Commissariat à la
protection de la vie privée
du Canada

Office of the
Privacy Commissioner
of Canada

Vérification de la protection de la vie privée des opérations liées au passeport canadien

Décembre 2008

Table des matières

Résumé

1.1 La vérification visait l'évaluation de la mesure dans laquelle Passeport Canada gère les renseignements personnels de façon à ce que la vie privée des Canadiennes et des Canadiens soit protégée. La vérification a débuté le 12 octobre 2006. Le travail sur le terrain a pris fin le 31 janvier 2008, date à laquelle nos observations et nos recommandations ont pris effet.

1.2 Au cours de notre vérification, nous avons constaté que Passeport Canada accorde une grande importance au service et tient à assurer l'intégrité du passeport canadien. Nous avons également noté que l'organisation subit de grandes pressions en raison du volume sans précédent de nouvelles demandes de passeports qu'elle doit traiter, qui atteint des millions.

1.3 Bien que nous ayons relevé des éléments positifs en ce qui concerne la protection de la vie privée, nous avons décelé des lacunes dans un certain nombre de domaines qui nécessitent une attention de la part des cadres de Passeport Canada et du ministère des Affaires étrangères et du Commerce international (MAECI). Prises ensemble, ces lacunes posent un risque considérable à la protection générale des renseignements personnels des Canadiennes et des Canadiens. Nous concluons que le cadre de gestion de la protection de la vie privée régissant les activités liées au passeport doit être renforcé par différentes mesures importantes et interdépendantes. À cette fin, nous faisons 15 recommandations (voir annexe A).

1.4 Nous aimerions remercier de nombreux employés de Passeport Canada et du MAECI pour leur aide, leur collaboration et leur réceptivité tout au long de notre vérification. Les fonctionnaires ont fait preuve en tout temps d'empressement, de respect et de professionnalisme.

Collecte des renseignements personnels

1.5 Nous avons des réserves tenant au fait que Passeport Canada recueille des renseignements personnels de nature délicate au moyen d'un seul formulaire de demande de passeport. Plus particulièrement, nous sommes préoccupés par le fait que les renseignements concernant la carte de crédit du demandeur et la déclaration du répondant sont recueillis en combinaison avec d'autres renseignements permettant d'établir l'identité (p. ex. le nom, l'adresse, le numéro de téléphone et la date de naissance) sur le même formulaire de demande, et que la carte d'assurance sociale est acceptée comme preuve d'identité. Cette pratique de collecte de renseignements pourrait accroître le risque de vol d'identité pour les Canadiennes et les Canadiens si l'information était utilisée ou communiquée de façon inappropriée.

Contrôle de la consultation, de l'utilisation et de la communication des renseignements personnels

1.6 Des mesures de contrôle servant à limiter l'accès aux renseignements personnels nécessitent une attention car elles ne tiennent pas toujours compte du fait que les renseignements relatifs au passeport sont définis comme des renseignements « de nature particulièrement délicate » portant la mention « Protégé B » dans le *Guide de classification de l'information* de Passeport Canada. Nous avons également constaté que le principe du « besoin de connaître » n'était pas appliqué uniformément et que l'accès aux systèmes d'information n'était pas suffisamment contrôlé pour s'assurer que seuls les employés qui ont besoin de l'information pour s'acquitter de leurs tâches ont accès à celle-ci. Par exemple, nous avons découvert que les agents consulaires dans les missions à l'étranger avaient accès aux dossiers de passeport traités dans d'autres missions du monde entier alors qu'ils avaient rarement besoin de ces renseignements et qu'ils auraient pu les obtenir, au besoin, auprès du MAECI ou de Passeport Canada. Un vaste accès aux dossiers de passeport à l'étranger augmente les risques de communication indue des renseignements personnels.

1.7 Nous avons constaté qu'aucun employé à Passeport Canada ou au MAECI n'était expressément chargé de s'assurer que les droits d'accès soient mis à jour pour rendre compte des changements dans le personnel. Bien que les employés du centre d'assistance en TI aient la responsabilité de modifier les droits d'accès, ils ne sont pas toujours au courant des changements dans le personnel ou dans les fonctions des employés qui ont une incidence sur les droits d'accès. Dans un cas, un employé qui avait pris sa retraite six mois auparavant avait toujours accès au système du consulat. Dans d'autres cas, des employés qui ne participaient pas au processus relatif au passeport détenaient des droits d'accès au système de passeports du consulat. Le nom d'autres personnes apparaissait sur des listes d'accès alors que ces personnes ne possédaient plus de droits d'accès.

1.8 Plus important encore, nous avons découvert que le système IRIS et le système du Programme de gestion des passeports (PMP) – journal électronique permettant de savoir qui a consulté les demandes de passeport – n'étaient soumis à aucun contrôle de base. Selon nous, cela augmente les risques que des renseignements concernant un demandeur soient utilisés ou communiqués de façon inappropriée.

Mesures appropriées de conservation et d'élimination des renseignements personnels

1.9 Passeport Canada archive les dossiers de passeport électroniques pour une période allant jusqu'à 100 ans. Il n'est pas clair pourquoi il procède ainsi. Nous avons observé que ces renseignements personnels ne sont pas chiffrés, ce qui augmente les risques qu'on les consulte ou qu'on les utilise de façon inappropriée alors qu'ils sont sous la garde de Passeport Canada. En vertu de la *Loi sur la protection des renseignements personnels*, les renseignements ne devraient être conservés qu'aussi longtemps qu'ils sont utiles à des fins administratives, à moins de dispositions contraires dans les règlements.

1.10 Nous avons décelé des lacunes dans certaines des pratiques actuelles de Passeport Canada en ce qui a trait à l'élimination ou à la destruction de fichiers contenant des renseignements personnels sur supports papier et électronique. Par exemple, nous avons constaté que dans un certain nombre de bureaux à Passeport Canada et dans les missions, des formulaires administratifs contenant des renseignements personnels étaient jetés dans des poubelles et dans des bacs de recyclage ordinaires. Dans une installation de déchiquetage du secteur privé, des photos de passeport entières étaient visibles et des documents pouvaient être reconstitués et rendus lisibles même après avoir été passés dans la déchiqueteuse.

1.11 Nous remarquons que le recours à des messagers du secteur privé pour transporter du matériel informatique excédentaire contenant des renseignements de nature délicate d'un bureau de Passeport Canada à l'autre comporte des risques, comme en témoignent les récentes atteintes à la sécurité des données survenues ailleurs dans les secteurs public et privé et mettant en cause cette pratique.

Mesures de sécurité essentielles

1.12 Les systèmes mis en place par Passeport Canada et le MAECI (« Services consulaires »[1]) pour assurer la sécurité de leur matériel, de leur personnel et des TI offrent généralement une bonne protection de la vie privée. Cependant, nous avons décelé certaines lacunes importantes dans les mesures de sécurité internes, qui devraient être corrigées.

1.13 Selon les endroits visités, les mesures de sécurité matérielle adoptées pour empêcher toute personne de l'extérieur de pénétrer dans les zones d'accès restreint à Passeport Canada et au MAECI semblent efficaces dans les deux organisations. Toutefois, les pratiques internes d'entreposage des dossiers de passeport et des documents à l'appui (p. ex. dans des sacs de plastique transparents et sur des rayons à libre accès) sont inappropriées. À notre avis, cette méthode d'entreposage est inadéquate pour des dossiers de nature aussi délicate, car elle protège mal les dossiers contre un accès inapproprié ou involontaire de la part d'employés qui pourraient ne pas avoir besoin de ces renseignements pour s'acquitter de leurs tâches.

1.14 Nous avons remarqué, en comparant la conception et la disposition des différentes sections consulaires des missions du MAECI que nous avons visitées à l'étranger, que le niveau de protection de la vie privée n'était pas uniforme. Dans plusieurs missions, les conversations entre les demandeurs et les fonctionnaires consulaires pouvaient être entendues depuis la salle d'attente. Nous faisons remarquer, toutefois, que lorsque nous avons attiré l'attention des fonctionnaires sur ce problème dans les missions visitées, ceux-ci ont pris des mesures immédiates pour corriger la situation et ont indiqué que davantage d'efforts seront déployés pour régler ce problème.

[1] On entend par « Services consulaires », dans le contexte de la présente vérification, les services offerts au public dans les missions canadiennes à l'étranger se rapportant aux passeports et aux titres de voyage. D'autres services consulaires sont fournis au public à ces missions, mais ils n'étaient pas visés par notre vérification du programme de passeport canadien. La section opérationnelle à l'administration centrale du MAECI qui appuie ces services à l'étranger est le Secteur des services consulaires et de la gestion des urgences.

1.15 Les difficultés liées à l'obtention des dossiers judiciaires et des dossiers de renseignements dans certains pays autres que le Canada aux fins des enquêtes de sécurité et du processus d'autorisation de sécurité pour les employés des « Services consulaires » recrutés sur place – qui peuvent être des citoyens canadiens ou non – représentent un défi pour le MAECI au moment où Passeport Canada augmente le niveau minimal requis pour la cote de sécurité de ses employés, la faisant passer de « Fiable » à « Secret ». Cependant, on pourrait atténuer les risques que pose cette situation en corrigeant certaines lacunes notées dans notre rapport, notamment en améliorant les contrôles d'accès aux renseignements personnels et en dotant les systèmes des TI de mécanismes de suivi des activités.

Sécurité des technologies d'informatiques (TI)

1.16 Nos inquiétudes dans ce domaine ont trait à l'utilisation de dispositifs de stockage portatifs et aux lacunes observées dans le chiffrement de certains renseignements personnels stockés dans les systèmes des TI et figurant dans les courriels diffusés à l'extérieur de Passeport Canada et du MAECI.

1.17 Ni Passeport Canada ni le MAECI ne disposent d'une politique organisationnelle restreignant l'utilisation des dispositifs de stockage portatifs, comme les clés USB, les lecteurs MP3 et les téléphones cellulaires, dans les bureaux de Passeport Canada ou dans les secteurs consulaires des missions du MAECI. Quiconque a accès à ces bureaux et aux systèmes d'information sur les passeports pourrait facilement photographier, télécharger ou copier des renseignements personnels stockés dans les ordinateurs des organisations sans être repéré. Compte tenu du risque inhérent lié à l'utilisation de ces nouveaux outils technologiques à des fins d'entreposage de renseignements personnels de nature délicate, nous croyons qu'il est urgent que les deux organisations élaborent et mettent en œuvre des politiques régissant l'utilisation des dispositifs de stockage portatifs dans leurs bureaux.

1.18 Le fonds permanent de renseignements personnels stockés dans la principale base de données de Passeport Canada, IRIS, et dans le système du Programme de gestion des passeports du MAECI n'est pas chiffré. L'absence de cette mesure de protection importante accroît les risques d'accès non autorisé à ces renseignements en « texte clair », un problème de sécurité qui devrait préoccuper les deux organisations. Voir l'annexe E pour un résumé concernant les systèmes d'information sur les passeports.

1.19 Nous avons constaté que Passeport Canada et le MAECI ont recours au chiffrement pour leurs réseaux internes afin de protéger les courriels transmis à d'autres employés. Cependant, plusieurs des employés interrogés ignoraient que les courriels diffusés à l'extérieur des réseaux internes protégés pouvaient ne pas être chiffrés. Tout renseignement personnel figurant dans des courriels envoyés sous une forme non chiffrée à des réseaux externes risque d'être intercepté, copié, modifié et utilisé de façon inappropriée par des pirates informatiques.

1.20 Enfin, nous insistons sur le fait que notre vérification ne visait pas à déceler les atteintes à la vie privée. De fait, aucun cas n'a été porté à notre attention au cours de notre examen, à l'exception de l'incident lié au passeport en direct (PED) – voir le paragraphe 3.114. Ce qui nous inquiète, à la lumière des lacunes dans les mesures de contrôle mentionnées ci-dessus et compte tenu du fait que les incidents liés à la protection des données ne sont pas systématiquement rapportés, c'est que des renseignements personnels pourraient disparaître sans que les organisations en aient connaissance.

Établissement d'un cadre de gestion de la protection de la vie privée et de la sécurité

1.21 L'ensemble des mesures de gestion de la protection de la vie privée de Passeport Canada doit être renforcé, comme en témoignent nos constatations ci-dessus. À ce chapitre, nous nous inquiétons notamment du fait que l'organisation n'a pas de <<chef de la protection de la vie privée>> et que le MAECI n'a pas délégué les pleins pouvoirs en matière d'accès à l'information et de protection des renseignements personnels (AIPRP) à Passeport Canada pour ce qui est des questions de protection de la vie privée. Sans ces pouvoirs, Passeport Canada doit s'en remettre à la section de l'AIPRP du MAECI pour remplir ses responsabilités en ce qui concerne la protection des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels*. Par conséquent, les principales responsabilités concernant la protection de la vie privée dans le cadre du programme des passeports sont dispersées et, comme nous le mentionnons plus loin dans la section des observations et des recommandations, nous ne croyons pas qu'elles aient fait l'objet d'une attention suffisante.

Un élément important de la gestion de la protection de la vie privée et de la sécurité est de s'assurer que les employés qui traitent des renseignements personnels de nature délicate dans le cadre de leurs activités quotidiennes comprennent leurs responsabilités en ce qui a trait à la protection de ces renseignements en vertu de la *Loi sur la protection des renseignements personnels*, ainsi que leurs responsabilités de base en ce qui concerne la sécurité en vertu de la Politique du gouvernement sur la sécurité. Nous avons constaté des lacunes dans les connaissances des employés dans certains domaines de la protection de la vie privée et de la sécurité de l'information. Nous notons, toutefois, que Passeport Canada a commencé à offrir à son personnel des séances de formation sur la protection de la vie privée dans ces domaines clés.

Introduction

Pourquoi cette vérification des opérations liées au passeport canadien est importante

2.1 Pour remplir son mandat, Passeport Canada, en collaboration avec ses partenaires, recueille et utilise des renseignements personnels de nature très délicate sur tous les Canadiennes et les Canadiens qui demandent un passeport ou tout autre titre de voyage. Certains de ces renseignements peuvent également être communiqués à des tierces parties à des fins légitimes. Passeport Canada a actuellement la garde de plus de 30 millions de dossiers de passeport.

2.2 Protéger les renseignements personnels de nature délicate des Canadiennes et des Canadiens est extrêmement important. Si l'information sur les passeports tombait dans « de mauvaises mains », elle pourrait être perdue, détruite ou utilisée de façon inappropriée. Le vol et l'utilisation inappropriée de renseignements personnels pourraient entraîner de graves conséquences pour la personne à qui appartiennent ces renseignements personnels, comme le vol d'identité et la fraude financière.

2.3 Pour ces raisons, il est essentiel que Passeport Canada fournisse l'assurance, à un niveau élevé, que les renseignements personnels en sa possession sont gérés de façon efficace tout au long de leur cycle de vie (de la collecte à la destruction), quel que soit l'endroit où les demandes de passeport sont traitées.

Le Canada et le système de passeport mondial

2.4 La mondialisation apparue à la fin du XX^{e} siècle et au début du XXI^{e} siècle signifie l'accroissement des mouvements de biens, de services, de main-d'œuvre, de technologie et de capital à l'échelle internationale. Bien qu'il ne s'agisse pas d'un phénomène nouveau, la mondialisation a pris beaucoup d'ampleur avec l'arrivée des nouvelles technologies, particulièrement dans le domaine des télécommunications.

2.5 La mondialisation a brouillé le concept de frontières nationales en permettant aux échanges et au commerce de s'étendre, ce qui a donné lieu à certains problèmes comme la traite transfrontalière de personnes, le crime organisé et le terrorisme international. Ces risques ont eu pour effet de resserrer les exigences internationales à l'endroit des voyageurs qui demandent un passeport. Par ailleurs, les Nations Unies et d'autres organisations internationales ont contribué à harmoniser davantage les exigences en matière d'intégrité et de sécurité des passeports à l'échelle mondiale.

2.6 Le Canada et quelque193 autres pays délivrent chaque année des millions de passeports pour permettre aux citoyens de voyager d'un pays à l'autre en toute sécurité. Les passeports, toutefois, ne remplissent plus uniquement cette fonction de base; ils sont devenus des pièces d'identité dont les particuliers ont besoin pour participer à l'économie mondiale.

