œuvre de stratégies d'atténuation du risque lié à la consultation, à l'utilisation et à la communication non autorisées de renseignements personnels.

74. Notre enquête a établi que l'unité du PCPE est située dans une zone opérationnelle qui n'est accessible qu'aux employés autorisés du Ministère. L'accès à cette zone est contrôlé à l'aide d'un système de cartes électroniques, et la zone fait l'objet d'une surveillance au moyen d'un système d'alarme de sécurité en dehors des heures normales de travail. L'accès à l'édifice est surveillé par un commissionnaire, et l'accès des visiteurs est rigoureusement contrôlé (signature du registre et laissez-passer).

75. Même si la présence de mesures de sécurité de l'immeuble de base est fondamentale pour protéger les employés et les biens du gouvernement, des stratégies en matière de sécurité matérielle doivent également avoir été adoptées pour protéger l'information et se conformer aux politiques du gouvernement du Canada.

76. Conformément au Manuel des politiques et méthodes de sécurité d'EDSC et à la Norme opérationnelle sur la sécurité matérielle du gouvernement du Canada, l'information protégée, qui englobe les renseignements personnels, doit être conservée dans un coffre de sécurité approuvé (p. ex. classeur approuvé). Il faut s'assurer que les renseignements désignés et les biens précieux sont protégés convenablement lorsque les utilisateurs sont absents de leur poste de travail pour tout laps de temps. Par conséquent, les clés et les autres dispositifs de verrouillage des coffres de sécurité doivent aussi être protégés.

77. Nous soulignons que les renseignements personnels contenus sur le disque dur égaré avaient la cote de sécurité « Protégé B », selon les normes de classification du gouvernement du Canada. Le SCT indique que cette cote s'applique aux renseignements personnels, à l'information sur la vie privée et à l'information sur les entreprises de nature délicate pour lesquels toute atteinte à l'intégrité risquerait de causer un préjudice sérieux (p. ex. perte de réputation, vol d'identité, etc.).

78. Le Manuel des politiques et méthodes de sécurité d'EDSC exige que, lorsqu'un support amovible est utilisé pour conserver de l'information de nature délicate, y compris des renseignements personnels, ce support doit être conservé dans un coffre de sécurité approuvé lorsqu'il n'est pas utilisé.

79. Notre enquête a établi que le disque dur était souvent laissé sans protection pendant de longues périodes, sans être conservé dans un classeur. Même lorsqu'il était rangé dans le classeur, celui-ci n'était pas toujours verrouillé et d'autres employés savaient où se trouvaient les clés.

80. Les dispositifs portables sont des biens attrayants et des mesures doivent être mises en place pour protéger les renseignements personnels qui y sont conservés. À cet égard, nous ne sommes pas convaincus qu'EDSC avait mis en place des contrôles de sécurité physique rigoureux pour atténuer le risque de compromission du disque dur externe et des renseignements personnels qui y étaient stockés.

II. Contrôles techniques

81. Comme l'exige la Politique sur la sécurité du gouvernement (PSG), les ministères et organismes fédéraux doivent protéger l'information et les biens gouvernementaux, y compris les renseignements personnels, et ils doivent se doter d'une stratégie sur la sécurité des TI pour protéger l'information tout au long de son cycle de vie. L'expression « sécurité des TI » désigne les mesures de protection visant à préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique.

82. Le Manuel des politiques et méthodes de sécurité d'EDSC exige que des mesures soient établies pour protéger les renseignements personnels et les autres renseignements de nature délicate pendant toute la durée de leur cycle de vie. Cela comprend le traitement, la conservation, la manipulation, la communication, la transmission et la destruction de l'information sensible de manière sécuritaire, conformément aux normes de sécurité du Ministère et en fonction des conclusions d'une évaluation de la menace et des risques (EMR). Ce manuel précise en outre que les renseignements personnels ou autres renseignements sensibles doivent être répertoriés et désignés selon le niveau de sécurité le plus élevé applicable.

83. Notre enquête nous a permis de déterminer que, au moment de l'incident, les supports amovibles (p. ex. disques durs externes, clés USB, etc.) ne devaient pas faire l'objet d'une évaluation des risques en matière de sécurité. EDSC n'exigeait pas qu'une EMR ou qu'une évaluation des facteurs relatifs à la vie privée (EFVP) soit réalisée en ce qui a trait à l'utilisation de supports amovibles contenant des renseignements personnels. De plus, le disque dur externe qui a disparu n'était pas identifié comme l'exige la politique d'EDSC.

84. EDSC affirme qu'il effectue une évaluation des risques tous les ans. Cependant, comme les ressources sont limitées, la priorité a été donnée aux menaces de plus haut niveau. Les supports amovibles n'étaient pas considérés comme une menace de haut niveau. EDSC précise en outre que l'utilisation de supports amovibles avec le matériel et les logiciels des ordinateurs de bureau ou du réseau ne faisaient pas partie des systèmes examinés au moment de l'incident. Le Ministère a indiqué qu'il s'occupe maintenant de la certification et de l'accréditation graduelle de ses systèmes.

85. Le Manuel des politiques et méthodes de sécurité d'EDSC prévoit que, lorsqu'un support amovible est utilisé pour conserver de l'information de nature délicate, y compris des renseignements personnels, cette information doit être chiffrée. Par ailleurs, le bulletin de sécurité d'EDSC intitulé *Exigences en matière de chiffrement* (décembre 2008) indique que, dans la mesure du possible, la direction devrait limiter les situations où les employés doivent conserver de l'information protégée, y compris des renseignements personnels, sur des dispositifs portatifs. Lorsque cela est inévitable, il incombe à l'employé de s'assurer que l'information est chiffrée.