2.7 Passeport Canada a expliqué que « les passeports sont devenus un bien essentiel pour le Canada et pour les Canadiennes et les Canadiens. Ils fournissent une preuve de l'identité et de la citoyenneté, une preuve à l'appui de l'admissibilité à tous les types de services et de prestations du gouvernement; ils facilitent les déplacements à l'étranger et le commerce international; ils favorisent la coopération internationale dans le cadre de la lutte antiterroriste; enfin, ils contribuent à la sécurité internationale et nationale ». (Source : Rapport annuel de Passeport Canada de 2006-2007, annexe A, p. 1)

2.8 Depuis les attentats du 11 septembre 2001, de fortes pressions sont exercées sur les pays pour qu'ils augmentent la sécurité et l'intégrité des passeports qu'ils délivrent à leurs citoyens. Cet impératif mondial a eu pour effet de forcer certains bureaux de passeports, comme Passeport Canada, à rapatrier la fonction d'impression des passeports assumée par les missions, à mettre en place de nouvelles mesures de sécurité pour limiter la fraude de passeport, à redoubler de vigilance dans l'examen des demandes de passeport et à étendre les ententes sur l'échange d'information avec les services de police et les organismes de renseignements au pays et à l'étranger.

2.9 Malgré la peur du terrorisme et le resserrement de ces mesures de sécurité, les Canadiennes et les Canadiens n'ont pas cessé de voyager. Au contraire, en 2007 seulement, les Canadiennes et les Canadiens ont effectué plus de 21 millions de voyages à l'étranger, dont 16 millions aux États-Unis. La plupart de ces personnes devaient être munies d'un passeport valide ou d'un titre de voyage officiel délivré par Passeport Canada ou par le MAECI pour être autorisées à voyager à l'étranger.

2.10 L'Initiative relative aux voyages dans l'hémisphère occidental (IVHO) fait partie de l'*Intelligence Reform and Terrorism Prevention Act*, une loi américaine adoptée en 2004. Le 23 janvier 2007, l'IVHO est entrée en vigueur, et tous les voyageurs aériens devaient présenter un passeport à leur arrivée aux États-Unis. D'ici le 1er juin 2009, toutes les personnes qui se rendront aux États-Unis par voie terrestre ou maritime devront avoir en main un passeport ou un autre titre de voyage approuvé, comme la carte NEXUS.

2.11 Lors de la rédaction de notre rapport, nous avons tenu compte des changements survenus au sein de Passeport Canada et chez ses partenaires avant la fin de notre examen, soit le 31 janvier 2008, qui ont eu des répercussions sur la gestion des renseignements personnels.

Passeport Canada

2.12 En vertu du *Décret sur les passeports canadiens* (TR-81-86) tel que modifié (DPC), le ministre des Affaires étrangères et du Commerce international confère à Passeport Canada le mandat et le pouvoir légal de délivrer, de refuser de délivrer, de révoquer, de retenir et de surveiller l'utilisation des passeports et des autres titres de voyage pour les Canadiennes et les Canadiens et les résidents canadiens.

2.13 Passeport Canada, un organisme de service spécial (OSS) relevant du MAECI, a été créé en 1990 pour remplacer le Bureau des passeports. Son titre d'OSS lui confère le droit, dans une certaine mesure, de gérer ses opérations courantes comme une entreprise du secteur privé, bien que légalement, il fait toujours partie du MAECI et doit rendre compte à son ministre. Passeport Canada est également assujetti aux lois et aux règlements applicables au secteur public, comme la *Loi sur la protection des renseignements personnels* et les lignes directrices du Secrétariat du Conseil de Trésor (SCT) sur la protection des renseignements personnels.

2.14 Le processus d'examen des demandes de passeport à Passeport Canada et au MAECI comprend quatre étapes :

- réception des demandes remplies, accompagnées des droits, des pièces d'identité, d'une preuve de citoyenneté et d'autres documents pertinents à un comptoir ou par courrier;
- saisie des données, numérisation des documents et authentification de l'identité et de la citoyenneté;
- vérifications de sécurité pour cerner les risques, contrôle de la qualité et décision quant à l'admissibilité au passeport;
- impression et délivrance des passeports aux demandeurs, en personne ou par courrier.

2.15 Selon les renseignements dont nous disposions au moment de notre vérification, Passeport Canada compte plus de 2 200 employés. Son administration centrale est située à Gatineau (Québec). Le traitement des passeports et les opérations liées aux services s'effectuent dans des points de service situés dans la région de la capitale nationale et dans quatre autres régions administratives : l'Est/le Québec, l'Ontario, le Centre et l'Ouest.

2.16 On retrouve 33 points de service de Passeport Canada au Canada pour servir le public en personne et pour recevoir les demandes de passeport envoyées par la poste. Dans près de 80 % des cas, les demandes de passeport se font en personne, à un comptoir de Passeport Canada, et dans un peu moins de 13 % des cas, par la poste. Les demandes restantes sont traitées par l'entremise d'autres modes de prestation de services, comme les missions, les agents réceptionnaires et le système de passeport en direct.

2.17 Passeport Canada et le Secteur des services consulaires et de la gestion des urgences du MAECI coordonnent la prestation outre-mer des services de passeport aux Canadiennes et Canadiens par l'intermédiaire de 139 missions canadiennes et de plus de 100 bureaux de consul honoraire (pour les titres de voyage d'urgence). Ces missions ont délivré plus de 136 000 passeports en date du 31 mars 2007, ce qui ne représente qu'environ 3,5 % des passeports canadiens délivrés au cours de l'exercice précédent. Bien qu'il ne s'agisse pas d'un volume important, le MAECI a précisé que la prestation de services de passeport à l'étranger est exposée à un risque inhérent élevé.

2.18 Les agents réceptionnaires – la Société canadienne des postes (SCP) et Service Canada (SC) – sont engagés à contrat par Passeport Canada pour recevoir et examiner les demandes de passeport dans plus de 150 points de service situés partout au pays. Leur rôle est de recueillir les droits de traitement et de s'assurer que les demandes sont dûment remplies avant de les acheminer à Passeport Canada pour la détermination de l'admissibilité. L'année dernière, les agents réceptionnaires ont traité l'équivalent de 4,4 % de toutes les demandes de passeport. Ce volume devrait grossir puisque le nombre d'agents réceptionnaires a augmenté de 50 % au cours de la même période.

2.19 Comme les demandeurs de passeport appuient financièrement le programme de passeport au moyen de divers droits de service, on s'attend grandement à ce que Passeport Canada soit en mesure d'offrir un service opportun et de qualité. Dans son Plan d'entreprise 2006-2009, Passeport Canada indique que « son premier impératif […] est de soulager les pressions qui s'exercent sur les zones de services tout en observant de strictes exigences de sécurité ». Ce défi s'est avéré plus difficile à relever puisque Passeport Canada rapporte que les responsabilités en matière de sécurité ont entraîné une hausse des frais de délivrance des passeports et que les droits demandés aux Canadiennes et Canadiens n'ont pas été majorés en conséquence. Passeport Canada a signalé qu'il accuse un déficit budgétaire.

2.20 Le nombre de demandes de passeport a atteint un volume record au Canada en raison des nouvelles règles concernant les voyages aux États-Unis et à la vigueur de l'économie canadienne observée ces dernières années. Passeport Canada a délivré 3,66 millions de passeports en 2006-2007, ce qui représente une hausse de 22 % par rapport à l'exercice précédent.

2.21 Pour relever les défis associés à ce volume sans précédent de demandes de passeport, Passeport Canada a simplifié certains de ses formulaires de demande, modifié et réorganisé ses processus, mis en œuvre de nouvelles technologies et transféré certaines activités.

2.22 Entre avril 2007 et mars 2008, Passeport Canada a embauché 1 257 employés et 494 ont quitté l'organisation. En outre, l'effectif de Passeport Canada est passé de 2 091 employés en novembre 2006 à 3 190 en mars 2008. On nous a informés que cette augmentation record de l'effectif a entraîné une réorientation importante des ressources opérationnelles et de gestion réalisée dans le but d'appuyer la formation et l'encadrement des nouveaux employés. Compte tenu de cette croissance et de ces changements soudains, il est possible qu'à certains moments, les procédures obligatoires n'étaient pas prises en compte dans les tâches quotidiennes. Comme notre vérification s'est déroulée pendant une période marquée par une forte augmentation du volume de demandes de passeport au cours de laquelle une formation était dispensée de façon progressive, il se peut que certains employés observés par l'équipe de vérification ne possédaient pas les connaissances et l'expérience qu'ils possèdent maintenant, alors que leur formation est terminée.

2.23 On peut obtenir des renseignements détaillés sur Passeport Canada en consultant son site Web à www.ppt.gc.ca.

Observations et recommandations

Collecte de renseignements personnels

3.1 L'article 4 de la *Loi sur la protection des renseignements personnels* énonce l'un des principes fondamentaux en matière de protection des renseignements personnels concernant la collecte, à savoir que : « les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités ». Ce principe de base vise à s'assurer que les institutions fédérales ne se livrent pas à des collectes arbitraires de renseignements personnels.

3.2 Le Bureau des passeports a pris l'engagement organisationnel de ne recueillir auprès des demandeurs que les renseignements qui semblent, pour des raisons plausibles, nécessaires à l'application appropriée du *Décret sur les passeports canadiens*.

3.3 Nous avons constaté que les renseignements personnels que Passeport Canada recueille au cours du processus relatif au passeport sont clairement nécessaires à la réalisation de son mandat en vertu du *Décret sur les passeports canadiens*, et que la plupart des renseignements personnels sont recueillis directement auprès des demandeurs, avec leur consentement.

3.4 Les demandeurs de passeport fournissent de nombreux renseignements personnels de nature délicate sur un seul formulaire, qui vont de renseignements de base, comme le nom, l'adresse, les numéros de téléphone et la date de naissance, à des renseignements sur l'emploi et le lieu de résidence, comme les preuves de citoyenneté canadienne, l'information figurant sur les cartes d'identité, les détails liés aux voyages, le numéro de passeport du répondant et sa date d'expiration et/ou l'information sur les références, et l'information relative à la carte de crédit du demandeur. Passeport Canada peut également demander d'autres documents pertinents, comme le passeport précédent.

3.5 D'autres renseignements personnels sur les demandeurs peuvent être recueillis, au besoin, auprès de tierces parties, dont Citoyenneté et Immigration Canada, Service correctionnel du Canada, les registres provinciaux et d'autres organismes de renseignements et d'application de la loi, afin de déterminer l'admissibilité et de protéger l'intégrité du système de passeport. Les formulaires de demande de passeport contiennent également certains renseignements sur les membres de la famille, les répondants et/ou les références.

3.6 En ce qui concerne la question de la collecte, ce qui nous préoccupe le plus est le fait que certains types de renseignements personnels sont recueillis sur un seul formulaire de demande de passeport. Des renseignements personnels de nature délicate, tels que l'information financière, l'information sur le répondant et le numéro d'assurance sociale, peuvent être recueillis, de même que bien d'autres types de renseignements personnels sur le demandeur, comme nous l'avons mentionné plus haut.

3.7 Cette méthode de collecte au moyen d'« un seul formulaire » est probablement d'une grande efficacité lorsqu'il s'agit de traiter des millions de demandes de passeport. Cependant, en rassemblant un vaste éventail de renseignements personnels de nature délicate dans un seul document, on expose les demandeurs à des risques accrus s'il arrivait qu'une personne consulte, utilise, communique, détruise ou modifie le formulaire de demande de façon inappropriée.

3.8 **Numéro d'assurance sociale (NAS).** Les demandeurs doivent fournir l'information figurant sur au moins un des documents énumérés dans les directives du formulaire de demande de passeport à des fins d'identification. Parmi ces documents figurent : le permis de conduire provincial ou la carte relative aux soins de santé ou toute autre pièce d'identité délivrée par un organisme du gouvernement. Selon nos observations, les fonctionnaires de Passeport Canada recueillent le NAS lorsqu'un demandeur l'inscrit dans le formulaire.

3.9 Bien que la carte d'assurance sociale ne soit pas mentionnée comme tel dans la liste des documents acceptables à l'appui de l'identité dans le formulaire de demande de passeport, on pourrait considérer qu'elle tombe dans la catégorie « autre pièce d'identité fédérale, provinciale/territoriale/étatique ou municipale ».

3.10 On nous a informés que bien que Passeport Canada n'encourage pas la collecte du NAS aux fins de vérification de l'identité, il l'accepte si les demandeurs le fournissent.

3.11 Par ailleurs, le Manuel de la politique de Passeport Canada, le manuel sur la formation relative aux passeports du MAECI et les documents de formation en matière de protection de la vie privée fournis par Passeport Canada et le MAECI ne contiennent aucune directive particulière selon laquelle les employés devraient décourager activement les demandeurs d'utiliser leur NAS comme preuve d'identité dans le processus relatif au passeport.

3.12 Le Commissariat s'est publiquement opposé à la collecte routinière du NAS à des fins d'identification lorsque cela n'est pas absolument nécessaire ou expressément prévu par la loi ou par le SCT comme utilisation acceptable. Le NAS n'est pas un type ordinaire de renseignement lié à l'identité. Il est considéré comme l'un des éléments de données clés recherchés par les voleurs d'identité pour commettre des fraudes financières. Par conséquent, la collecte du NAS pose un risque particulièrement élevé lorsque cette information est consignée avec d'autres renseignements permettant d'établir l'identité, comme le nom, l'adresse, la date de naissance et l'information concernant la carte de crédit, des renseignements qui figurent tous dans un formulaire type de demande de passeport.

3.13 La collecte et l'utilisation accrues du NAS dans les secteurs public et privé sont considérées comme d'importants facteurs à l'origine de la forte augmentation du vol d'identité et des crimes connexes liés à la fraude au Canada.

3.14 **Information concernant la carte de crédit.** Des droits sont perçus pour chaque demande de passeport. Les formulaires de demande de passeport, lorsqu'ils sont envoyés par la poste à Passeport Canada, comprennent une section où l'information concernant la carte de crédit est consignée, y compris le nom du titulaire de la carte, le type de carte, son numéro et sa date d'expiration. Lorsque ces renseignements financiers sont fournis, Passeport Canada les conserve dans son système d'information électronique.

3.15 Puisque l'information concernant la carte de crédit d'un demandeur figure, avec le reste de l'information, sur le formulaire de demande, sur supports papier et électronique, pratiquement n'importe quel employé qui participe à la détermination de l'admissibilité ou à la délivrance des passeports pourrait potentiellement y avoir accès. Les employés peuvent consulter cette information financière de nature délicate même s'ils n'en ont pas besoin pour s'acquitter de leurs tâches.

3.16 L'information financière comme un numéro de carte de crédit est considérée comme un renseignement personnel de nature très délicate pour les Canadiennes et les Canadiens. Rappelons que l'information financière, lorsque combinée à des renseignements de base et à un NAS, est un élément d'information clé recherché par les voleurs d'identité et les fraudeurs financiers.

3.17 **Information concernant le répondant.** Nous avons repéré un autre domaine où la méthode de collecte d'information au moyen d'un seul formulaire pourrait entraîner des atteintes à la vie privée. Cela a trait à la nouvelle politique concernant les répondants entrée en vigueur à l'automne 2007.

3.18 En vertu de la nouvelle politique, les personnes qui font une demande de passeport générale pour adultes peuvent maintenant nommer presque n'importe quel adulte détenant un passeport valide (y compris un membre de la famille et une personne résidant à la même adresse) comme répondant, au lieu de choisir parmi une liste restreinte de professionnels, comme c'était le cas auparavant. Les personnes qui sont admissibles au processus de renouvellement simplifié de passeport pour adultes ne sont pas tenues de fournir des renseignements sur le répondant.

3.19 Des demandeurs se tournent encore spontanément vers leur médecin, leur avocat ou un membre du clergé pour assumer le rôle de répondant. Bien que nul ne soit obligé d'accepter d'être répondant, nous avons appris que, compte tenu de leur relation étroite avec le demandeur, ces professionnels trouvent difficile de refuser une telle demande.

3.20 En vertu de la nouvelle politique, les répondants doivent maintenant fournir leur numéro de passeport et sa date d'expiration aux demandeurs. Les demandeurs inscrivent ces renseignements sur leur formulaire de demande avant de le soumettre à Passeport Canada en personne ou par la poste.

3.21 Certaines de ces personnes se sont plaintes au Commissariat d'avoir à fournir ces renseignements personnels de nature délicate directement au demandeur, qui pourrait éventuellement les perdre ou les utiliser de façon inappropriée avant de les soumettre à Passeport Canada.

3.22 Nous reconnaissons qu'il est important pour Passeport Canada, du point de vue des opérations, de recueillir des renseignements de la façon la plus efficace possible. Cependant, ce besoin d'efficacité doit être mis en balance avec le besoin d'assurer la protection des renseignements personnels des Canadiennes et des Canadiens.

3.23 Recommandation : Passeport Canada devrait explorer des options quant à la meilleure façon de recueillir l'information financière des demandeurs et les données personnelles des répondants de manière à ne pas nuire indûment au processus relatif au passeport, tout en prenant en considération la vie privée de ces personnes. Il devrait également modifier ses documents sur la formation et les politiques de façon à limiter la collecte du NAS, tout en encourageant activement les demandeurs à utiliser d'autres formes d'identification qui posent moins de risque pour la vie privée.

Réponse de la direction (Passeport Canada) : D'accord. Passeport Canada a commencé l'examen de ses pratiques de collecte d'information pour cibler davantage la collecte des renseignements essentiels quand il s'agit d'évaluer l'admissibilité du client à un titre de voyage. Passeport Canada examinera et modifiera les lignes directrices et les documents de formation en ce qui concerne les pratiques liées à la collecte, à l'utilisation et à la communication des renseignements personnels dans le but particulier de dissuader les clients d'inscrire leur NAS en tant qu'élément d'identification. Passeport Canada créera aussi des normes et des outils applicables à des pratiques de collecte d'information conformes aux exigences opérationnelles et aux pratiques recommandées énoncées par la commissaire à la protection de la vie privée. La mise en œuvre de ces initiatives est prévue pour 2009-2010.

Contrôle de la consultation, de l'utilisation et de la communication des renseignements personnels

3.24 **Consultation et utilisation des renseignements personnels.** Comme nous l'avons mentionné précédemment dans le présent rapport, les renseignements relatifs au passeport portent la mention « Protégé B » et sont décrits par Passeport Canada comme étant « de nature particulièrement délicate » [des renseignements pour lesquels toute atteinte à l'intégrité risquerait de causer un préjudice grave à des personnes]. Par conséquent, nous nous attendions à ce que Passeport Canada applique le principe du « besoin de connaître » de façon uniforme et mette en œuvre des mesures pour limiter l'accès des employés à cette information.

3.25 Pour protéger les renseignements personnels, il convient d'en limiter l'accès aux employés qui en ont besoin pour s'acquitter de leurs tâches. L'accès électronique à ces renseignements aux fins de consultation, de modification, de copie ou de suppression devrait également être limité en fonction du même principe du « besoin de connaître » pour les systèmes des TI de sorte que le plus petit nombre de personnes possible y ait accès sans que cela ne nuise aux exigences opérationnelles. Le principe du « besoin de connaître » et ses mesures de contrôle connexes concourent à atténuer les risques d'utilisation ou de communication inappropriée des renseignements par un employé, ainsi que les risques subséquents pour la personne concernée par les renseignements.

3.26 Diverses mesures de sécurité administratives, matérielles et techniques sont généralement utilisées pour contrôler l'accès aux renseignements personnels.

3.27 Au cours de notre vérification, nous avons évalué la mesure dans laquelle le droit d'accès aux renseignements relatifs au passeport dont disposent les employés de Passeport Canada et des (<<Services consulaires>>) dans les missions cadre bien avec leurs rôles et leurs responsabilités. Bien qu'en général, nous soyons convaincus que les privilèges d'accès particuliers accordés par Passeport Canada et le MAECI sont conformes au rôle et aux responsabilités des employés, nous avons relevé des problèmes à ce chapitre.

3.28 Dans une mission à l'étranger, nous avons découvert que du personnel de niveau supérieur avait communiqué son mot de passe et son nom de connexion à des subalternes. Par conséquent, ces employés pouvaient consulter des renseignements dans le système sans y être autorisés. Dans un autre cas, un employé qui avait pris sa retraite plus de six mois auparavant détenait toujours des droits d'accès à un système

consulaire. D'autres employés disposaient de droits d'accès alors que leur travail ne touchait en aucune façon au processus relatif au passeport. D'autres encore figuraient sur une liste d'accès bien qu'ils ne détenaient plus de droits. Cela laisse supposer que la liste d'accès n'était pas mise à jour régulièrement dans certaines missions en fonction des changements survenus dans le personnel et dans le rôle des employés au regard du processus relatif au passeport.

3.29 Bien que les deux organisations doivent avoir la capacité de modifier rapidement les droits d'accès pour répondre à des exigences opérationnelles soudaines ou inattendues, les employés ne devraient pas figurer sur des listes d'accès simplement « au cas où » une situation d'urgence surviendrait.

3.30 Nous avons également constaté qu'aucune unité centrale au MAECI ou à Passeport Canada, comme le centre d'assistance en TI, n'est pleinement responsable de voir à ce que les droits d'accès à l'information dans les systèmes des TI tiennent compte de l'effectif actuel et du rôle des employés. Le système et le processus de mise à jour des droits d'accès reposent en grande partie sur l'information communiquée au centre d'assistance par les gestionnaires et les superviseurs relativement aux changements survenus dans les fonctions de leurs employés ou aux départs temporaires ou permanents de leurs employés. Les TI s'en tiennent à des vérifications ponctuelles de ces listes et les services des Ressources humaines des deux organisations ne jouent pas un rôle actif dans la communication aux TI des changements survenus dans l'effectif, que les gestionnaires ou les superviseurs auraient pu avoir oublié de mentionner. Le résultat final est que le système de contrôle décentralisé actuel ne peut pas toujours garantir de façon efficace que des droits d'accès aussi importants en matière de TI sont tenus à jour.

3.31 Si les droits d'accès devraient être fondés sur le rôle et les fonctions des employés, l'accès à des renseignements précis devrait être fondé sur les besoins opérationnels démontrés. Au cours de notre vérification des missions à l'étranger, nous avons constaté que le personnel consulaire avait accès à beaucoup plus de renseignements relatifs au passeport que ce dont il avait besoin pour s'acquitter de ses tâches quotidiennes. Les renseignements auxquels les fonctionnaires consulaires avaient accès dans le système PMP du MAECI ne se limitaient pas aux formulaires remplis à la mission où ils travaillent, mais également à tous les dossiers des autres missions à l'étranger. Autrement dit, n'importe quelle mission peut consulter des renseignements sur les passeports recueillis par n'importe quelle autre mission. Par exemple, le personnel de la mission à Paris peut consulter des formulaires de demande de passeport remplis à Beijing, à Los Angeles, à Mexico ou à Moscou, et vice-versa.

3.32 Nous avons constaté que les sections consulaires avaient rarement besoin de consulter ces renseignements et qu'ils pourraient les obtenir, au besoin, auprès du MAECI ou de Passeport Canada.

3.33 Nous avons aussi constaté qu'il existe un journal de vérification électronique pour les demandes de passeport en cours de traitement (c.-à-d. les travaux en cours [TC]) par Passeport Canada et pour toute modification apportée aux formulaires remplis. Cependant, une fois que les dossiers TC sont transférés dans les dossiers du fichier central IRIS et dans le fonds permanent, les pistes de vérification des TC sont effacées. Nous avons constaté que le fichier central IRIS et les fonds permanents du système PMP ne sont pas munis d'un mécanisme permettant de savoir quand une personne a consulté un formulaire de passeport rempli.

3.34 Les pistes de vérification sont des mécanismes de contrôle de base des systèmes des TI qui permettent de s'assurer que les utilisateurs autorisés n'abusent pas de leurs droits d'accès en consultant des renseignements personnels à des fins autres que celles liées à leur travail. Nous avons été surpris de constater que de tels mécanismes de sécurité ne sont pas en place pour savoir qui a consulté les formulaires de passeport remplis dans le système PMP du MAECI ou dans le système IRIS de Passeport Canada.

3.35 Plus loin, dans la section du présent rapport portant sur les mesures de sécurité, nous exposerons dans le détail les risques pour la sécurité associés au fait que les renseignements électroniques sur les passeports ne sont pas stockés dans les systèmes PMP et IRIS sous une forme chiffrée. Ces lacunes en matière de sécurité de l'information, qui s'ajoutent aux problèmes liés aux droits d'accès et aux pistes de vérification que nous venons de mentionner, pourraient exposer les renseignements relatifs au passeport des Canadiennes et des Canadiens à un risque plus important.

3.36 ***Recommandation : Passeport Canada et le MAECI devraient prendre ensemble les mesures qui s'imposent pour contrôler l'accès des employés aux renseignements personnels. Ces mesures devraient tenir compte de la désignation « Protégé B » de ces renseignements, respecter le principe du besoin de connaître et comprendre des pistes de vérification électroniques pour les systèmes IRIS et PMP afin de réduire les risques d'accès inapproprié aux renseignements personnels.***

Réponse de la direction (MAECI) : D'accord. Le MAECI a mis en œuvre des journaux de transactions en mai 2008 pour l'ouverture de session lorsqu'un employé a consulté certains éléments de l'application de la demande de services consulaires. Ces capacités seront encore perfectionnées dans un proche avenir.

Le MAECI et Passeport Canada travailleront aussi de concert de sorte que les systèmes PMP et IRIS aient les programmes et les mesures de sécurité voulus pour réduire les risques d'accès inapproprié aux renseignements personnels.

Réponse de la direction (Passeport Canada) : D'accord. En 2007-2008, Passeport Canada a mené à bien un examen et un remaniement de tous les profils d'utilisateurs du système IRIS de manière à refléter avec plus d'exactitude le « besoin de savoir ». De plus, le nouvel outil d'entrée de données qui sera mis en œuvre pendant le présent exercice sera doté de capacités d'ouverture de session plus perfectionnées pour le système IRIS et sera lié au système de profils IRIS. Le MAECI et Passeport Canada travailleront aussi de concert de sorte que les systèmes PMP et IRIS aient les programmes et les mesures de sécurité voulus pour réduire les risques d'accès inapproprié aux renseignements personnels.

3.37 **Impartition de la fonction « retour par la poste » à la Société canadienne des postes (SCP).** Selon les conditions d'un contrat conclu avec Passeport Canada, la SCP a la responsabilité de ramasser les demandes de passeport incomplètes et les documents à l'appui à l'administration centrale de Passeport Canada et de les apporter à l'une de ses installations à Ottawa. Elle vérifie alors le contenu de chaque dossier et renvoie l'information aux demandeurs.

3.38 Nous avions des préoccupations quant à la façon dont ces documents étaient transportés (dans des sacs de plastique transparents et des contenants ouverts) aux installations de la SCP en vertu de son contrat. Nous nous inquiétions également du fait que les employés de la SCP avaient accès aux formulaires de demande complets et aux documents à l'appui, y compris les renseignements personnels de nature délicate qu'ils contenaient.

3.39 Nous avons écrit à Passeport Canada le 28 juin 2007 au sujet de cette entente d'impartition. Passeport Canada a fourni une réponse initiale le 5 septembre 2007, suite à quoi nous avons rédigé le 18 février 2008 une autre lettre soulevant des préoccupations additionnelles. Le 14 mars 2008, Passeport Canada a avisé le Commissariat qu'à compter du 1er avril 2008, il reprendrait en main toutes les activités liées au retour par la poste des demandes de passeport rejetées.

Mesures appropriées de conservation et d'élimination des renseignements personnels

3.40 La *Loi sur la protection des renseignements personnels* adopte une approche de protection des renseignements personnels axée sur le cycle de vie (les renseignements sont recueillis et communiqués à des fins administratives et doivent être éliminés de façon sécuritaire lorsqu'ils ne sont plus nécessaires à la réalisation de ces fins).

3.41 En vertu de la *Loi sur la Bibliothèque et les Archives du Canada*, les institutions fédérales doivent établir des calendriers de conservation et d'élimination qui précisent la période pendant laquelle les renseignements organisationnels (y compris les renseignements personnels) peuvent être conservés avant d'être détruits ou archivés.

3.42 Nous avons examiné les procédures de conservation et d'élimination des dossiers sur supports papier et électronique contenant des renseignements personnels à Passeport Canada et dans les bureaux des agents réceptionnaires au Canada, ainsi que dans les sections consulaires des missions à l'étranger du MAECI.

3.43 **Conservation.** À Passeport Canada, les demandes et les dossiers de passeport sur support papier sont généralement conservés pour une période d'environ six semaines après qu'ils ont été traités, après quoi ils sont détruits. Les documents originaux soumis à titre de preuve de citoyenneté canadienne sont renvoyés aux demandeurs. Les passeports périmés ou annulés, qui ne sont pas renvoyés aux demandeurs, sont annulés et détruits peu de temps après la délivrance du nouveau passeport.

3.44 Au MAECI, les formulaires de demande de passeport remplis dont Passeport Canada n'a pas besoin sont conservés pour une période de 90 jours à compter de la fin du mois au cours duquel la demande a été traitée. Les demandes et tous les documents et photographies connexes devraient ensuite être déchiquetés au moyen de destructeurs de documents avec coupe en travers approuvés.

3.45 Cependant, la version électronique et les copies microfilmées (produites avant 2002) des renseignements relatifs au passeport à Passeport Canada et les fichiers électroniques au MAECI peuvent être conservés pour une période allant jusqu'à 100 ans.

3.46 Passeport Canada conserve les renseignements électroniques sur les passeports dans deux grandes bases de données, l'une située dans la région du Grand Toronto et l'autre, dans la région de la capitale nationale. Ces deux bases de données réunies contiennent une masse critique de plus de 30 millions de demandes de passeport présentées par des

Canadiennes et des Canadiens. Comme nous l'avons mentionné précédemment, il s'agit d'information de nature particulièrement délicate.

3.47 Les nombreux renseignements relatifs au passeport recueillis chaque année auprès de millions de Canadiennes et de Canadiens constituent les principales ressources d'information dont Passeport Canada a besoin pour assurer l'intégrité du processus relatif au passeport et pour délivrer des passeports à des Canadiennes et à des Canadiens légitimes de façon opportune.

3.48 Mais tant et aussi longtemps que ces renseignements de nature particulièrement délicate sur les passeports sont conservés par Passeport Canada, ces renseignements présentent un risque pour l'organisation du fait qu'ils pourraient éventuellement être consultés ou utilisés de façon inappropriée pendant qu'ils sont sous sa garde.

3.49 D'après des discussions avec des fonctionnaires de Passeport Canada, la raison pour laquelle les renseignements relatifs au passeport sont conservés pour une période allant jusqu'à 100 ans n'est pas claire. Cette période semble être plus longue que nécessaire pour répondre aux besoins administratifs et liés aux programmes de Passeport Canada et pose des risques inutiles pour les renseignements relatifs au passeport des Canadiennes et des Canadiens du simple fait qu'ils sont là.

3.50 ***Recommandation : Étant donné les risques inhérents associés à la conservation des renseignements relatifs au passeport pour une période de 100 ans, et compte tenu des exigences de la* Loi sur la protection des renseignements personnels *selon lesquelles les renseignements personnels ne doivent être conservés qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées ou selon les dispositions des règlements, Passeport Canada devrait consulter Bibliothèque et Archives Canada en vue de réévaluer cette période anormalement longue de conservation des dossiers.***

Réponse de la direction (Passeport Canada) : D'accord. La période de conservation pour les renseignements relatifs au passeport a été revue pour être portée 100 ans en décembre 2006 : une période d'activité de 12 ans, suivie d'une période d'inactivité de 88 ans avant le transfert à Bibliothèque et Archives Canada. La période d'inactivité de 88 ans permet la conservation des antécédents du client en matière de passeport, ce qui est essentiel pour la vérification de l'identité et de l'admissibilité constante à un passeport. Passeport Canada reverra cette période de conservation au cours des trois prochaines années puisque les nouveaux programmes et nouvelles technologies, comme le processus simplifié de renouvellement du passeport et la reconnaissance faciale, pourraient influer sur les périodes de conservation et d'élimination des demandes de passeport.

3.51 **Élimination.** Nous avons décelé des lacunes en ce qui a trait au transport et à la destruction des données personnelles conservées sur supports papier et électronique (p. ex. disques durs et autres supports d'enregistrement de données). Le transport des renseignements relatifs au passeport entre Passeport Canada et la Société canadienne des postes, comme nous l'avons mentionné précédemment, est un exemple du type de risque que pose le transfert d'un lieu physique à un autre de renseignements personnels de nature délicate.

3.52 Dans un certain nombre de bureaux de Passeport Canada et de missions à l'étranger, des formulaires de demande de passeport contenant des renseignements personnels, comme le nom et la date de naissance du demandeur, ont été retrouvés dans des poubelles et des bacs de recyclage ordinaires sans avoir été déchiquetés. Dans un bureau de Service Canada (SC)[2], la destruction des renseignements relatifs au passeport avait été impartie à un entrepreneur du secteur privé. Lorsque nous avons rendu visite à cet entrepreneur, nous avons découvert que Service Canada ne supervisait pas de façon systématique le transport et la destruction des dossiers de passeport de nature délicate.

3.53 Nous avons également constaté que même une fois que les documents avaient été apparemment déchiquetés, des photos de passeport demeuraient intactes et d'autres renseignements relatifs aux demandes de passeport pouvaient facilement être reconstitués et rendus lisibles, ce qui les exposait à un accès ou à une utilisation inappropriée.