86. Bien qu'EDSC soutienne que les utilisateurs du disque dur externe pouvaient recourir à au moins deux procédures approuvées — 1) la fonction de protection par mot de passe; 2) l'utilisation du logiciel de chiffrement Entrust —, l'enquête a révélé qu'aucune mesure de protection technologique n'avait été prise pour protéger l'information contenue sur le disque dur dans ce cas précis.

87. Nous savons qu'EDSC a diffusé une nouvelle directive sur les dispositifs de stockage USB en janvier 2013. Cette directive interdit l'utilisation de clés USB et de disques durs non chiffrés sur les ordinateurs du Ministère. Nous encourageons EDSC à poursuivre la mise en œuvre de cette stratégie de gestion du risque, entre autres en scannant régulièrement les lecteurs réseau pour détecter les dispositifs non autorisés et en communiquant clairement la nouvelle directive à tous les employés du Ministère.

III. Contrôles administratifs

88. Les contrôles administratifs sont les mesures de protection procédurales mises en place pour le traitement sécuritaire des renseignements personnels, ce qui comprend l'application des politiques, directives et processus d'une institution devant assurer la protection des renseignements personnels tout au long de leur cycle de vie.

89. Pour qu'une institution fédérale puisse protéger comme il se doit les renseignements personnels qu'elle détient, elle doit savoir clairement où les données sont recueillies et où elles sont conservées. L'identification et le contrôle des biens, qu'il s'agisse de biens matériels ou d'information, est un aspect fondamental extrêmement important du respect de la vie privée qui contribue à réduire les risques de perte ou de dommages liés aux biens et à l'information du gouvernement fédéral, y compris les renseignements personnels.

90. Le Manuel des politiques et méthodes de sécurité d'EDSC stipule que le directeur, ou son délégué, est responsable de la sécurité de tous les biens matériels répertoriés pour le bureau. L'unité de la gestion des biens doit être consultée au sujet des exigences liées au contrôle et à l'inventaire des biens.

91. Notre examen nous a permis de déterminer que, au moment de l'incident, il n'y avait pas d'inventaire exhaustif des dispositifs portatifs sous la responsabilité de l'unité du PCPE. En fait, nous avons pu confirmer que les employés qui travaillaient au projet de migration des données n'étaient pas obligés de signer un registre pour utiliser le disque dur externe et que le dispositif ne contenait ni numéro d'inventaire, ni numéro de suivi. En outre, EDSC n'a pas été en mesure de confirmer de façon concluante le numéro de série du disque dur perdu.

92. Les ministères doivent non seulement toujours savoir quels biens ils ont en leur possession, mais ils doivent aussi connaître le degré de sensibilité et d'importance qui y est associé. C'est le fondement même d'une philosophie de gestion du risque.

93. Nous sommes également d'avis que la gestion et le contrôle des renseignements personnels contenus sur le disque dur n'étaient pas efficaces. Nous attirons plus particulièrement l'attention sur les observations suivantes :

- Bien qu'EDSC affirme que l'information en cause avait initialement été sauvegardée sur le disque dur en 2011 par la Division du soutien des programmes opérationnels, l'enquête n'a pas pu établir de manière concluante le contenu exact du disque dur lorsqu'il a été remis aux membres du projet de migration des données (unité du PCPE).

- Notre enquête a montré que les membres du projet de migration des données ne savaient pas exactement ce que contenait le disque dur externe.

- Notre enquête n'a pas pu établir quels renseignements précis ont été sauvegardés sur le disque dur par les membres de l'équipe de migration des données, ou le contenu exact du disque dur au moment où on s'est rendu compte qu'il avait disparu.

94. En fait, comme il est indiqué au paragraphe 17, EDSC affirme qu'il n'y a pas moyen de déterminer de manière concluante ce que contenait le disque dur au moment où on a signalé sa disparition, en novembre 2012. EDSC a créé un algorithme pour balayer le lecteur réseau afin d'identifier les fichiers et les dossiers contenant des renseignements personnels. Lorsqu'EDSC a indiqué quels types de renseignements contenait le disque dur, il s'agissait de l'information identifiée au cours de ce balayage du réseau.

95. À cet égard, nous ne sommes pas convaincus qu'EDSC a identifié ou classé l'information correctement, selon son degré de sensibilité (c.-à-d. « Protégé B »), ou que des mesures de contrôle étaient en place pour garantir la sécurité de cette information tout au long de son cycle de vie, ce qui comprend la sensibilisation des employés au caractère sensible de l'information.

96. Les contrôles administratifs font également référence à l'application des politiques, directives, procédures et processus dont une institution s'est dotée pour protéger les renseignements personnels.

97. Comme indiqué au paragraphe 70, même si nous sommes convaincus qu'au moment de l'incident EDSC avait de bonnes politiques pour la gestion de ses fonds de renseignements personnels, nous pensons qu'il y avait une lacune manifeste dans l'application de ces politiques aux activités quotidiennes du Ministère.

98. Par conséquent, nous ne sommes pas convaincus qu'au moment de l'incident EDSC avait des contrôles efficaces pour gérer l'information en question durant tout son cycle de vie.

IV. Contrôles de sécurité du personnel

99. Les contrôles de sécurité du personnel désignent la gestion, par un ministère, de ses employés — qualifications professionnelles, formation adéquate, supervision et mesures disciplinaires.

100. L'évaluation de la fiabilité des employés et de leurs qualifications professionnelles relativement à la protection des intérêts de l'employeur se fait au moyen d'enquêtes de sécurité et d'une vérification de la fiabilité, qui sont des conditions d'emploi aux termes de la *Loi sur l'emploi dans la fonction publique* (LEFP).