3.54 Comme le risque est toujours plus élevé lorsque les renseignements sont transportés à l'extérieur du site pour être détruits, l'élimination sur place devrait être l'option privilégiée dans la mesure du possible. En ne transportant pas de dossiers personnels à l'extérieur du site et en veillant à ce que la destruction physique se fasse dans un endroit sécurisé par des employés du gouvernement, une organisation gouvernementale peut avoir une assurance plus élevée que les renseignements personnels des Canadiennes et des Canadiens sont correctement protégés.

3.55 Cela ne veut pas dire que l'on ne peut pas confier la tâche de destruction des dossiers à un entrepreneur, mais cette option exige la mise en place de contrôles rigoureux (p. ex. la surveillance, la tenue de dossiers et le contrôle de la qualité) pour atténuer les risques plus élevés associés à une telle pratique.

3.56 En plus des demandes de passeport sur support papier que Passeport Canada entrepose, l'organisation conserve également une grande quantité de données informatiques dans ses installations. Un important disque dur ou une importante bande de sauvegarde informatique pourrait potentiellement contenir des dossiers de passeport de millions de Canadiennes et de Canadiens.

3.57 Lorsque les ordinateurs et l'information qu'ils contiennent sont arrivés à la fin de leur cycle de vie utile, ils doivent être détruits selon une méthode sécuritaire en fonction d'une évaluation de la menace et des risques pour la vie privée et pour la sécurité.

3.58 Passeport Canada a une politique sur la sécurité des TI qui explique clairement comment les appareils de stockage des renseignements électroniques doivent être éliminés et détruits. Cette politique stipule que les bandes de sauvegarde et les disques durs doivent être remis au personnel des TI à l'administration centrale de Passeport Canada, qui utilise des procédures approuvées par le gouvernement pour détruire les données en les rendant illisibles et inaccessibles. Selon cette politique, le personnel du Centre de protection de l'information doit prendre les arrangements nécessaires avec le client pour le ramassage ou la livraison du matériel si celui-ci se trouve à l'administration centrale. Tout matériel remis à l'administration centrale par les bureaux régionaux doit être envoyé par courrier sécurisé.

[2] Service Canada et la Société canadienne des postes ont conclu des ententes avec Passeport Canada pour la prestation de services limités de passeport au public en de nombreux points de service aux quatre coins du pays.

3.59 Au moment de la vérification, nous avons découvert que les bureaux régionaux de Passeport Canada recouraient à des services de messagerie commerciaux pour expédier leur matériel informatique excédentaire à l'administration centrale. En relisant la documentation, nous avons constaté que plusieurs importantes atteintes à la vie privée sont survenues ailleurs ces dernières années dans les secteurs public et privé dans des cas où l'on avait confié à des messagers le soin de transporter d'un bureau à l'autre des disques durs et d'autres appareils de stockage contenant des renseignements personnels de nature délicate.

3.60 ***Recommandation : Passeport Canada devrait évaluer les risques pour la vie privée et la sécurité que posent ses pratiques actuelles d'élimination et/ou de destruction des renseignements personnels de nature délicate, et ce, pour tous les types de dossiers.***

Réponse de la direction (Passeport Canada) : D'accord. La Division des dossiers de l'entreprise de Passeport Canada élimine et détruit les renseignements délicats contenus dans tous les types de documents, conformément à la Politique du gouvernement sur la sécurité. De plus, Passeport Canada a mis en œuvre des procédures d'expurgation et de destruction des médias de nature délicate. Passeport Canada travaillera en collaboration avec le MAECI et Service Canada pour définir les mesures appropriées de collecte et d'élimination des renseignements relatifs au passeport.

Mesures de sécurité essentielles

3.61 Dans l'important préambule à la *Loi sur la protection des renseignements personnels*, on mentionne que la *Loi* a pour objet « de compléter la législation canadienne en matière de protection des renseignements personnels ». Les articles 4 à 8 de la *Loi* stipulent également que les renseignements personnels ne peuvent être recueillis, utilisés ou communiqués qu'à des fins administratives, à moins de dispositions contraires dans les règlements. Par conséquent, la sécurité et la protection des renseignements personnels sont importantes pour répondre aux attentes énoncées dans la *Loi* à cet égard.

3.62 La Politique du gouvernement sur la sécurité et d'autres directives connexes précisent quel type de mesures de sécurité convient à l'information compte tenu de sa nature délicate et des répercussions que toute atteinte à l'intégrité aurait sur le gouvernement et/ou les citoyens.

3.63 Passeport Canada et le MAECI (« Services consulaires ») ont adopté une approche multidimensionnelle et holistique à l'égard de la sécurité de l'information qui est conçue pour protéger les dossiers de passeport de nature délicate des Canadiennes et des Canadiens et pour limiter les menaces et les risques connus auxquels ces dossiers sont exposés. Cette approche comprend des éléments liés à la sécurité matérielle et administrative et à la sécurité du personnel et des TI, qui, combinés, offrent généralement une protection adéquate des renseignements personnels. Malgré ces mesures de sécurité, nous avons décelé d'importantes lacunes dans les contrôles internes, qui pourraient se traduire par une perte ou par une utilisation ou une communication inappropriée de renseignements personnels. Certaines de ces lacunes ont été abordées précédemment comme elles étaient liées à des questions que nous traitions et d'autres sont mentionnées plus loin.

3.64 **Sécurité matérielle.** Les mesures de sécurité matérielle comprennent, sans s'y limiter, le verrouillage des portes et des armoires, l'utilisation de systèmes d'alarme effraction et de gardiens de sécurité et le contrôle des zones d'accès restreint. Les mesures de sécurité matérielle aident à protéger les renseignements personnels en empêchant les membres du public et du personnel qui n'ont pas besoin de consulter ces renseignements de pénétrer dans les secteurs opérationnels où les renseignements personnels sont recueillis et traités.

3.65 Les bureaux de Passeport Canada et du MAECI que nous avons visités semblent avoir des mesures de sécurité matérielle adéquates pour empêcher les personnes de l'extérieur d'avoir accès aux renseignements relatifs au passeport. Bien qu'une telle protection périmétrique soit importante, il est tout de même nécessaire d'entreposer convenablement les renseignements personnels de nature délicate et d'en limiter l'accès à l'intérieur des bureaux.

3.66 Comme nous l'avons mentionné précédemment, les renseignements relatifs au passeport sont de nature particulièrement délicate. Compte tenu de la nature et de la concentration des renseignements personnels relatifs au passeport détenus dans les bureaux de Passeport Canada et des missions du MAECI à l'étranger, ces renseignements devraient être considérés comme les plus sensibles de la catégorie « Protégé B » et pourraient nécessiter une protection additionnelle allant au-delà de celle offerte aux renseignements « Protégé B » de nature moins délicate.

3.67 L'un des problèmes de sécurité matérielle interne communs que nous avons observés dans presque tous les bureaux de Passeport Canada et des missions du MAECI visités a trait à la façon dont les dossiers de passeport et les documents à l'appui étaient entreposés. Comme nous l'avons mentionné précédemment, les demandes de passeport et les documents à l'appui étaient entreposés dans des sacs de plastique transparents de type Ziplock. Ces dossiers de nature délicate demeurent dans ces sacs du moment qu'ils sont reçus à Passeport Canada, dans les missions et aux bureaux des agents réceptionnaires jusqu'à ce que les passeports soient délivrés aux demandeurs. Pour le MAECI, cette observation de vérification s'applique aux cinq missions qui ont été visitées à Beijing, Berne, Los Angeles, Paris et Taipei.

3.68 Nous avons deux inquiétudes concernant cette pratique. Premièrement, tout employé qui détient un droit d'accès physique aux installations pourrait voir des renseignements personnels de nature délicate à travers les sacs de plastique transparents. Deuxièmement, l'entreposage des documents relatifs au passeport, y compris des documents à l'appui originaux et des passeports périmés et nouveaux, sur des étagères ouvertes ou dans des contenants sans couvercle est inadéquat, car tout employé détenant un droit d'accès physique pourrait les consulter ou les utiliser de façon inappropriée, ou les prendre, les communiquer ou les détruire.

3.69 Par ailleurs, on nous a informés que si un lot de formulaires de demande de passeport remplies disparaissait des bureaux de Passeport Canada ou des missions, les fonctionnaires n'auraient aucune façon de le savoir puisqu'ils ne surveillent pas ces documents une fois les passeports délivrés. Bien que ces dossiers ne soient plus nécessaires à des fins administratives une fois les passeports délivrés, ils doivent toujours être protégés compte tenu des renseignements de nature délicate qu'ils contiennent.

3.70 Nous avons également constaté, dans plusieurs bureaux de Passeport Canada et des missions à l'étranger, que des télécopies et des courriels contenant des renseignements personnels étaient entreposés dans des contenants ouverts pendant la nuit.

3.71 Il importe de noter que certains bureaux de Passeport Canada et sections consulaires gardaient les dossiers de passeport sous clé pendant la nuit, bien que la majorité des bureaux visités ne le faisait pas. Même les bureaux qui disposent de classeurs verrouillables ne rangeaient pas systématiquement les dossiers dans ces classeurs.

3.72 L'équipe de vérification a également constaté que dans un certain nombre de sections consulaires à l'étranger, les employés qui ne travaillaient pas dans ces sections pouvaient néanmoins y avoir accès et que ces employés accompagnaient parfois un membre du public qui demandait des services de passeport. On nous a assurés que des employés consulaires étaient toujours présents lorsque ces « visiteurs » se trouvaient dans la section consulaire. Toutefois, ces personnes pourraient potentiellement voir ou consulter des renseignements de nature délicate relatifs au passeport, y compris des passeports périmés et nouveaux, des pièces d'identité originales et des formulaires de demande entreposés dans des sacs transparents et des contenants à découvert et sur des étagères ouvertes. Pendant notre examen, aucune raison ne nous a été fournie pour expliquer pourquoi ces demandeurs ne pourraient pas être servis au comptoir de service au public situé à l'extérieur de la section de traitement consulaire.

3.73 Nous avons relevé des cas semblables où des personnes détenaient un accès physique inapproprié à des installations dans certains bureaux de Passeport Canada. Des gardiens de sécurité avaient un accès régulier à certaines zones de traitement de Passeport Canada où des renseignements personnels étaient bien en vue sur des bureaux et des étagères ouvertes, alors que leur travail n'exigeait pas un tel accès, sauf si un incident de sécurité survenait. De même, certains préposés au nettoyage, qui n'avaient apparemment pas la cote de sécurité, disposaient d'un accès sans escorte aux installations de Passeport Canada.

3.74 Un autre aspect important des mesures de sécurité matérielle internes a trait à la conception et à la disposition des installations où les clients sont servis. Nous avons constaté que dans certains bureaux de Passeport Canada et des agents réceptionnaires, ces installations n'étaient pas conçues de façon à assurer une distance acceptable entre les clients de sorte que leurs conversations puissent demeurer confidentielles au comptoir de service. Dans ces bureaux, les conversations pouvaient aisément être entendues par d'autres personnes. Dans certains points de service visités, les clients auraient pu se tourner de côté ou regarder par-dessus l'épaule d'autres clients pour voir leurs renseignements personnels.

3.75 En ce qui concerne la disposition de nombreux secteurs de service à la clientèle consulaires dans les missions du MAECI visitées, nous avons observé un manque d'uniformité dans le niveau d'intimité physique offert aux clients. La disposition de certaines salles d'attente publiques était excellente, tandis que celle d'autres salles l'était beaucoup moins. Par exemple, la salle d'attente de la mission à Taipei était bien conçue du point de vue de la protection de la vie privée et pourrait servir de modèle à d'autres bureaux.

3.76 Les zones de service au public dans certaines missions, comme celles établies à Beijing et à Paris, posent plusieurs problèmes au chapitre de la protection de la vie privée des clients. Nous avons constaté que le MAECI avait prévu des pièces fermées séparées dans ces endroits pour assurer la confidentialité des discussions entre le personnel consulaire et les clients. Toutefois, la conception de ces pièces semblait au contraire amplifier les conversations privées des clients avec le personnel consulaire. En outre, l'organisation prévue pour les clients qui attendaient sur des chaises ou en ligne ne

permettait pas d'assurer une distance acceptable entre le client qui était servi au comptoir et ceux qui attendaient derrière.

3.77 Si dans certains cas, ces problèmes ne peuvent être facilement corrigés en raison de la disposition physique des bureaux, dans d'autres cas, des modifications mineures pourraient être apportées pour améliorer la protection de la vie privée des clients.

3.78 Il importe de noter que dans plusieurs bureaux de missions visités, les fonctionnaires ont pris des mesures correctives immédiates pour améliorer la protection de la vie privée de leurs clients lorsque nous leur avons fait part de nos observations au moment de notre vérification. On nous a également informés que d'autres mesures seront prises pour améliorer davantage la protection de la vie privée des demandeurs dans les salles d'attente publiques.

3.79 ***Recommandation : Passeport Canada et le MAECI devraient s'assurer que leurs dossiers sur support papier contenant des renseignements relatifs au passeport sont entreposés de façon appropriée pour des renseignements « Protégé B » de nature particulièrement délicate conformément à la Politique du gouvernement sur la sécurité.***

Réponse de la direction (MAECI) : D'accord. Le MAECI fournit des contenants de sécurité adéquats pour l'entreposage des renseignements « Protégé B », conformément à la Politique du gouvernement sur la sécurité. Cette pratique est réévaluée à l'occasion d'inspections de sécurité de routine. Lorsque les conteneurs ne sont plus jugés adéquats, des dispositions sont prises pour leur remplacement par d'autres plus appropriés. De plus, les marches à suivre pour l'entreposage des documents sont revues avec le gestionnaire compétent.

Réponse de la direction (Passeport Canada) : D'accord. Les mesures de sécurité matérielle, comme l'accès et les contrôles électroniques, les niveaux d'autorisation de l'accès, le zonage de sécurité dans la conception et l'aménagement des bureaux de Passeport Canada et l'existence de systèmes (systèmes vidéo de surveillance électronique) installés en des points stratégiques dans chaque bureau réduisent les risques de perte, de vol, de destruction et de compromission des renseignements personnels. Passeport Canada continuera à veiller à ce que les dossiers sur support papier contenant des renseignements relatifs au passeport soient protégés comme il se doit contre les risques et les menaces déterminés grâce à des examens de la sécurité matérielle et des vérifications de la conformité menés régulièrement et à la prestation d'une formation sur la protection des renseignements personnels et d'une sensibilisation à la sécurité. Les dossiers de renseignements relatifs au passeport qui doivent être conservés sur support papier sont entreposés dans la zone de sécurité « Protégé B » avec un accès restreint, conformément à la Politique du gouvernement sur la sécurité.

3.80 ***Recommandation : Passeport Canada et le MAECI devraient revoir leurs mesures de sécurité matérielle et leurs autres mesures de sécurité pour s'assurer que l'accès aux endroits où les passeports sont traités n'est accordé qu'aux personnes qui en ont besoin pour s'acquitter de leurs tâches.***

Réponse de la direction (MAECI) : D'accord. Dans les missions à l'étranger, le MAECI veille à ce que l'accès aux aires de traitement des passeports soit contrôlé par un éventail de mesures : l'employé(e) doit avoir subi la vérification de sécurité qui s'impose et reçoit les codes électroniques nécessaires pour accéder aux lieux. Les gestionnaires et les employés compétents reçoivent de l'information sur les protocoles et les mesures à suivre. Ces procédures sont revues à l'occasion des inspections des missions.

Réponse de la direction (Passeport Canada) : D'accord. Les évaluations et examens des risques de la Section de la sécurité matérielle de Passeport Canada sont prévus pour certains bureaux chaque année de manière à veiller à ce que les mesures voulues soient appliquées pour la protection des biens en fonction des risques et menaces déterminés. Les mesures de sécurité matérielle, comme l'accès et les contrôles électroniques, les niveaux d'autorisation de l'accès, le zonage de sécurité dans la conception et l'aménagement des bureaux de Passeport Canada et l'existence de systèmes (systèmes vidéo de surveillance électronique) installés en des points stratégiques dans chaque bureau accroissent la sécurité de sorte que seuls les employés qui doivent, pour les besoins du service, avoir accès aux lieux de traitement des passeports y entrent. Passeport Canada continuera de surveiller et d'évaluer le respect et l'efficacité de ses mesures de sécurité matérielle.

3.81 ***Recommandation : Passeport Canada et le MAECI devraient revoir la disposition et l'acoustique de toutes les zones de service au public pour fournir un niveau adéquat de protection de la vie privée à leurs clients au moyen d'une signalisation et de barrières visuelles et acoustiques appropriées.***

Réponse de la direction (MAECI) : D'accord. Au cours des inspections de sécurité, le MAECI revoit l'aménagement et l'acoustique des zones de service au public. Dans la mesure du possible, les lieux sont reconfigurés, si nécessaire. Ce processus est constant, et les zones les plus à risques sont traitées en premier.

Réponse de la direction (Passeport Canada) : D'accord. Les normes d'aménagement en vigueur à Passeport Canada, qui sont approuvées par TPSGC, prévoient des caractéristiques permettant d'assurer la norme de protection de la vie privée qui s'applique à tous les organismes de la fonction publique offrant des services au comptoir au public. Lorsque les bureaux de Passeport Canada sont relocalisés ou rénovés, selon un échéancier maximal de 10 ans, des éléments supplémentaires et plus perfectionnés liés à la protection de la vie privée sont ajoutés dans les plans d'aménagement.

3.82 **Enquête de sécurité sur le personnel.** Même si le fait qu'une cote de sécurité ait été accordée à un employé ne suffit pas à garantir la fiabilité de ce dernier, il s'agit d'un outil de filtrage utile et objectif qui permet de veiller à ce que les personnes ayant un casier judiciaire ou dont on peut douter de la fiabilité ne soient pas embauchées dans un poste de confiance où elles seront appelées à traiter les renseignements personnels de nature délicate des Canadiennes et Canadiens.

3.83 Le niveau de sécurité de base du personnel pour les employés appelés à traiter des renseignements protégés est la « Fiabilité » et nécessite la conduite d'une vérification du casier judiciaire ainsi que d'autres vérifications fondamentales.

3.84 Selon la *Norme sur la sécurité du personnel* du Conseil du Trésor, « L'enquête de sécurité du personnel doit correspondre à la plus élevée des mentions de sécurité accordées aux renseignements et aux biens ». Un rapport de Passeport Canada sur les services de passeport fournis dans les missions canadiennes à l'étranger indique (traduction libre) : « Les stocks de passeport représentent un élément de sécurité nationale et ont la cote "Secret" ». De plus, le Guide de classification de l'information fourni par Passeport Canada dans le cadre de la présente vérification définit « les documents servant à la production de passeports (par ex. les livrets de passeport vierges) » comme des renseignements protégés au niveau « Secret ». Normalement, ces dispositions devraient signifier que les employés appelés à traiter les livrets de passeport vierges devraient avoir la cote de sécurité « Secret ».

3.85 Le MAECI nous fait savoir qu'il avait instauré dans les missions à l'étranger des marches à suivre limitant l'accès aux renseignements « Protégés B » aux employés ayant subi une vérification de la fiabilité, dont le « besoin de savoir » est avéré et ayant reçu l'autorisation de leur gestionnaire de programme (par ex. fonctionnaire consulaire EC) et de l'agent de sécurité de la mission. Les employés recrutés sur place ont accès aux passeports vierges d'urgence et temporaires et produisent les passeports requis sous la surveillance et la vigilance étroites d'un agent canadien à l'étranger ayant l'autorisation de sécurité voulue, selon des procédures très strictes. Les procédures en question sont revues à l'occasion des vérifications de sécurité des missions. Nous n'avons pas vérifié cette affirmation.

3.86 Les processus d'enquête sur la sécurité « Secret » et « Très secret » supposent la collecte de renseignements plus exhaustifs auprès de l'intéressé(e) ainsi qu'un examen plus approfondi des renseignements détenus à son sujet par la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS) que la simple vérification de la fiabilité. Nous avons cependant appris que le SCRS participe au processus d'enquête pour les employés recrutés sur place dans les missions., bien que le type d'enquête menée par le SCRS pour le compte du MAECI n'ait pas été défini.

3.87 En vue de la mise en place, par le SCT, de lignes directrices en matière de sécurité du personnel plus strictes, Passeport Canada a rehaussé le niveau d'enquête de sécurité sur le personnel exigé pour ses employés des opérations, le faisant passer du niveau de base « Fiabilité » au niveau « Secret ». Or, un grand nombre d'employés consulaires, y compris la plupart des employés recrutés sur place et les employés des agents réceptionnaires, ne possèdent toujours que la cote « Fiabilité ».

3.88 Nous reconnaissons que, dans bon nombre de pays, les casiers judiciaires et les dossiers de renseignement ne sont pas aussi faciles à obtenir qu'ils le sont au Canada et dans certains pays occidentaux. Cette situation peut faire en sorte que le MAECI ait plus de difficulté à obtenir la cote de sécurité « Secret » pour les employés recrutés sur place dans certains pays. Nous ne voulons pas remettre en question l'intégrité ou la loyauté des employés recrutés sur place mais seulement souligner les limites de la réalisation d'une enquête de sécurité à l'étranger en fonction des normes en vigueur à l'échelle nationale. Les employés recrutés sur place que nous avons reçus en entrevue semblaient bien renseignés et avoir à cœur de bien faire leur travail, qui consistait à traiter les demandes de passeport. Il n'en reste pas moins que, à notre avis, le MAECI assume un risque plus élevé pour les employés recrutés localement qui n'ont pas reçu la cote de sécurité « Secret ».

3.89 Dans un rapport de 2006 sur les services relatifs aux passeports dans les missions canadiennes Passeport Canada indiquait que 167 employés canadiens et 284 employés recrutés sur place contribuaient au programme relatif aux passeports à l'étranger. Tous les employés canadiens étaient des citoyens canadiens travaillant pour le MAECI à titre d'agents du service extérieur tandis que la majorité des employés recrutés sur place n'étaient pas des citoyens canadiens.

3.90 La supervision des « Services consulaires » et de leur programme relatif aux passeports incombe à un agent canadien dans chaque mission. Cependant, les agents canadiens du service extérieur ont tendance à occuper plus fréquemment différents postes dans différentes missions pendant leurs affectations à l'étranger alors que les employés recrutés sur place, qui vivent dans le pays où la mission est située, ont tendance à occuper plus longtemps le même poste dans un endroit donné. Par conséquent, les nouveaux agents consulaires du service extérieur misent beaucoup sur l'expérience et la fiabilité des employés recrutés sur place pour les questions liées au traitement des passeports. Plusieurs employés recrutés sur place, même ceux qui occupent un poste de niveau intermédiaire, sont responsables de déterminer l'admissibilité au passeport sans que leur décision ne fasse l'objet d'un examen direct par un employé canadien.

3.91 Même s'il ne nous revient pas de dire au MAECI qui devrait déterminer l'admissibilité des demandeurs de passeport, la situation en cours dans les bureaux des « Services consulaires » à l'étranger, ainsi que les renseignements susmentionnés au sujet du processus de filtrage de sécurité pour les employés recrutés sur place, soulèvent des préoccupations quant au caractère approprié de tel arrangements en matière de supervision en ce qui a trait à la protection des renseignements personnels des Canadiennes et Canadiens.

3.92 À notre avis, étant donné tous les facteurs qui interviennent dans l'émission de passeports à l'étranger, y compris la répartition des fonctions relatives aux passeports entre 138 missions et plus de 100 bureaux de consuls honoraires (pour les titres de voyage d'urgence), l'absence de certaines mesures de contrôle en matière de TI dans les missions, l'écart entre les cotes de sécurité détenues par les employés recrutés sur place et les employés canadiens, ainsi que le vaste accès des employés des services consulaires aux renseignements relatifs aux passeports, la situation pose un risque supérieur d'atteinte à la vie privée.

3.93 Compte tenu de l'importance de la contribution des employés recrutés sur place au programme relatif aux passeports à l'étranger, il ne serait pas raisonnable de s'attendre à ce que le MAECI se prive de leurs services. Il existe néanmoins certaines mesures que le MAECI pourrait envisager de mettre en place afin d'atténuer le risque lié au recours à

des employés recrutés sur place pour l'exécution du programme relatif aux passeports à l'étranger.

3.94 ***Recommandation : Passeport Canada et le MAECI devraient veiller à ce que tous les employés et les entrepreneurs appelés à traiter des renseignements relatifs aux passeports possèdent la cote de sécurité appropriée, comme l'exigent la Politique du gouvernement sur la sécurité et la politique du Conseil du Trésor. Tout entrepreneur, employé d'entretien ménager ou visiteur ne détenant pas la cote de sécurité voulue devrait être escorté, en tout temps, par un employé de Passeport Canada ou du MAECI.***

Réponse de la direction (MAECI) : D'accord. Les employés canadiens qui sont affectés à l'étranger doivent disposer d'une cote de sécurité de niveau très secret. Dans les cas exceptionnels, pour les raisons opérationnelles urgentes, ils peuvent travailler à l'étranger avec, au moins, une cote de sécurité de niveau secret, en attendant de recevoir la cote de sécurité de niveau très secret. Les employés recrutés sur place reçoivent la cote « Fiabilité », qui représente le niveau minimum de vérification de la sécurité prescrit par la Politique du gouvernement sur la sécurité. Les employés recrutés sur place ont accès à l'information « Protégé B » seulement avec l'autorisation du gestionnaire du programme et de l'agent de sécurité de la mission. Le MAECI applique les conditions de la Politique du gouvernement sur la sécurité concernant les entrepreneurs, les préposés à l'entretien ou les visiteurs. Les visiteurs et les entrepreneurs ont accès à la mission sous surveillance, tandis que les préposés à l'entretien sont accompagnés dans toutes les zones de traitement de documents de nature délicate.

Réponse de la direction (Passeport Canada) : D'accord. Passeport Canada veille à ce que tous les employés, entrepreneurs, préposés à l'entretien et autres personnes ayant accès aux installations de Passeport Canada au Canada ou à des renseignements de nature délicate subissent la vérification de sécurité correspondant aux dispositions de la Politique du gouvernement sur la sécurité avant de commencer à travailler. Les visiteurs ne reçoivent pas de carte d'accès, mais sont accompagnés en tout temps par un employé de Passeport Canada désigné. Passeport Canada continuera de faire en sorte que les politiques en vigueur sur la vérification de la sécurité soient respectées en tout temps.

3.95 ***Recommandation : Lorsqu'il est impossible d'obtenir une cote de sécurité pour les employés recrutés sur place qui soit équivalente à celle des employés canadiens, le MAECI devrait avoir davantage recours à des mesures de contrôle de l'accès et à des journaux de transactions.***

Réponse de la direction (MAECI) : D'accord. Comme il est indiqué à la Recommandation 3.94 plus haut, les employés recrutés sur place reçoivent la cote « Fiabilité », qui est le niveau minimal prescrit par la Politique du gouvernement sur la sécurité, et font l'objet d'une vérification de la sécurité. De plus, il est difficile pour le MAECI de mener des enquêtes de sécurité à l'étranger.

3.96 **Sécurité des TI.** Nous avons discuté, plus haut, de l'accès aux renseignements conservés dans les systèmes des TI. Nous avons souligné les vulnérabilités liées à l'utilisation inappropriée des mots de passe ainsi que la nécessité d'établir une piste de vérification électronique pour surveiller l'accès aux renseignements personnels conservés dans les systèmes des TI et l'utilisation qui en est faite. Voir l'annexe E pour des précisions sur les systèmes de TI des passeports.

3.97 Notre vérification a également soulevé deux autres préoccupations en matière de sécurité des TI liées à l'utilisation de dispositifs portatifs et au fait que certains systèmes et renseignements ne sont pas chiffrés.

3.98 **Utilisation de dispositifs portatifs de stockage de renseignements.** Au cours de la dernière décennie, la popularité, la diversité et la capacité de stockage de données des ordinateurs portatifs et des dispositifs à mémoire électroniques ont crû de façon exponentielle. Les téléphones cellulaires, désormais omniprésents, peuvent maintenant servir à prendre des photographies numériques. Les clés USB, qui peuvent entrer dans la poche d'un vêtement, peuvent contenir plus de données que ne le pouvaient certains ordinateurs de bureau il y a tout juste quelques années. Les BlackBerries peuvent transmettre des documents comportant une grande quantité de données par l'intermédiaire d'un réseau sans fil partout dans le monde. Ces dispositifs de stockage de données électroniques sont devenus indispensables dans les secteurs public et privé. Les employés portent souvent leurs propres dispositifs, en plus de ceux qui leur sont fournis par leur employeur.

3.99 L'introduction croissante de ces dispositifs dans le milieu de travail par les employés et les employeurs s'accompagne de nouveaux risques en ce qui a trait à la protection des renseignements personnels. Ces nouvelles technologies peuvent facilement et rapidement être utilisées pour photographier, copier, enregistrer, télécharger, transmettre ou supprimer de grandes quantités de renseignements avec peu de risques de détection. Il est aussi important de souligner que de tels dispositifs peuvent également entraîner l'introduction de virus informatiques provenant de systèmes externes.

3.100 En outre, tous les dispositifs électroniques, et plus particulièrement les dispositifs sans fil, peuvent facilement être modifiés afin d'être utilisés comme microphones, enregistreurs ou transmetteurs clandestins, même lorsqu'ils sont éteints. Les dispositifs de poche, quant à eux, peuvent facilement être perdus, égarés ou volés.

3.101 Dans un document portant sur l'utilisation de dispositifs sans fil dans les missions, le MAECI indique que la présence de dispositifs sans fil à des endroits où des activités gouvernementales privilégiées ont lieu, que ce soit de façon verbale ou électronique, peut représenter un danger pour la confidentialité de l'information.

3.102 Pendant nos travaux de vérification dans les bureaux des passeports et dans les missions à l'étranger, nous avons constaté que les employés chargés des passeports et le personnel consulaire portaient couramment un téléphone cellulaire ou un BlackBerry. Des restrictions sont imposées dans certaines aires des missions canadiennes, qui ne sont pas rattachées aux « Services consulaires », au sujet du port et de l'utilisation de tels appareils. Les employés doivent déposer leurs téléphones cellulaires et leurs assistants numériques personnels à la porte avant de pénétrer dans ces aires. De la même manière, Passeport Canada a émis une directive interdisant les téléphones cellulaires ou les appareils de poche dans ses centres d'impression, mais cette directive ne s'applique pas aux autres aires de traitement des passeports.

3.103 Nous avons également constaté que ni Passeport Canada ni le MAECI n'avaient mis en place de politique restreignant l'utilisation de dispositifs à mémoire portatifs comme les clés USB, les lecteurs MP3 et les téléphones cellulaires dans toutes les installations de Passeport Canada ou dans les aires consulaires des missions.

3.104 Au moment où nous avons effectué notre vérification, ni Passeport Canada ni le MAECI n'avaient mis en place un mécanisme permettant de surveiller ou d'empêcher l'utilisation de dispositifs comme des clés USB sur les systèmes relatifs aux passeports. Nous avons également constaté qu'il n'existe aucun programme de réalisation de vérifications de sécurité périodiques et aléatoires consistant à demander aux employés qui quittent la mission après leur journée de travail s'ils sont en possession de tout document, de format papier ou électronique, contenant des renseignements personnels et se rapportant au traitement des demandes de passeport. À notre avis, un plus grand nombre de contrôles devraient être réalisés afin de renforcer la confiance qui est placée dans l'intégrité de chacun des employés des missions à l'étranger, et dans les personnes qui travaillent aux opérations relatives aux passeports au Canada, étant donné la nature hautement délicate des renseignements relatifs aux passeports.

3.105 Compte tenu du fait que cette question pourrait se poser quant à l'ensemble du gouvernement, nous en avons discuté avec des fonctionnaires du Secrétariat du Conseil du Trésor. Nous leur avons demandé s'ils croyaient qu'un nombre suffisant de documents d'orientation avaient été élaborés jusqu'à maintenant au sujet des risques liés à ces nouvelles technologies. Le Secrétariat du Conseil du Trésor nous a informés que même s'il n'existe aucun document unique faisant état de tous les renseignements voulus à cet égard, les divers documents d'orientation communiqués aux ministères sont suffisants. Ils ont ajouté que chaque ministère est responsable d'évaluer les risques qui lui sont propres en ce qui a trait à l'utilisation de dispositifs portatifs, comme il le ferait pour tout système des TI, en vertu de la Politique du gouvernement sur la sécurité et des politiques connexes. Les ministères devraient normalement réaliser une évaluation de la menace et des risques et veiller à ce que les politiques, les pratiques et les mesures de contrôle appropriées soient mises en place afin de composer avec les risques liés à leurs opérations, qui peuvent varier d'un programme à l'autre et d'un ministère à l'autre.

3.106 Il importe de souligner que la portée de notre vérification ne comprenait pas une évaluation des documents d'orientation élaborés par le Secrétariat du Conseil du Trésor. Nous avons toutefois constaté qu'au moins une province (l'Ontario) avait produit un document d'orientation exhaustif au sujet des dispositifs portatifs. Nos observations au sujet des « Services consulaires » du MAECI et de Passeport Canada pourraient servir de rappel aux autres ministères et organismes fédéraux en ce qui concerne l'évaluation de leurs politiques et de leurs procédures existantes en ce qui a trait à la gestion de l'utilisation des dispositifs portatifs.