101. Notre enquête a confirmé que les employés qui avaient accès à l'information contenue sur le disque dur externe avaient tous une autorisation de sécurité valide correspondant au niveau de classification de l'information qu'ils devaient traiter dans le cadre de leur travail.

102. Les employés du gouvernement du Canada sont responsables de la gestion de l'information qu'ils recueillent, créent et utilisent à l'appui des programmes et services qu'ils mettent en œuvre.

103. À cette fin, ils ont la responsabilité d'appliquer les instruments de politique du gouvernement du Canada et du Ministère (politiques, normes et procédures connexes). Il est donc essentiel que les employés aient accès en temps opportun à de la formation pour qu'ils possèdent les connaissances, les aptitudes et les compétences requises pour s'acquitter de leurs tâches de façon efficace.

104. Nous ne sommes pas convaincus que, dans le cas qui nous occupe, les employés qui avaient accès au disque dur externe comprenaient bien les risques en matière de protection des renseignements personnels inhérents à l'utilisation de dispositifs portatifs, ou les vulnérabilités de l'information stockée sur le dispositif. En fait, nous pensons que les employés questionnés au cours de l'enquête ne savaient pas du tout quelle information contenait le disque dur.

105. Comme indiqué aux paragraphes 70 et 97, nous sommes d'avis qu'il y a une lacune manifeste dans l'application des politiques du Ministère aux activités quotidiennes qui s'y déroulent. Nous attirons l'attention sur la sensibilisation inadéquate des employés aux domaines suivants, ce qui a contribué à la vulnérabilité des pratiques de gestion de l'information d'EDSC au moment de l'incident :

- gérance de l'information — identification et traitement des renseignements personnels;
- responsabilités en matière de sécurité — procédures pour la conservation des renseignements personnels et des biens contenant des renseignements personnels;
- contrôles et responsabilités en matière de TI — mise en place de mesures de sécurité pour protéger les renseignements personnels, en particulier les renseignements stockés sur des dispositifs portatifs (p. ex. chiffrement);
- menaces — sensibilisation aux risques inhérents associés à la perte ou à l'accès, l'utilisation ou la communication non autorisées de renseignements personnels.

106. La sensibilisation des employés se fait grâce à une gestion efficace, au leadership et à la supervision des employés, et elle facilite les pratiques de gestion de l'information et réduit les risques d'erreur humaine, de méfait et de négligence. La sensibilisation peut prendre la forme d'une orientation officielle, de suivis, de supervision, d'inspections et de contrôles de vérification. La non-conformité entraîne des conséquences, et des mesures

doivent être prises pour déceler les risques et les gérer avant qu'ils ne se manifestent.

107. EDSC affirme que le Centre d'excellence de la sécurité de la TI diffuse tous les mois des conseils et des mises en garde à l'intention du personnel dans le cadre du Programme de sensibilisation à la sécurité de la TI. De plus, le Ministère rappelle régulièrement aux employés qu'il est important de protéger les renseignements personnels des Canadiens et que le traitement de ces renseignements doit se conformer à des procédures rigoureuses. Un cours de sensibilisation à la sécurité informatique a également été jugé nécessaire en juin 2009 lors de l'approbation par EDSC de la Politique ministérielle sur la gestion de la sécurité en technologie de l'information.

108. Comme il est dit au paragraphe 60, EDSC affirme que des efforts sont en cours en vue de la conception et de la fourniture d'une formation intégrée améliorée au personnel. Tous les employés devront suivre une formation obligatoire sur la protection des renseignements personnels, la sécurité, la sécurité des technologies de l'information, la gestion de l'information, et les valeurs et l'éthique.

109. Nous encourageons EDSC à continuer à mettre au point un programme complet de formation et de sensibilisation de manière à ce que les employés aient les connaissances, les aptitudes et les compétences nécessaires pour accomplir efficacement leurs tâches liées à la gestion de l'information.

110. Comme il est dit au paragraphe 52, EDSC affirme que des mesures administratives appropriées ont été prises dans le cas présent. Les ministères sont autorisés à établir des normes de discipline et à prescrire des mesures disciplinaires, y compris le licenciement, la suspension, la rétrogradation à un poste dont l'échelle de traitement comporte un plafond inférieur et des sanctions pécuniaires, pour un manquement à la discipline ou une inconduite, conformément aux Lignes directrices concernant la discipline du Secrétariat du Conseil du Trésor (SCT).

Constatations

111. La *Loi sur la protection des renseignements personnels* oblige les institutions fédérales à respecter la vie privée des individus en gérant comme il se doit la collecte, l'usage, la communication, la conservation et le retrait des renseignements personnels.

112. EDSC recueille périodiquement des renseignements personnels pour l'administration du PCPE. Il va sans dire que, afin de se conformer à son obligation de veiller à ne pas utiliser ni communiquer les renseignements personnels d'une manière contrevenant à la *Loi*, EDSC doit protéger les renseignements personnels qui ont été recueillis pendant leur cycle de vie — à partir du moment de la collecte jusqu'à leur destruction par une méthode approuvée.

113. Afin de protéger les renseignements personnels contre les utilisations et les communications non autorisées, les institutions fédérales doivent mettre en œuvre des mesures de sécurité adéquates.

114. Ce principe est soutenu par des politiques dans l'ensemble de l'administration fédérale. Par exemple, la Directive sur les pratiques relatives à la protection de la vie privée du SCT préconise la limitation de l'accès aux renseignements personnels et de l'utilisation de ceux-ci par des moyens administratifs, techniques et physiques afin de protéger les renseignements personnels, et la Politique sur la sécurité du gouvernement du SCT et ses normes connexes établissent des mesures de protection minimales pour la protection et la préservation de la confidentialité et de l'intégrité des biens gouvernementaux, y compris les renseignements personnels.

115. Le fait qu'EDSC n'a pas mis en œuvre les mesures de sécurité qui conviennent pour protéger les renseignements personnels en cause a créé un risque considérable d'accès, d'utilisation ou de communication non autorisés — ce contre quoi le gouvernement du Canada est censé les protéger. L'on s'inquiète particulièrement du volume et du caractère délicat des renseignements personnels figurant sur les disques durs externes — des renseignements qui, s'ils tombaient entre de mauvaises mains, pourraient ouvrir la porte au vol d'identité et à la fraude.

116. Il incombe également à EDSC de veiller à éliminer les renseignements personnels conformément aux exigences de la *Loi*, ce qui comprend l'obligation de procéder au retrait des renseignements conformément aux directives ou lignes directrices émises par le ministre désigné (c.-à-d. le président du Conseil du Trésor).

117. À cet égard, la Directive sur les pratiques relatives à la protection de la vie privée du SCT prévoit que les institutions fédérales éliminent les documents qui contiennent des renseignements personnels conformément aux dispositions de la *Loi sur la Bibliothèque et les Archives du Canada* et aux normes de sécurité gouvernementales.

118. Étant donné que, dans le cas qui nous occupe, le disque dur a été égaré, EDSC n'est pas en mesure de montrer qu'il s'est conformé à ces exigences pour éliminer comme il se devait les renseignements personnels contenus sur le disque.

119. Compte tenu de ce qui précède, nous ne sommes pas convaincus qu'EDSC a respecté les exigences du paragraphe 6(3) et des articles 7 ou 8 de la *Loi sur la protection des renseignements personnels* dans le cas qui nous occupe.

120. Par conséquent, nous avons conclu que la plainte était **fondée**.

Recommandations

121. Dans une lettre datée du 4 novembre 2013, le Commissariat a fourni un Rapport préliminaire de conclusions à EDSC conformément au paragraphe 33(2) de la *Loi sur la protection des renseignements personnels.* Le Rapport contenait des précisions sur notre enquête et énonçait les conclusions et recommandations préliminaires découlant de celle-ci.

122. À cette fin, nous avons recommandé qu'EDSC mette en œuvre un certain nombre de mesures de sécurité qui contribueraient à prévenir qu'un incident semblable ne se reproduise et qui aideraient le Ministère à répondre aux exigences de la *Loi* afin d'éviter les utilisations et les communications non autorisées de renseignements personnels. Les recommandations faites à EDSC reposaient sur les quatre types de mesures de contrôle que le Commissariat a énoncées comme offrant une protection contre les atteintes à la sécurité des renseignements personnels, conformément au paragraphe 72 du présent rapport.

123. Dans sa réponse au Rapport préliminaire de conclusions que nous avons reçue le 4 décembre 2013, EDSC a accepté nos recommandations intégralement. Nos recommandations et la réponse d'EDSC à chacune d'elles sont énoncées ci-après.

Recommandation 1 du Commissariat

Nous avons recommandé qu'EDSC revoie ses pratiques de contrôle de la sécurité physique de sorte que son programme de sécurité comporte des activités de surveillance et des inspections régulières. Cette mesure contribuera à faire en sorte que les renseignements personnels soient conservés dans des classeurs approuvés lorsque les employés ne sont pas à leur bureau pendant un certain temps; que les classeurs soient verrouillés en conséquence; que les clés des classeurs soient protégées comme il se doit; et que les biens attrayants ou précieux (p. ex. disques durs externes, ordinateurs portatifs, etc.) contenant des renseignements personnels soient protégés adéquatement.

Réponse d'EDSC

EDSC soutient avoir commencé à effectuer des ratissages de sécurité dans ses immeubles, y compris les cubicules et les bureaux des employés. EDSC affirme que cette initiative sensibilisera les employés à la perte possible des biens et des renseignements gouvernementaux et contribuera à atténuer le risque de tels incidents. EDSC met la dernière main à un plan prévoyant la conduite de ratissages de sécurité dans toutes les régions.

EDSC a souligné qu'il est en train d'élaborer un cadre de sécurité ministérielle qui établira les paramètres d'une gestion efficace des responsabilités en matière de sécurité et comportera des principes et pratiques de sécurité aux niveaux stratégique et opérationnel. Le cadre et les plans connexes contribueront à définir différents types d'exigences relatives à la sécurité et définiront les améliorations à apporter aux fonctions de sécurité tout en favorisant la formation et la sensibilisation en matière de sécurité.

Recommandation 2 du Commissariat

L'EFVP est un processus officiel permettant d'établir si les initiatives supposant l'utilisation de renseignements personnels posent des risques en matière de protection de la vie privée et propose des solutions pour l'élimination ou l'atténuation des risques en question à un niveau acceptable. L'EMR facilite la définition des exigences relatives à la sécurité des TI et peut être brève et simple, selon le caractère délicat, la pertinence et la complexité du programme, du système ou du service en cours d'évaluation. Nous avons recommandé qu'EDSC élabore des protocoles pour la coordination de l'inventaire et la classification de ses fonds de renseignements personnels et ses biens en menant des EFVP et des EMR à l'échelle du Ministère de manière à atténuer tous les risques relevés se rapportant à la protection de la vie privée.