3.107 **Chiffrement des renseignements relatifs aux passeports.** Le chiffrement des renseignements personnels de nature délicate conservés dans des bases de données ou transmis par courriel constitue une importante mesure de sécurité afin d'éviter leur interception ou leur utilisation non autorisée. Le chiffrement est une méthode de protection des données qui consiste à en brouiller le contenu de façon à ce qu'elles ne puissent pas être comprises par des personnes non autorisées. Seules les personnes munies de l'autorisation voulue et des clés de déchiffrement sont en mesure de déchiffrer les données chiffrées et de les rendre lisibles.

3.108 Nous avons constaté que les renseignements relatifs aux passeports qui sont conservés dans la principale base de données de Passeport Canada, soit le système IRIS, ainsi que dans le système PMP du MAECI, ne sont pas chiffrés. Passeport Canada a toutefois indiqué qu'il étudiait la possibilité d'ajouter une fonction de chiffrement à la prochaine mise à jour du système IRIS ou au système qui le remplacera.

3.109 Passeport Canada et le MAECI utilisent des réseaux internes sécurisés pour protéger les courriels envoyés d'un employé à un autre. De la même manière, les courriels envoyés aux autres ministères qui se sont dotés de protocoles de sécurité compatibles sont aussi sécurisés.

3.110 Les renseignements personnels contenus dans les nombreux courriels envoyés à des récipiendaires qui se trouvent à l'extérieur de ces réseaux fermés, cependant, courent le risque d'être interceptés, copiés, modifiés ou détruits par un pirate informatique. Lors de discussions avec divers employés du MAECI à l'étranger et à l'administration centrale, nous avons pu constater que certains employés croyaient, à tort, que tous les courriels envoyés à un récipiendaire de l'extérieur du ministère, y compris ceux envoyés à l'extérieur du réseau sécurisé du MAECI, étaient protégés.

3.111 En vertu de la Politique du gouvernement sur la sécurité, chaque ministère est responsable d'évaluer les risques liés au stockage et à la transmission de ses documents. Le Conseil du Trésor a élaboré des documents d'orientation au sujet de l'utilisation d'outils de chiffrement pour les renseignements « Protégé B » et le Centre de la sécurité des télécommunications peut aider les ministères à faire un choix parmi les différentes méthodes de chiffrement.

3.112 ***Recommandation : Passeport Canada et le MAECI devraient élaborer une politique restreignant l'utilisation de dispositifs à mémoire et de dispositifs d'enregistrement portatifs dans leurs installations, et étudier la possibilité de mettre en place des mesures permettant de gérer la capacité des employés à brancher de tels dispositifs aux systèmes d'information internes. Les employés devraient être mis au courant du contenu de la politique et des avis devraient être affichés aux entrées principales des aires de traitement des passeports. Des balayages périodiques devraient en outre être effectués afin de veiller au respect de la politique.***

Réponse de la direction (MAECI) ***:*** D'accord. Le MAECI examine de façon continue les politiques, y compris celles qui concernent l'utilisation des dispositifs de mémoire et des dispositifs enregistreurs portables. En outre, on met l'accent sur l'amélioration de l'éducation, de la sensibilisation et de la formation en matière de sécurité. Les inspections de la sécurité matérielle et de la sécurité des TI qui sont menées portent présentement sur les politiques et les marches à suivre en vigueur sur les technologies de l'information et la sécurité matérielle.

Réponse de la direction (Passeport Canada) : D'accord. Passeport Canada examinera les lacunes des politiques actuelles en ce qui concerne l'utilisation et la gestion en général de tous les dispositifs portatifs (carte à mémoire, *Blackberries*, etc.) ainsi que l'accès à nos systèmes grâce à ces dispositifs et élaborera par la suite les politiques et les marches à suivre qui s'imposent.

3.113 ***Recommandation : Passeport Canada et le MAECI devraient envisager de chiffrer tous les renseignements relatifs aux passeports conservés dans le système IRIS et dans le système PMP afin de mieux les protéger de tout accès inapproprié, et mettre au point des stratégies afin de veiller à ce que les courriels contenant des renseignements personnels envoyés à des destinataires à l'extérieur des réseaux sécurisés soient chiffrés ou envoyés de façon sécurisée.***

Réponse de la direction (MAECI) ***:*** D'accord. Nous nous employons à renforcer les pratiques de protection de l'information, et le Ministère cherche activement à améliorer la sécurité des technologies de l'information, la sensibilisation à la sécurité et l'éducation en la matière. De plus, nous permettrons le chiffrement de la connexion réseau reliant Passeport Canada et le MAECI pour l'échange de données entre le PMP et IRIS. Le MAECI envisagera le chiffrement de l'information sur les passeports qui est stockée dans les bases de données utilisées dans le cadre du système PMP.

Réponse de la direction (Passeport Canada) : D'accord. Passeport Canada est en train de remplacer son système de fichier central ainsi que de mettre en œuvre de nouveaux systèmes de gestion des dossiers de sécurité et de reconnaissance faciale. Dans le cadre de ces projets, Passeport Canada étudiera et adaptera les options les mieux indiquées pour le renforcement des mesures de protection des renseignements personnels emmagasinés dans nos systèmes électroniques. Passeport Canada lancera aussi un projet de réseau sécuritaire afin d'évaluer d'autres aspects de la sécurité dans le but d'élaborer une vaste stratégie ministérielle visant le renforcement de nos pratiques de protection de l'information. Pour donner suite à certaines préoccupations immédiates, nous permettrons le chiffrement de la connexion réseau reliant Passeport Canada et le MAECI pour l'échange de données entre le PMP et IRIS.

3.114 **Le système Passeport en direct (PED).** Depuis février 2005, Passeport Canada permet aux Canadiennes et Canadiens de remplir une demande de passeport sur Internet au moyen du système PED. On nous a dit qu'en moyenne, le système PED contient environ 28 000 demandes de passeport en ligne actives à n'importe quel moment.

3.115 Les demandeurs accèdent au système PED grâce à l'« epass », l'interface sécurisée du gouvernement fédéral pour tous les programmes et les services du Gouvernement en direct. Chacune des demandes contenues dans le système PED est active pour une période de 60 jours. Une fois qu'il a rempli la demande en ligne, le demandeur doit en faire imprimer une copie et l'apporter à son bureau des passeports local.

3.116 En décembre 2007, le Commissariat à la protection de la vie privée a appris, grâce aux médias, l'existence d'une atteinte à la vie privée au moyen du système PED. Une personne a indiqué à Passeport Canada que, alors qu'elle se trouvait dans le système PED, elle avait découvert qu'elle pouvait accéder aux renseignements personnels de nature délicate relatifs au passeport d'autres demandeurs. Ces renseignements comprenaient le numéro de permis de conduire, le numéro d'assurance sociale ou de carte d'assurance-maladie, ainsi que l'adresse et le numéro de téléphone. La personne a pu obtenir ces renseignements en changeant tout simplement un chiffre au hasard dans

l'adresse URL de la page Web. L'adresse URL est un localisateur alphanumérique unique qui apparaît tout en haut de chaque page Web sur Internet.

3.117 Peu de temps après avoir appris l'existence de cette atteinte à la vie privée, Passeport Canada a mis en arrêt le système PED et a corrigé l'erreur dans la programmation du système qui causait le problème, ce qui a permis de prévenir efficacement tout autre cas d'accès inapproprié à des renseignements personnels. Au moment où nous avons présenté nos demandes d'information en décembre 2007, les représentants de Passeport Canada nous ont indiqué qu'ils ne connaissaient l'existence que d'une seule atteinte à la vie privée de ce genre, et qu'elle concernait l'accès, par une personne, à un petit nombre de documents relatifs à d'autres demandeurs. Puisque c'est la personne ayant accédé aux documents concernant d'autres demandeurs qui a attiré l'attention de Passeport Canada sur le risque d'atteinte à la vie privée, le risque pour les renseignements personnels relatifs aux passeports des Canadiennes et Canadiens a été jugé comme étant minimal par Passeport Canada.

3.118 Une partie de notre vérification des systèmes des TI de Passeport Canada consistait à procéder à l'examen du cadre de contrôle des TI du cycle chronologique d'élaboration des systèmes (CCES). Le CCES est un processus complexe dans le cadre duquel tous les programmes informatiques font l'objet d'un examen et d'une validation avant d'être mis en œuvre dans le milieu de production ou modifiés. Ce processus interne d'examen et d'approbation à plusieurs étapes vise à veiller à ce que de tels programmes soient exécutés de manière appropriée, et à ce qu'ils soient en mesure de protéger les renseignements contre tout accès inapproprié. L'examen que nous avons réalisé nous a permis de déterminer que Passeport Canada avait mis en place un processus de CCES raisonnablement solide, muni des ressources et des pratiques nécessaires, et que ce processus avait fait l'objet d'un examen par le Centre de la sécurité des télécommunications.

3.119 La faille dans le système, qui a été mise en évidence par l'atteinte à la vie privée, était probablement due à une erreur humaine. Or, le risque d'erreurs humaines peut être limité, mais pas totalement éliminé, dans tout système complexe en matière de TI. Passeport Canada étudie toutefois des solutions possibles pour éviter qu'un tel cas d'atteinte à la vie privée ne se reproduise.

3.120 Lorsque nous avons terminé nos travaux de vérification, le 31 janvier 2008, Passeport Canada était en train de réaliser une analyse par arbre des causes afin de cerner l'origine du problème et le nombre de personnes qui pourraient avoir accédé, de manière inappropriée, aux renseignements relatifs au passeport d'autres demandeurs au moyen du système PED. Il est possible qu'une faille dans le codage ait été présente depuis la mise en œuvre du système. Une fois que Passeport Canada aura mené à bien son enquête, nous effectuerons un suivi afin d'examiner les conclusions de l'organisme. Passeport Canada s'est engagé à fournir une copie de son rapport d'enquête au Commissariat à la protection de la vie privée.

3.121 L'équipe chargée de la vérification a aussi été informée du fait que le système PED de Passeport Canada sera remplacé par un autre système au cours de l'année prochaine, et que le nouveau système comportera des fonctions de chiffrement et de protection des renseignements personnels.

Établissement d'un cadre de gestion de la protection de la vie privée et de la sécurité

3.122 Compte tenu du volume et de la nature délicate des renseignements personnels gérés par Passeport Canada, de son modèle de prestation de services complexe nécessitant la participation de partenaires au Canada et à l'étranger, ainsi que des attentes des Canadiennes et Canadiens en ce qui a trait à la protection de leur vie privée, on s'attend à ce que l'organisme s'acquitte de ses responsabilités en matière de protection de la vie privée conformément à la *Loi sur la protection des renseignements personnels* et aux directives du Secrétariat du Conseil du Trésor, et à ce qu'il fournisse le degré de protection de la vie privée le plus élevé possible. Passeport Canada a élaboré un certain nombre d'éléments se rapportant à un cadre visant à permettre la gestion de la protection de la vie privée et à veiller à ce que les renseignements personnels qu'il détient soient en sécurité. Nous avons toutefois constaté que certains éléments clés du cadre étaient manquants ou déficients.

3.123 **Responsabilité en matière de protection de la vie privée.** Un rapport de vérification élaboré en 2006 par le MAECI au sujet des services liés aux passeports fournis dans les missions indiquait qu'il serait possible d'atténuer les risques inhérents à la nature peu centralisée des rôles et responsabilités, associés au caractère nouveau de la Direction des opérations à l'étranger à Passeport Canada, en déterminant clairement les structures de gouvernance, les liens hiérarchiques ainsi que les délégations de pouvoir et en établissant et en communiquant une procédure officielle claire de recours à la hiérarchie pour les problèmes liés aux passeports survenant à l'étranger.

3.124 La création de la Direction des opérations à l'étranger au sein de la Direction générale de la sécurité de Passeport Canada, aux fins de la coordination des services de passeports offerts dans les consulats avec le MAECI, constitue un exemple positif des efforts déployés par Passeport Canada afin de renforcer la reddition de comptes et le contrôle en ce qui a trait aux opérations liées aux passeports dans les consulats. Or, tandis que des progrès tels que celui-ci ont été réalisés depuis la publication du rapport du MAECI, d'autres aspects du cadre de contrôle de gestion entre Passeport Canada et le MAECI sont toujours inexistants ou sont inadéquats pour ce qui est de la protection des renseignements personnels.

3.125 Puisque les renseignements personnels concernant les Canadiennes et Canadiens constituent le matériau brut essentiel aux opérations de Passeport Canada et à l'accomplissement de son mandat, nous nous attendions à ce que la protection de ces renseignements de nature délicate constitue une priorité stratégique pour Passeport Canada. Toutefois, au moment où nous avons procédé à notre vérification, la protection des renseignements personnels ne faisait pas partie des objectifs fondamentaux pour le respect de la mission de Passeport Canada. Les objectifs organisationnels de Passeport Canada mettent l'accent sur ce qui suit : premièrement, veiller à l'intégrité et à la sécurité du processus d'admissibilité, et deuxièmement, maintenir des normes élevées de service au public. Bien que nous ne remettions pas en question la validité des objectifs fondamentaux choisis par Passeport Canada, nous considérons que l'objectif qui consiste à rechercher l'excellence en matière de protection des renseignements concernant les passeports des Canadiennes et Canadiens compléterait et renforcerait les deux autres objectifs.

3.126 Nous avons aussi constaté que Passeport Canada ne peut pas compter sur un <<chef de la protection de la vie privée>> ou sur un autre haut fonctionnaire tenu de rendre des comptes pour l'ensemble des responsabilités en matière de vie privée liées à la protection des renseignements personnels.

3.127 Bien que la *Loi sur la protection des renseignements personnels* n'oblige pas les institutions fédérales à nommer un haut fonctionnaire au poste de <<chef de la protection de la vie privée>>, de plus en plus de ministères et d'organismes qui gèrent des fonds de renseignements personnels d'envergure nomment un <<chef de la protection de la vie privée>> en reconnaissance de l'importance croissante des enjeux liés à la protection de la vie privée pour les Canadiennes et Canadiens et de la façon dont les atteintes à la vie privée peuvent nuire à la crédibilité d'un organisme auprès du public, et de ses partenaires nationaux et internationaux.

3.128 La désignation d'un <<chef de la protection de la vie privée>> permet aussi de faire en sorte que les enjeux liés à la protection de la vie privée puissent être défendus par un champion lors de la prise de décisions organisationnelles, tout en garantissant la reddition de comptes en ce qui concerne la coordination et la mise en œuvre uniforme du grand nombre d'éléments du programme de protection de la vie privée pour l'ensemble de l'organisme.

3.129 Nous avons en outre constaté que le MAECI n'avait pas délégué le plein pouvoir en matière d'accès à l'information et de protection des renseignements personnels (AIRP) à Passeport Canada en ce qui a trait aux questions relatives à l'accès à l'information et à la protection de la vie privée, bien qu'un coordonnateur en matière d'AIPRP et des employés supplémentaires aient été embauchés par Passeport Canada vers la fin de la période de vérification. Jusqu'à maintenant, le sous-ministre du MAECI a choisi de déléguer les responsabilités liées à la protection de la vie privée pour Passeport Canada au directeur de l'AIPRP du MAECI en vertu de l'article 73 de la *Loi sur la protection des renseignements personnels*. Le directeur de l'AIPRP travaille dans les bureaux de l'administration centrale du MAECI à Ottawa et doit donc se fier au personnel de l'AIPRP de Passeport Canada qui travaille dans les bureaux de l'administration centrale de l'organisme, à Gatineau, pour ce qui est de l'information sur les enjeux relatifs à la protection de la vie privée qui concernent le programme relatif aux passeports.

3.130 Sans cette délégation de pouvoir en matière d'AIPRP au coordonnateur en matière d'AIPRP de Passeport Canada, l'organisme dépend de l'équipe de l'AIPRP du MAECI pour l'exécution de ses activités clés en ce qui a trait à la protection des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels* dans le cadre du programme relatif aux passeports.

3.131 À notre avis, le risque lié à la complexité du programme relatif aux passeports et à la quantité de renseignements personnels de nature délicate détenus par l'organisme ne devrait pas être sous-estimé. Ces facteurs démontrent la nécessité, pour Passeport Canada, de coordonner, de mettre en place et de surveiller avec soin la manipulation de ses renseignements fondamentaux. Nous croyons que si Passeport Canada possédait son propre coordonnateur interne en matière d'AIPRP s'étant vu déléguer tous les pouvoirs à cet égard, cela représenterait un réel avantage pour l'organisme. Une telle unité serait davantage au courant des activités et des plans en cours de l'organisme, et serait donc mieux en mesure de comprendre ses défis et ses besoins uniques en ce qui a trait à l'information.