Réponse d'EDSC

EDSC a souligné que le recensement, l'évaluation et l'atténuation des risques relatifs à la vie privée constituent un pilier clé de son cadre de gestion des renseignements personnels. À l'issue de la première étape du Plan d'action pour le renouvellement de la protection des renseignements personnels de 2011 d'EDSC, lequel comprenait une série d'évaluations des risques relatifs à la vie privée à l'égard des principaux programmes législatifs et fonds de renseignements personnels du Ministère, des plans d'action en matière de protection des renseignements personnels associés aux programmes ont été élaborés et lancés pour les huit programmes législatifs du Ministère en 2012 dans le cadre de la deuxième étape du Plan d'action pour le renouvellement de la protection des renseignements personnels.

En 2012-2013, EDSC soutient avoir renouvelé son processus d'évaluation des facteurs relatifs à la vie privée (EFVP) afin d'améliorer et de rationaliser les méthodes d'évaluation et d'atténuation des risques relatifs à la vie privée et a lancé un nouveau processus de planification stratégique censé appuyer la mise en œuvre d'un plan de travail annuel sur la protection de la vie privée et la sécurité de l'information.

EDSC soutient qu'il continuera de soutenir la mise en œuvre d'une approche proactive et axée sur le risque à l'égard de la gestion de la protection des renseignements personnels en misant sur les progrès réalisés à ce jour et en recensant et en évaluant les nouveaux risques relatifs à la protection de la vie privée et à la sécurité.

Recommandation 3 du Commissariat

Nous avons recommandé qu'EDSC mène à bien un examen exhaustif de ses fonds d'équipements pour s'assurer que tous les renseignements personnels et les biens contenant des renseignements personnels sont répertoriés et désignés selon le niveau de sécurité le plus élevé qui s'applique (p. ex. « Protégé B »), conformément au Manuel des politiques et méthodes de sécurité d'EDSC et de la norme concernant l'organisation et l'administration de la sécurité du Conseil du Trésor en ce qui concerne le choix des mesures de protection minimales applicables aux renseignements et aux biens.

Réponse d'EDSC

EDSC a signalé qu'il est en train de mettre en application une stratégie de gestion de l'information dans toutes ses directions

générales et régions, qui comprend les éléments fondamentaux suivants :

i. *L'examen de tous les dépôts en vue de l'établissement d'un inventaire des biens contenant des renseignements;*

ii. *Des décisions éclairées concernant la conservation et le retrait afin de s'assurer que les documents éphémères qui ne sont plus nécessaires soient éliminés et que les documents présentant une valeur opérationnelle soient protégés;*

iii. *La classification des documents conservés selon le niveau de sécurité adéquat, en fonction du guide de classification de l'information du Ministère;*

iv. *La protection adéquate, au moyen des droits d'accès, du cryptage ou des deux, de l'information ayant reçu la cote « Protégé » ou une cote supérieure.*

Recommandation 4 du Commissariat

Nous avons recommandé que les appareils portatifs de stockage ne servent qu'en dernier recours pour la conservation ou le transfert de renseignements personnels et uniquement si cela est manifestement nécessaire pour atteindre une fin précise et documentée. Tous les renseignements délicats ou personnels stockés sur un appareil portatif doivent être protégés par des mesures technologiques robustes, dont le chiffrement.

Réponse d'EDSC

EDSC a souligné que des mesures avaient été prises pour restreindre et gérer le recours aux appareils portatifs de stockage, dont :

1) le 11 janvier 2013, la Directive concernant les périphériques de stockage USB est entrée en vigueur et limite l'utilisation des dispositifs portatifs de stockage aux cas où la direction en valide la nécessité, préconise l'utilisation de clés USB ou disques durs cryptés (de façon biométrique et par mot de passe) et impose des sanctions en cas de non-respect; 2) le 18 janvier 2013, est entrée en vigueur une initiative de surveillance des ordinateurs de bureau pour détecter les cas d'utilisation non autorisée de clés USB; 3) le 27 mai 2013, des logiciels de sécurité ont été déployés afin d'interdire l'utilisation non autorisée de clés USB; et 4) le 3 juin 2013, des logiciels de sécurité ont été déployés afin de bloquer tous les dispositifs portatifs de stockage, comme les médias optiques (CD/DVD) et les disquettes. Seuls les utilisateurs autorisés peuvent sauvegarder des données sur de tels dispositifs.

Recommandation 5 du Commissariat

Nous avons recommandé qu'EDSC établisse des méthodes adéquates de gestion du matériel afin de répertorier et de surveiller tous les biens susceptibles de servir à stocker ou à transmettre des renseignements personnels délicats. Cela peut comprendre l'apposition d'un code à barres ou d'autres mesures d'inventaire permettant le traçage du bien. De plus, l'élément d'information relatif au bien (p. ex. numéro de série) doit être communiqué au personnel autorisé de gestion des biens.

Réponse d'EDSC

EDSC a confirmé que, à la suite de l'incident, l'achat, la distribution et la gestion des dispositifs portatifs sont centralisés, et l'approbation du sous-ministre adjoint (SMA) est nécessaire pour l'utilisation de tels dispositifs. De plus, EDSC a

souligné que les ordinateurs portatifs sont marqués et suivis par un numéro de série et un rapport est envoyé à une console technique chaque fois qu'ils sont connectés de sorte que se déploie le logiciel de sécurité voulu. Les clés USB et les disques durs portatifs cryptés sont suivis par numéro de série — l'information est intégrée dans un logiciel et sert à déceler la connexion au réseau du Ministère. À titre de précaution, une étiquette de couleur est apposée aux dispositifs et porte le numéro 1-800 du service de dépannage du Ministère au cas où quelqu'un trouverait un tel dispositif. EDSC a aussi confirmé que la Politique de gestion du matériel du Ministère est en voie d'être actualisée pour refléter le traçage des dispositifs.

Recommandation 6 du Commissariat

Nous avons recommandé qu'EDSC inclue des examens de la sécurité ou des inspections matérielles ponctuels des biens contenant des renseignements personnels pour s'assurer que des mesures de sécurité adéquates sont mises en œuvre pour protéger les renseignements personnels.

Réponse d'EDSC

EDSC affirme que les mesures qui suivent aideront le Ministère à sensibiliser davantage ses employés et intensifieront l'atténuation des risques potentiels de perte de biens et de renseignements gouvernementaux :

i. *Les Lignes directrices en matière de rangement du bureau ont été communiquées à tous les employés en août 2013, afin de les encourager à ranger leur bureau de manière à prévenir la communication non autorisée de renseignements délicats et la perte d'effets personnels;*

ii. *Des inspections de ratissage à l'égard des cubicules et des bureaux des employés sont désormais effectuées;*

iii. *Une validation de la conformité est comprise dans la portée approuvée de la vérification interne sur la sécurité des technologies de l'information, dans le cadre de laquelle les supports numériques portatifs individuels seront examinés afin d'évaluer les mesures de contrôle dans les domaines de la gestion des politiques, de la sécurité technique ainsi que de la sécurité opérationnelle. L'étape de la réalisation de la vérification sera en cours jusqu'en juillet 2014.*

Recommandation 7 du Commissariat

Nous avons recommandé qu'EDSC conçoive et mette en application des mesures de contrôle de sorte que les renseignements personnels soient gérés de manière rigoureuse pendant tout leur cycle de vie. Cela comprend l'instauration de mesures pour la gestion et le traçage des renseignements personnels et la sensibilisation et responsabilisation des employés à l'égard des renseignements personnels pendant tout leur cycle de vie.

Réponse d'EDSC

EDSC affirme qu'un élément essentiel de sa stratégie de gestion de l'information consiste à faire en sorte que les documents reçoivent la cote de sécurité qui convient et que les documents « Protégé » ou plus soient conservés comme il se doit. Grâce à une formation adéquate, des processus définis et des suivis réguliers, EDSC estime que ses employés seront en tout temps sensibilisés à la

façon adéquate de traiter les documents délicats.

Dès juin 2013, un logiciel de prévention de la perte de données a été déployé et effectue le balayage régulier des fonds de renseignements. Des algorithmes perfectionnés détectent le moment où des dossiers délicats ne sont pas protégés adéquatement, ce qui permet à la direction de prendre les mesures voulues de sorte que les documents soient mieux gérés.

De plus, EDSC soutient que la sensibilisation et la responsabilisation des employés à l'égard des renseignements personnels pendant tout le cycle de vie constituent un élément clé du Plan d'action pour le renouvellement de la protection des renseignements personnels. EDSC a souligné certains de ses efforts constants, dont la tenue d'une semaine de sensibilisation à la protection de la vie privée, en janvier 2013; des activités organisées dans toutes les directions générales et les régions entre février et juin 2013 pour mobiliser les employés à l'égard de l'importance de la protection des renseignements personnels; le lancement, en août 2013, d'un portail de gestion de l'information qui offre aux employés des renseignements sur les rôles et les responsabilités, des politiques, des outils et d'autres ressources sur la protection de la vie privée, la sécurité, la gestion de l'information, et les valeurs et l'éthique. EDSC continuera de sensibiliser les employés quant à leurs rôles et à leurs responsabilités ainsi qu'aux risques et aux menaces associés à la protection des renseignements personnels au moyen d'interventions et d'activités ciblées.

Recommandation 8 du Commissariat

Nous avons recommandé que le programme de formation et de sensibilisation d'EDSC privilégie les éléments suivants :

- Des stratégies pour faire en sorte que tous les employés comprennent leurs rôles et leurs responsabilités dans la gestion des renseignements personnels au cours de leur cycle de vie, y compris le recensement et le traitement des renseignements personnels;
- Les exigences relatives à la sécurité physique énoncées dans le Manuel des politiques et méthodes de sécurité d'EDSC (classeurs approuvés, dispositifs de verrouillage, etc.), y compris les conditions relatives à l'utilisation et à la protection adéquates des biens attrayants ou précieux contenants des renseignements personnels (p. ex. disques durs externes, ordinateurs portatifs, etc.);
- Les exigences relatives à la protection des renseignements personnels, y compris les mesures de contrôle de TI pour les dispositifs portatifs (p. ex. le cryptage). Les employés qui ont accès à des renseignements personnels délicats doivent être conscients des risques relatifs à la vie privée inhérents à l'utilisation des dispositifs portatifs et des vulnérabilités des données susceptibles d'être stockées sur ces dispositifs (p. ex. la perte de renseignements ou leur consultation, utilisation ou communication non autorisées);
- Les conséquences du non-respect des normes de sécurité et de protection de la vie privée du Ministère.

Réponse d'EDSC

EDSC a souligné qu'en avril 2013 il avait approuvé une stratégie d'acquisition du savoir intégrée visant les nouveaux employés et ceux en poste qui consolide les acquis dans les domaines clés se rapportant à la protection des renseignements personnels. À titre de mesure supplémentaire, tous les nouveaux employés et ceux déjà en poste doivent subir un examen tous les deux ans pour s'assurer qu'ils respectent les modalités se rapportant à la protection des renseignements personnels.