3.132 L'absence d'un fondé de pouvoir, conjuguée au fait qu'il n'y a pas de <<chef de la protection de la vie privée>>, a entraîné la dispersion et la négligence de certaines responsabilités clés en matière de protection de la vie privée pour le programme relatif aux passeports. Notre vérification a notamment révélé plusieurs lacunes en ce qui a trait à la coordination et à la mise en œuvre de responsabilités liées à la protection de la vie privée entre le MAECI et Passeport Canada. Par exemple, les données contenues dans Info Source (liste institutionnelle des fonds d'information) au sujet des dossiers de Passeport Canada n'avaient pas été mises à jour depuis des années, une évaluation des facteurs relatifs à la vie privée portant sur une nouvelle initiative importante d'impartition concernant la Société canadienne des postes n'avait pas été menée à bien avant la mise en œuvre de l'initiative, la connaissance des enjeux relatifs à la protection de la vie privée et à la sécurité des employés qui manipulent les renseignements relatifs aux passeports était insuffisante à certains égards, les dispositions concernant la protection de la vie privée dans le libellé des contrats, des protocoles d'entente et des accords de communication de l'information avec d'autres organisations n'avaient pas été pleinement prises en compte, et un protocole exhaustif en cas d'atteinte à la protection de la vie privée n'avait pas été élaboré.

3.133 ***Recommandation : Le PDG de Passeport Canada devrait tenter d'obtenir l'approbation du ministre du MAECI en vue de la nomination d'un <<chef de la protection de la vie privée>> chargé de la direction et de la coordination de tous les rôles relatifs à la protection de la vie privée et des questions qui y sont liées pour l'ensemble du programme relatif aux passeports, et de rendre des comptes à ce sujet. Passeport Canada devrait aussi chercher à obtenir la pleine délégation des pouvoirs liés à l'AIPRP afin de pouvoir gérer toutes les questions liées à l'accès à l'information et à la protection de la vie privée qui se rapportent au programme relatif aux passeports.***

Réponse de la direction (Passeport Canada) : D'accord. Passeport Canada a créé une division de l'AIPRP en janvier 2008 en vue se préparer à assumer les responsabilités liées à la direction et la coordination des questions d'accès à l'information et de protection des renseignements personnels se rapportant au programme relatif au passeport. L'objectif, ici, consiste à obtenir en 2008-2009 la pleine délégation des pouvoirs du ministre du MAECI pour la gestion de tous les aspects liés à l'AIPRP une fois que toutes les ressources et tous les processus seront en place. De plus, Passeport Canada étudiera la recommandation relative à la nomination d'un <<chef de la protection de la vie privée>>.

3.134 **Signalement des atteintes à la vie privée.** Nous avons constaté que Passeport Canada a mis en place une politique et des procédures opérationnelles pour le traitement des incidents relatifs à la sécurité et l'établissement de rapports à ce sujet. La politique s'applique à toutes les installations de Passeport Canada, que ce soit à l'administration centrale ou dans les bureaux régionaux. Cependant, les procédures en cas d'atteinte à la vie privée de Passeport Canada ne comprennent pas le signalement systématique à l'administration centrale de Passeport Canada de toute atteinte à la vie privée par les missions du MAECI et par l'un de ses agents réceptionnaires. En outre, le protocole en cas d'atteinte à la sécurité n'exige pas que l'équipe de l'AIPRP du MAECI et que les fonctionnaires responsables de l'AIPRP à Passeport Canada soient informés des

atteintes à la vie privée ou qu'on les consulte afin d'obtenir leurs conseils dans de tels cas.

3.135 L'accord conclu entre Passeport Canada et Service Canada comprend une disposition selon laquelle Service Canada doit informer rapidement Passeport Canada de toute communication ou utilisation non autorisée de renseignements personnels, alors que l'accord conclu entre Passeport Canada et la Société canadienne des postes ne contient aucune disposition semblable.

3.136 Nous avons été informés que quelques atteintes à la vie privée survenues par le passé, qui auraient pu nuire à la protection des renseignements personnels, n'avaient pas, de fait, été signalées à l'administration centrale de Passeport Canada. À notre avis, le fait que des atteintes à la vie privée ne soient pas systématiquement signalées et analysées de façon uniforme, afin d'en déterminer les causes et d'éviter que la situation ne se reproduise, représente une importante faiblesse pour la protection générale des renseignements personnels.

3.137 Le Secrétariat du Conseil du Trésor et le Commissariat à la protection de la vie privée ont rendu publics des lignes directrices et des conseils sur le traitement des atteintes à la vie privée. Les Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor indiquent qu'« il importe de mettre le coordonnateur de l'AIPRP et l'agent de sécurité du ministère (ASM) à contribution, pour que la protection de la vie privée et la sécurité des biens soient prises en compte dans le processus de résolution ».

3.138 ***Recommandation : Passeport Canada devrait veiller à ce que ses protocoles pour le signalement des incidents relatifs à la sécurité comprennent le signalement de toutes les atteintes à la vie privée par les fonctionnaires du programme relatif aux passeports, et ne visent pas uniquement ses employés, mais aussi ceux de ses agents réceptionnaires à l'échelle nationale et de ses partenaires consulaires à l'étranger. Le protocole devrait aussi comprendre l'analyse de toute atteinte afin d'éviter que la situation ne se reproduise, ainsi que des procédures pour la notification des clients touchés par une atteinte à la vie privée.***

Réponse de la direction (Passeport Canada) : D'accord. Conformément à la directive du Conseil du Trésor sur les atteintes à la vie privée, Passeport Canada est en train d'élaborer sa propre directive sur le sujet, qui devrait être mise en œuvre en 2008-2009. La directive viendra alors compléter les marches à suivre relatives aux incidents liés à la sécurité des TI. La formation combinée sur l'accès à l'information et la protection des renseignements personnels continuera d'être donnée à tous les employés et comprendra un programme de sensibilisation de sorte que tous les employés connaissent les Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor et leurs responsabilités en ce qui concerne la protection des renseignements personnels relevant d'eux. De plus, Passeport Canada et le MAECI oeuvreront de concert pour favoriser une mise en œuvre réussie des directives se rapportant aux passeports dans les missions canadiennes à l'étranger.

3.139 **Ententes d'échange de renseignements.** L'alinéa 8(2)(*f*) de la *Loi sur la protection des renseignements personnels* oblige les ministères à élaborer des dispositions ou des ententes concernant la communication de tout renseignement personnel avec d'autres organismes gouvernementaux au niveau international ou provincial. La politique du Conseil du Trésor exige quant à elle que les ministères élaborent des ententes écrites

signées par les parties définissant l'étendue de la communication d'information ainsi que les mesures mises en place pour protéger les renseignements personnels. Ces ententes visent à veiller à ce que les renseignements personnels communiqués soient utilisés de manière appropriée conformément aux fins indiquées, et qu'ils soient protégés de façon adéquate tout au long de leur cycle de vie.

3.140 Le Secrétariat du Conseil du Trésor (SCT) a collaboré avec l'Institut des services axés sur les citoyens à l'élaboration du document *Ententes d'échange de renseignements personnels entre gouvernements – Lignes directrices sur les pratiques exemplaires*, qui fournit des conseils et des modèles d'ententes d'échange de renseignements utiles pour aider les institutions fédérales dans leurs efforts en vue de conclure de telles ententes. Le SCT offre d'autres conseils pouvant s'appliquer aux contrats et aux ententes concernant la prestation de services conclus avec des tierces parties en ce qui a trait aux renseignements personnels des Canadiennes et Canadiens dans le *Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché.*

3.141 Passeport Canada a conclu diverses ententes d'échanges de services et de renseignements avec le MAECI, des agents réceptionnaires, des organismes du gouvernement fédéral, ainsi que des registres provinciaux et territoriaux des naissances et des décès. Les principaux partenaires au sein du gouvernement fédéral comprennent Citoyenneté et Immigration Canada, le Service correctionnel du Canada, le ministère de la Justice, l'Agence des services frontaliers du Canada, la Gendarmerie royale du Canada et le Service canadien du renseignement de sécurité.

3.142 Nous avons constaté que certaines des ententes d'échange de renseignements conclues par Passeport Canada dataient d'il y a plusieurs années et n'avaient pas été mises à jour récemment dans le but de veiller à ce qu'elles tiennent compte des pratiques en cours et des toutes dernières exigences en matière de protection de la vie privée. Plusieurs de ces ententes ne comprenaient pas non plus les dispositions clés en matière de protection de la vie privée énoncées dans les lignes directrices du Conseil du Trésor en ce qui a trait à la protection des renseignements personnels. Ces dispositions devraient définir, par exemple, les renseignements personnels qui seront communiqués, les limites relatives à l'arrangement en matière d'échange de renseignements, les mesures de sécurité, ainsi que les exigences relatives à la surveillance et aux vérifications visant à faire en sorte que les renseignements relatifs aux passeports soient sécuritaires et protégés de façon adéquate tout au long du cycle de vie de ces derniers.

3.143 Lors de la comparaison des textes des deux ententes que Passeport Canada a signées avec chacun de ses agents réceptionnaires (Service Canada et la Société canadienne des postes), nous avons constaté que l'entente conclue avec Service Canada comprend toute une section sur la protection de la vie privée, ce qui n'est pas le cas pour l'entente conclue avec la Société canadienne des postes. L'entente conclue avec Service Canada comprend aussi beaucoup plus de contraintes liées à la protection de la vie privée et à la sécurité visant à protéger les renseignements personnels que l'entente conclue avec la Société canadienne des postes.

3.144 Un rapport de vérification du Bureau du vérificateur général du Canada rendu public en 2006 demandait que soit élaborée une entente cadre entre Passeport Canada et le MAECI définissant les rôles respectifs de chaque intervenant dans le cadre du programme relatif aux passeports. Cette entente cadre n'avait pas encore été élaborée à ce moment-là, et aucune entente cadre semblable n'avait encore été signée par Passeport Canada et par le MAECI au moment de la vérification.

3.145 ***Recommandation : Tous les protocoles d'entente, les ententes et les autres arrangements visant l'échange de renseignements personnels entre Passeport Canada et ses partenaires devraient être mis à jour dans un avenir prochain dans le but de veiller à ce qu'ils rendent compte des pratiques en cours et qu'ils soient conformes à toutes les exigences en matière de protection de la vie privée, de sécurité et de passation de marchés du Conseil du Trésor.***

> ***Réponse de la direction* (Passeport Canada) :** D'accord. Passeport Canada est déterminé à renforcer les ententes en vigueur sur l'échange de renseignements ainsi qu'à explorer d'autres secteurs de collaboration future susceptibles de l'aider à s'acquitter de sa mission. La négociation de protocoles d'entente est un processus complexe et dépend de la disponibilité de ressources à Passeport Canada et dans les organisations partenaires. Passeport Canada reverra ses ententes en vigueur afin de relever les domaines dans lesquels l'amélioration des protocoles d'entente applicables à la sécurité et à la protection de la vie privée s'imposerait et sollicitera à cet égard la participation d'intervenants.

3.146 **Formation de sensibilisation à la protection de la vie privée et à la sécurité.** La protection des renseignements personnels au sein d'un organisme comme Passeport Canada revêt la plus grande importance. Les employés, qui traitent quotidiennement les renseignements personnels de nature délicate des Canadiennes et Canadiens dans le cadre de leurs fonctions, doivent comprendre clairement leurs responsabilités en ce qui a trait à la protection de ces renseignements en vertu de la *Loi sur la protection des renseignements personnels*, en plus de bien saisir leurs responsabilités fondamentales en matière de sécurité conformément à la Politique du gouvernement sur la sécurité.

3.147 Les employés du gouvernement devraient donc recevoir, à cette fin, une formation continue de sensibilisation à la protection de la vie privée et à la sécurité, accompagnée de mises à jour. Une telle formation comprendrait la définition du rôle et des responsabilités de chacun en ce qui a trait à la protection des renseignements personnels contre l'accès, l'utilisation, la communication, la modification ou la destruction inapproprié. Elle couvrirait aussi d'autres sujets comme la restriction de la collecte de renseignements personnels et le droit des personnes à avoir accès à leurs propres renseignements personnels, et à y apporter des corrections.

3.148 Pendant nos travaux de vérification, nous avons en général constaté que la plupart des employés du programme de Passeport Canada, des services consulaires du MAECI et des agents réceptionnaires, connaissaient les dispositions concernant la confidentialité contenues dans la *Loi sur la protection des renseignements personnels*. Nous avons cependant également constaté que les connaissances des autres dispositions relatives à la protection de la vie privée et à la sécurité de l'information étaient limitées. La majorité des employés que nous avons rencontrés en entrevue pendant notre vérification ne se souvenaient pas d'avoir reçu une formation sur la protection de la vie privée ou une formation récente sur la sécurité de l'information.

3.149 Par exemple, un grand nombre d'employés du MAECI reçus en entrevue dans des missions diplomatiques ne connaissaient pas le niveau de leur cote de sécurité personnelle. La plupart des employés de Passeport Canada et du MAECI ne savaient pas non plus que le fait de conserver des documents comme des demandes de

passeport, des passeports et des documents d'identité originaux sur des étagères à libre accès ou dans des contenants sans couvercles constituait un risque possible d'atteinte à la vie privée ou à la sécurité lié à l'accès inapproprié à des renseignements personnels de nature délicate.

3.150 Il est arrivé plusieurs fois que des employés se débarrassent de formulaires de passeport contenant des renseignements personnels de façon inappropriée, soit en les jetant avec les ordures régulières, soit en les déposant dans les bacs à recyclage. Lorsque nous avons abordé la question, les employés ont semblé ne pas savoir que les documents dont ils s'étaient débarrassés contenaient des « renseignements personnels » correspondant à la définition qui est donnée de ce terme dans la *Loi sur la protection des renseignements personnels*.

3.151 Nous avons aussi constaté que dans certains consulats à l'étranger, le personnel des missions, c'est-à-dire les employés canadiens et les employés recrutés sur place, ne comprenaient pas clairement les risques liés à la sécurité et les politiques internes régissant l'utilisation d'appareils électroniques comme les téléphones cellulaires, les clés USB et les BlackBerries dans leur mission. Certains membres du personnel ont indiqué qu'ils pouvaient apporter ces appareils dans les aires réservées au consulat, alors que d'autres ont indiqué qu'ils n'étaient pas autorisés à le faire.

3.152 La Direction de l'AIPRP et le personnel chargé de la sécurité au MAECI donnent, depuis un certain nombre d'années, une formation de sensibilisation à la protection de la vie privée et à la sécurité aux diplomates canadiens et aux employés des consulats qui s'apprêtent à partir à l'étranger. Toutefois, comme la plupart des employés recrutés sur place n'ont pas la possibilité de venir au Canada, il pourrait être difficile, pour le MAECI, de leur fournir en personne une formation sur la protection de la vie privée et la sécurité qui soit équivalente à celle qui est donnée aux employés s'apprêtant à partir à l'étranger.

3.153 Passeport Canada a mis en œuvre un programme de formation sur la protection de la vie privée à l'intention de son personnel opérationnel et de ses cadres supérieurs en décembre 2007. Après avoir examiné les documents de formation qui nous ont été fournis par Passeport Canada et par le MAECI, nous sommes en mesure de dire qu'ils sont exhaustifs et que la matière y est bien présentée.

3.154 ***Recommandation : Afin de permettre aux employés de comprendre pleinement les tâches qu'ils doivent accomplir chaque jour et de veiller à ce que les renseignements personnels relatifs aux passeports soient protégés en tout temps, Passeport Canada et le MAECI devraient continuer d'utiliser les ressources liées à la protection de la vie privée et à la sécurité pour offrir des programmes coordonnés de formation sur la protection de la vie privée et la sécurité, ainsi que du matériel pédagogique connexe, aux employés de Passeport Canada qui travaillent au Canada ainsi qu'aux fonctionnaires en poste dans les consulats à l'étranger.***

Réponse de la direction (MAECI) : D'accord. La consigne veut que les fonctionnaires fédéraux reçoivent continuellement une formation de sensibilisation à la protection des renseignements personnels et à la sécurité. Dans le cadre de la formation de deux semaines destinée aux spécialistes consulaires, les employés recrutés sur place (de 60 à 80 étudiants par année) suivent cette formation. En septembre, le cours comprendra un module sur la sécurité de l'information. Le MAECI offre un cours d'une demi-journée sur la sécurité de l'information à

quelques reprises pendant l'année. Un représentant du bureau d'accès à l'information et de protection des renseignements personnels du MAECI y participe pour offrir le point de vue d'un expert et répondre aux questions des participants. Le MAECI indique également, dans son cours obligatoire d'initiation à la sécurité, les divers niveaux d'information classifiée et protégée ainsi que les méthodes appropriées de protection des renseignements de nature délicate. Le MAECI lancera un nouveau cours en ligne sur la sécurité à l'automne 2008, qui servira à renforcer les pratiques exemplaires en matière de sécurité et devra être suivi à intervalles réguliers par tous les employés. Le bureau de l'AIPRP est en train d'instaurer une capacité permanente d'élaboration de stratégies et de formation qui permettra la prestation à intervalles réguliers d'une sensibilisation à l'AIPRP à tous les responsables du MAECI, y compris la mise en œuvre d'un tutoriel en ligne sur l'AIPRP destiné aux employés du MAECI à l'étranger. De plus, la division de l'AIPRP oeuvrera étroitement avec les divisions de la gestion de l'information et de la sécurité pour assurer l'adoption d'une approche coordonnée en matière de formation sur la protection de la vie privée, certes, mais aussi sur la sécurité et la confidentialité des renseignements personnels.