En outre, EDSC soutient que lorsqu'un dispositif portatif est remis à un employé, celui-ci signe une déclaration signifiant qu'il a reçu le dispositif et comprend les dispositions se rapportant à son utilisation.

Recommandation 9 du Commissariat

Nous avons recommandé que la participation aux séances de formation soit obligatoire et qu'elle soit documentée.

Réponse d'EDSC

Conformément à son ensemble de politiques sur l'acquisition du savoir, EDSC soutient que de nouvelles lignes directrices obligatoires sur la formation ont été approuvées, qu'elles énoncent clairement la marche à suivre, les rôles et les responsabilités des cadres et des employés concernant les exigences en matière d'acquisition du savoir eu égard au nouveau programme obligatoire de formation sur la gestion de l'information et les comportements à adopter en milieu de travail. Ce programme de formation, qui porte sur la protection des renseignements personnels, la sécurité des technologies de l'information, la gestion de l'information, la sécurité et les valeurs, ainsi que l'éthique et le code de déontologie, a été approuvé à titre d'objectif d'apprentissage obligatoire du Ministère et a été lancé en septembre 2013. Pendant la première étape de sa mise en œuvre, le programme de formation a été perfectionné et des problèmes liés aux systèmes ont été résolus. Le programme de formation a par la suite été lancé à nouveau en février 2014. On s'attend à ce que tous les employés aient suivi la formation d'ici le mois d'août 2014.

Tous les employés devront suivre la formation et subir les examens obligatoires. Le Ministère suivra le respect de cet objectif au moyen d'un système de gestion de l'acquisition du savoir et des rapports trimestriels seront envoyés à cet égard aux cadres supérieurs. Il revient à ceux-ci de suivre les employés en ce qui concerne la participation à la formation, les examens et les revalidations obligatoires.

Recommandation 10 du Commissariat

Nous avons recommandé qu'EDSC adopte des mesures permettant de suivre les méthodes de gestion des renseignements personnels, particulièrement dans les cas où il est nécessaire d'utiliser ou de transférer des renseignements personnels sur des dispositifs portatifs de stockage (p. ex. disques durs externes, ordinateurs portatifs, etc.). Cela peut comprendre des orientations, des suivis, des inspections ou des vérifications officielles.

Réponse d'EDSC

EDSC soutient que les mesures qui suivent ont été instaurées pour suivre les méthodes de gestion de l'information se rapportant aux renseignements personnels pouvant être délicats :

- *Conformément à la Directive concernant les périphériques de stockage USB, tous les dispositifs USB pour le stockage de données doivent être cryptés de façon biométrique ou au moyen d'un mot de passe;*

- *Chaque employé qui reçoit un dispositif crypté signe une déclaration indiquant qu'il connaît la norme pour l'utilisation acceptable du dispositif et l'engageant à présenter l'appareil en tout temps aux fins de vérification. La vérification interne de la sécurité des TI comprendra une disposition pour les vérifications de conformité;*

- *Les ports USB sont surveillés, et la Sécurité des TI établit un rapport hebdomadaire sur les utilisations non autorisées potentielles de dispositifs USB;*

- *Les outils de prévention de la perte de données ratissent les dépôts de fichiers afin de relever les fichiers susceptibles de présenter un risque.*

Autres observations

124. Dans le Rapport préliminaire de conclusions, nous avons aussi fait des observations à EDSC en ce qui concerne la façon dont l'organisation a réagi à l'incident — notamment les mesures immédiates prises par le Ministère à la suite de l'incident et la notification des personnes touchées.

125. Des personnes qui ont porté plainte auprès du Commissariat ont exprimé des préoccupations au sujet du temps pris par EDSC pour aviser les personnes touchées par cet incident. Conformément aux Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor, la notification des personnes touchées par l'incident, particulièrement dans les cas où des renseignements personnels délicats sont compromis, devrait intervenir « [...] dans les meilleurs délais, pour leur permettre de prendre des mesures de protection ou d'atténuer les préjudices causés par le vol d'identité ou les autres torts possibles ».

126. Nous estimons, étant donné l'étendue de l'incident et des mesures d'atténuation qu'a dû prendre EDSC à la suite de la perte du disque dur externe, que le temps pris par l'organisation pour aviser les personnes touchées par écrit était raisonnable dans les circonstances.

127. Nous reconnaissons dans ce cas que des efforts considérables ont été déployés pour chercher le disque dur externe égaré, y compris la conduite d'analyses informatico-judiciaires; le recensement des personnes touchées par l'incident et la confirmation de leur adresse; le lancement d'une campagne d'information du public (établissement d'un centre d'appels, rédaction de communiqués, etc.); la coordination de la surveillance des NAS; la négociation d'une entente avec Equifax pour la prestation de services de protection du crédit; et, bien entendu, la diffusion d'une déclaration publique le 11 janvier 2013.

128. Nonobstant ce qui précède, nous aimerions souligner que davantage de renseignements personnels que ceux signalés par EDSC aux personnes touchées pourraient avoir été compromis à la suite de la perte du disque dur. Conformément au paragraphe 20, les observations d'EDSC décrivaient les champs d'information particuliers susceptibles d'avoir été compromis à la suite de l'incident.

129. Bien qu'EDSC soutienne que ces champs ont été regroupés en sept types de renseignements personnels afin d'informer les personnes atteintes le plus rapidement possible, nous ne pouvons pas comprendre en quoi certains des renseignements personnels qui n'ont pas été signalés dans la lettre d'avis d'EDSC aux personnes touchées — par exemple, le sexe, la langue ou l'état matrimonial de l'emprunteur — ont pu être regroupés dans les « sept types de renseignements personnels », comme le prétend EDSC.

130. Nous estimons que la combinaison de certains types de renseignements personnels délicats augmente les risques de vol d'identité et, par conséquent, il est essentiel à notre avis qu'une liste complète des éléments de renseignements personnels se rapportant à la personne qui sont susceptibles d'avoir été compromis ou pouvant avoir été compromis soit incluse dans l'avis.

131. La transparence est le principe fondamental clé associé à la responsabilité gouvernementale. À cette fin, nous signalons à EDSC les orientations du Conseil du Trésor pour le signalement des atteintes à la vie privée et les mesures à prendre à cet égard, particulièrement les Lignes directrices sur les atteintes à la vie privée. Nous soulignons aussi l'importance de respecter la Politique sur la protection de la vie privée du Conseil du Trésor, laquelle a notamment pour objectif de favoriser une application efficace de la *Loi sur la protection des renseignements personnels* et son *Règlement*.

132. Nous soulignons les observations faites par EDSC dans sa réponse au Commissariat datée du 4 décembre 2013 :

    - *EDSC soutient que la portée et l'étendue de l'incident l'obligeaient à prendre un certain nombre de mesures afin d'établir ce que contenait l'objet égaré et les personnes touchées. Il était alors essentiel d'informer la population canadienne et les clients le plus rapidement possible et, par conséquent, EDSC a envoyé des avis écrits et assuré le suivi avec des lettres destinées à tous les clients pour qui le Ministère possédait une adresse valide.*

- *EDSC soutient que le fait d'attendre pour rédiger des lettres personnalisées contenant les renseignements particuliers susceptibles de figurer sur le disque dur aurait retardé inutilement le processus de notification. Après l'envoi par la poste de la première lettre, les clients ont contacté le Ministère pour demander la confirmation des renseignements susceptibles de figurer sur le disque dur. Le Ministère a répondu à ces demandes en fournissant les renseignements personnels exacts associés au client ayant fait la demande.*

- *En outre, EDSC soutient qu'à ce jour, elle n'a reçu aucune information voulant que les renseignements personnels susceptibles de figurer sur le disque dur externe aient été consultés ou utilisés à des fins frauduleuses. EDSC se dit en mesure de faire une telle affirmation après avoir examiné les résultats du suivi des numéros d'assurance sociale et après les analyses approfondies menées par Equifax, le bureau de crédit avec lequel le Ministère a conclu un contrat pour surveiller le dossier de crédit des personnes touchées par l'incident.*

Conclusion

133. Notre enquête a porté sur les mesures de contrôle physiques, techniques, administratives et de sécurité du personnel qui étaient en vigueur à EDSC au moment de l'incident — ce que nous appelons les quatre piliers d'une bonne gestion de la protection de la vie privée. À notre avis, ces mesures devraient être incorporées dans le cadre de gestion des renseignements personnels d'une institution afin de prévenir les atteintes à la vie privée, y compris la collecte, l'utilisation, la communication, la conservation et/ou l'élimination de renseignements personnels contraires aux règles ou non autorisées.

134. Notre enquête a fait ressortir un écart mesurable dans la mise en œuvre par EDSC de ses politiques sur la protection de la vie privée et la sécurité en ce qui a trait aux opérations courantes du Ministère. Cet écart a entraîné des faiblesses dans les mesures de contrôle de gestion de l'information, les mesures de contrôle de la sécurité physique et, surtout, la sensibilisation des employés aux politiques et aux méthodes du Ministère.

135. Bien que nous ayons constaté qu'EDSC contrevient au paragraphe 6(3), à l'article 7 ou à l'article 8 de la *Loi sur la protection des renseignements personnels*, dans ce cas, le Ministère a accepté toutes nos recommandations intégralement et réalise d'importants progrès dans la mise en œuvre d'un bon nombre d'entre elles.

136. Pour cette raison, nous sommes convaincus que le Commissariat n'a pas besoin d'intervenir à nouveau pour le moment. Quoi qu'il en soit, nous reprendrons contact avec EDSC dans un an pour confirmer les progrès réalisés dans la mise en œuvre de nos recommandations et les efforts déployés par l'organisation au plan de la gestion de ses fonds de renseignements personnels.

137. Nous profitons de l'occasion pour souligner l'importance d'établir une synergie entre les mesures de contrôle de la protection de la vie privée et de la sécurité afin d'atténuer efficacement les risques relatifs à la vie privée. C'est la mise en œuvre de ces mesures qui aidera EDSC à bien protéger les renseignements personnels que la population canadienne lui confie.

138. Nous nous attendons à ce qu'EDSC respecte l'esprit et les dispositions de la *Loi sur la protection des renseignements personnels* — la protection de la vie privée constitue une valeur fondamentale pour les Canadiennes et les Canadiens et représente un élément essentiel pour conserver la confiance du public dans l'administration publique. Par conséquent, nous rappelons à EDSC qu'il lui faut constamment être conscient des renseignements personnels et des biens qu'il détient, ainsi que de leur caractère délicat et de leur importance. La protection des renseignements personnels doit faire partie intégrante de toutes les fonctions du Ministère, ce qui suppose l'établissement d'une structure de gouvernance ayant le poids, les éléments et le mandat voulus pour assurer une mise en œuvre efficace des instruments de politique.

Renseignements supplémentaires

139. Pour obtenir des renseignements supplémentaires sur le Commissariat et les pouvoirs de la commissaire à la protection de la vie privée, veuillez visiter notre site Web à l'adresse www.priv.gc.ca. Notre site offre également des ressources documentaires susceptibles d'intéresser les personnes touchées par l'incident, notamment sur le vol d'identité et la fraude.