Réponse de la direction (Passeport Canada) : D'accord. Passeport Canada continuera de travailler avec des partenaires externes et internes à l'élaboration, à l'exécution et à la surveillance d'une formation sur la sécurité et la protection des renseignements personnels. L'organisme a élaboré un cours spécifique sur la protection des renseignements personnels en 2007 et l'offre de manière continue à tous les employés. Une approche multidisciplinaire sera adoptée, si le contexte s'y prête, pour organiser et coordonner l'exécution des programmes relatifs à la protection de la vie privée et à la sécurité et la prestation des documents de sensibilisation s'y rapportant.

3.155 **Autres questions** – Voir l'annexe B pour la liste des autres enjeux relatifs à la protection de la vie privée qui ont été soulevés pendant la vérification.

Au sujet de la vérification

Objectif de la vérification

L'objectif de la vérification consiste à rassembler des données prouvant, de façon raisonnable, que les renseignements personnels des Canadiennes et Canadiens et des résidents canadiens qui sont traités par Passeport Canada et par ses partenaires sont protégés de façon adéquate tout au long de leur cycle de vie, et à proposer des améliorations aux processus et au cadre de gestion de la protection de la vie privée et de la sécurité qui sont utilisés par Passeport Canada et par ses partenaires dans l'ensemble du système relatif aux passeports.

Mandat de vérification

Le mandat du Commissariat à la protection de la vie privée du Canada (CPVP) consiste à réaliser des examens de la conformité (vérifications) en vertu du paragraphe 37(1) de la *Loi sur la protection des renseignements personnels* en ce qui a trait aux pratiques de traitement des renseignements personnels des institutions fédérales comme Passeport Canada et le ministère des Affaires étrangères et du Commerce international (MAECI).

Établissement de la portée de la vérification

4.1 Notre vérification a débuté par une enquête ou un exercice de détermination de la portée visant à cerner les secteurs du programme relatif aux passeports présentant le plus grand risque possible pour la protection de la vie privée des Canadiennes et Canadiens. Pendant cette étape de la vérification, l'équipe chargée de la vérification s'est penchée sur les documents mis à la disposition du public au sujet de Passeport Canada et a examiné les dossiers concernant les enquêtes menées à la suite de plaintes déposées au Commissariat, les dossiers des évaluations des facteurs relatifs à la vie privée effectuées, ainsi que les rapports élaborés par d'autres organismes de surveillance comme le Bureau du vérificateur général du Canada. Nous avons également procédé à l'examen de nombreux programmes de Passeport Canada et de nombreuses politiques et procédures consulaires du MAECI en ce qui a trait aux opérations liées aux passeports.

Travaux de vérification

4.2 Les travaux de vérification sur le terrain ont pris la forme de visites aux endroits suivants : principaux centres d'impression des passeports de Passeport Canada situés dans la région de la capitale nationale et dans la région du Grand Toronto; télécentres de la région de la capitale nationale et de Montréal; installations de prestation de services de la Société canadienne des postes et de Service Canada (agents réceptionnaires) à l'administration centrale ainsi que dans les régions du Québec/de l'Atlantique, du Grand Toronto et de l'Ouest.

4.3 Les installations qui ont fait l'objet d'un examen comprenaient les aires d'attente pour le public dans les installations de prestation de services, les comptoirs de services, les aires de traitement, les installations où sont entreposés les dossiers, les installations où sont détruits les dossiers, ainsi que les salles des serveurs des TI.

4.4 Des activités de vérification semblables ont eu lieu dans les missions du MAECI à Berne, à Paris, à Beijing, à Los Angeles et à Taipei, où nous avons examiné la prestation des services liés aux passeports dans l'aire réservée aux « Services consulaires ». Nous avons aussi posé des questions au sujet du rôle joué par les consuls honoraires, qui fournissent aux Canadiennes et aux Canadiens des titres de voyage d'urgence dans plus de 100 emplacements à l'étranger.

4.5 Nous nous sommes également penchés sur diverses fonctions organisationnelles en place à Passeport Canada et au MAECI qui appuient le programme relatif aux passeports. Ces fonctions comprenaient les activités liées à la protection de la vie privée au Secrétariat de l'AIPRP, ainsi que les fonctions liées à la sécurité des installations physiques, du personnel et des TI. Nous avons aussi passé en revue les arrangements concernant l'échange de renseignements entre Passeport Canada et ses partenaires, les fonctions liées aux enquêtes et aux renseignements, ainsi que les activités de formation liées à la protection de la vie privée et à la sécurité offertes aux employés.

4.6 Nous avons complété les travaux de vérification susmentionnés en procédant à un examen détaillé des documents de référence et des demandes présentées par écrit aux fonctionnaires concernés, et à un grand nombre d'entrevues dirigées pour chaque activité, installation et secteur de programme examiné.

4.7 Même si les députés fournissent de l'aide à leurs électeurs en ce qui concerne les demandes de passeport, ces activités n'étaient pas visées par notre vérification; le mandat du Commissariat à la protection de la vie privée ne comprend pas l'examen des activités des parlementaires.

4.8 L'équipe chargée de la vérification du Commissariat à la protection de la vie privée a obtenu une collaboration exceptionnelle de la part de Passeport Canada et de ses partenaires tout au long de sa vérification, et ce, malgré une lourde charge de travail et des pressions opérationnelles concurrentes. Un accès intégral et opportun à l'information, à la documentation, aux installations et au personnel a été fourni sur demande.

4.9 Les travaux de vérification sur le terrain ont en grande partie été menés à bien avant le 31 janvier 2008.

Méthodologie utilisée pour la vérification

4.10 La méthode utilisée pour la vérification combinait un certain nombre d'approches. Nous avons commencé par établir la liste des critères de vérification en passant en revue les lois et les règlements pertinents, les décrets, ainsi que les politiques et les directives du Secrétariat du Conseil du Trésor et du gouvernement. Nous avons aussi examiné les politiques opérationnelles, les pratiques, les accords, les contrats et les documents de formation en fonction des critères établis pour la vérification de la protection de la vie privée.

4.11 Des examens des dossiers et des documents ont été réalisés aux fins de la compréhension des fonctions de contrôle de la qualité, de renseignement et d'enquête au sein de la Direction générale de la sécurité de Passeport Canada.

4.12 L'équipe chargée de la vérification a aussi procédé à une visite des installations afin d'observer les mesures en place en ce qui a trait au traitement et au stockage des documents, ainsi qu'à leur sécurité matérielle. Nous avons en outre assisté à plusieurs démonstrations en direct des systèmes des TI utilisés à Passeport Canada et au MAECI

afin d'observer la façon dont les renseignements personnels sont recueillis, utilisés, échangés et communiqués.

4.13 Enfin, le Commissariat à la protection de la vie privée a embauché un consultant de l'extérieur qu'il a chargé de procéder à une évaluation du site Web public de Passeport Canada en accordant une attention spéciale aux mesures de contrôle en matière de sécurité et de protection de la vie privée utilisées.

Critères de vérification

4.14 Dès le début de la vérification, l'équipe chargée de la vérification s'attendait à ce que Passeport Canada et ses partenaires gèrent les renseignements personnels des Canadiennes et Canadiens de façon :

- à respecter les obligations énoncées dans le Décret sur les passeports canadiens, tel que modifié;
- à respecter les articles 4 à 8 de la *Loi sur la protection des renseignements personnels*;
- à respecter les politiques applicables du Conseil du Trésor et du gouvernement du Canada;
- à observer les dix principes relatifs à l'équité dans le traitement des renseignements reconnus à l'échelle internationale et énoncés dans la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Nota : *Veuillez consulter les annexes C et D pour connaître les champs d'enquête et les critères de vérification détaillés. Les champs d'enquête et les critères de vérification ont été communiqués à Passeport Canada, et le Commissariat à la protection de la vie privée a reçu la confirmation de leur acceptation en tant que fondement des travaux de vérification.*

Normes relatives à la vérification

4.15 Les travaux de vérification décrits dans le présent document ont été réalisés conformément au mandat législatif, aux politiques et aux pratiques du Commissariat à la protection de la vie privée du Canada. Ils respectent les normes recommandées par l'Institut canadien des comptables agréés (ICCA).

Équipe chargée de la vérification

Trevor R. Shaw, CA CMA
Directeur général par intérim,
Vérification et revue

Raymond Brault
Agent principal de vérification et de revue

Tom J. Fitzpatrick
Gestionnaire, Vérification et revue
et responsable de la vérification

William Wilson
Agent de vérification et de revue

Annexe A – Liste des recommandations formulées à l'issue de la vérification

Collecte des renseignements personnels

1. Passeport Canada devrait explorer des options quant à la meilleure façon de recueillir l'information financière des demandeurs et les données personnelles des répondants de manière à ne pas nuire indûment au processus relatif au passeport, tout en prenant en considération la vie privée de ces personnes. Il devrait également modifier ses documents sur la formation et les politiques de façon à limiter la collecte du NAS, tout en encourageant activement les demandeurs à utiliser d'autres formes d'identification qui posent moins de risque pour la vie privée.

Contrôle de la consultation, de l'utilisation et de la communication des renseignements personnels

2. Passeport Canada et le MAECI devraient prendre ensemble les mesures qui s'imposent pour contrôler l'accès des employés aux renseignements personnels. Ces mesures devraient tenir compte de la désignation « Protégé B » de ces renseignements, respecter le principe du besoin de connaître et comprendre des pistes de vérification électroniques pour les systèmes IRIS et PMP afin de réduire les risques d'accès inapproprié aux renseignements personnels.

Mesures appropriées de conservation et d'élimination des renseignements personnels

3. Étant donné les risques inhérents associés à la conservation des renseignements relatifs au passeport pour une période de 100 ans, et compte tenu des exigences de la Loi sur la protection des renseignements personnels selon lesquelles les renseignements personnels ne doivent être conservés qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées ou selon les dispositions des règlements, Passeport Canada devrait consulter Bibliothèque et Archives Canada en vue de réévaluer cette période anormalement longue de conservation des dossiers.
4. Passeport Canada devrait évaluer les risques pour la vie privée et la sécurité que posent ses pratiques actuelles d'élimination et/ou de destruction des renseignements personnels de nature délicate, et ce, pour tous les types de dossiers.

Mesures de sécurité essentielles

5. **Sécurité matérielle.** Passeport Canada et le MAECI devraient s'assurer que leurs dossiers sur support papier contenant des renseignements relatifs au passeport sont entreposés de façon appropriée pour des renseignements « Protégé B » de nature particulièrement délicate conformément à la Politique du gouvernement sur la sécurité.
6. Passeport Canada et le MAECI devraient revoir leurs mesures de sécurité matérielle et leurs autres mesures de sécurité pour s'assurer que l'accès aux endroits où les passeports sont traités n'est accordé qu'aux personnes qui en ont besoin pour s'acquitter de leurs tâches.

7. Passeport Canada et le MAECI devraient revoir la disposition et l'acoustique de toutes les zones de service au public pour fournir un niveau adéquat de protection de la vie privée à leurs clients au moyen d'une signalisation et de barrières visuelles et acoustiques appropriées.
8. **Enquête de sécurité sur le personnel.** Passeport Canada et le MAECI devraient veiller à ce que tous les employés et les entrepreneurs appelés à traiter des renseignements relatifs aux passeports possèdent la cote de sécurité appropriée, comme l'exigent la Politique du gouvernement sur la sécurité et la politique du Conseil du Trésor. Tout entrepreneur, employé d'entretien ménager ou visiteur ne détenant pas la cote de sécurité voulue devrait être escorté, en tout temps, par un employé de Passeport Canada ou du MAECI.
9. Lorsqu'il est impossible d'obtenir une cote de sécurité pour les employés recrutés sur place qui soit équivalente à celle des employés canadiens, le MAECI devrait avoir davantage recours à des mesures de contrôle de l'accès et à des journaux de transactions.
10. **Sécurité des TI.** Passeport Canada et le MAECI devraient élaborer une politique restreignant l'utilisation de dispositifs à mémoire et de dispositifs d'enregistrement portatifs dans leurs installations, et étudier la possibilité de mettre en place des mesures permettant de gérer la capacité des employés à brancher de tels dispositifs aux systèmes d'information internes. Les employés devraient être mis au courant du contenu de la politique et des avis devraient être affichés aux entrées principales des aires de traitement des passeports. Des balayages périodiques devraient en outre être effectués afin de veiller au respect de la politique.
11. Passeport Canada et le MAECI devraient envisager de chiffrer tous les renseignements relatifs aux passeports conservés dans le système IRIS et dans le système PMP afin de mieux les protéger de tout accès inapproprié, et mettre au point des stratégies afin de veiller à ce que les courriels contenant des renseignements personnels envoyés à des destinataires à l'extérieur des réseaux sécurisés soient chiffrés ou envoyés de façon sécurisée.

Établissement d'un cadre de gestion de la protection de la vie privée et de la sécurité

12. **Responsabilité en matière de protection de la vie privée.** Le PDG de Passeport Canada devrait tenter d'obtenir l'approbation du ministre du MAECI en vue de la nomination d'un <<chef de la protection de la vie privée>> chargé de la direction et de la coordination de tous les rôles relatifs à la protection de la vie privée et des questions qui y sont liées pour l'ensemble du programme relatif aux passeports, et de rendre des comptes à ce sujet. Passeport Canada devrait aussi chercher à obtenir la pleine délégation des pouvoirs liés à l'AIPRP afin de pouvoir gérer toutes les questions liées à l'accès à l'information et à la protection de la vie privée qui se rapportent au programme relatif aux passeports.

13. **Atteintes à la vie privée.** Passeport Canada devrait veiller à ce que ses protocoles pour le signalement des incidents relatifs à la sécurité comprennent le signalement de toutes les atteintes à la vie privée par les fonctionnaires du programme relatif aux passeports, et ne visent pas uniquement ses employés, mais aussi ceux de ses agents réceptionnaires à l'échelle nationale et de ses partenaires consulaires à l'étranger. Le protocole devrait aussi comprendre l'analyse de toute atteinte afin d'éviter que la situation ne se reproduise, ainsi que des procédures pour la notification des clients touchés par une atteinte à la vie privée.
14. **Ententes d'échange de renseignements.** Tous les protocoles d'entente, les ententes et les autres arrangements visant l'échange de renseignements personnels entre Passeport Canada et ses partenaires devraient être mis à jour dans un avenir prochain dans le but de veiller à ce qu'ils rendent compte des pratiques en cours et qu'ils soient conformes à toutes les exigences en matière de protection de la vie privée, de sécurité et de passation de marchés du Conseil du Trésor.
15. **Formation de sensibilisation à la protection de la vie privée et à la sécurité.** Afin de permettre aux employés de comprendre pleinement les tâches qu'ils doivent accomplir chaque jour et de veiller à ce que les renseignements personnels relatifs aux passeports soient protégés en tout temps, Passeport Canada et le MAECI devraient continuer d'utiliser les ressources liées à la protection de la vie privée et à la sécurité pour offrir des programmes coordonnés de formation sur la protection de la vie privée et la sécurité, ainsi que du matériel pédagogique connexe, aux employés de Passeport Canada qui travaillent au Canada ainsi qu'aux fonctionnaires en poste dans les consulats à l'étranger.

Annexe B – Autres problèmes liés à la vérification

Les énoncés de problèmes qui suivent découlent de nos travaux de vérification et de notre analyse de la situation en ce qui a trait aux pratiques de gestion des renseignements personnels mises en œuvre à Passeport Canada, dans les missions du MAECI (« Services consulaires »), et chez les agents réceptionnaires. Un grand nombre de ces questions sont liées aux recommandations qui figurent dans le corps du rapport de vérification.

Mesures appropriées de conservation et d'élimination des renseignements personnels

- Les renseignements figurant sur la carte de crédit qui sont actuellement recueillis dans les demandes de passeport sont conservées pour une période supérieure à celle nécessaire aux fins du programme relatif aux passeports.
- Les documents liés aux demandes de passeport qui sont conservés par Passeport Canada et le MAECI ne font l'objet d'aucun suivi visant à éviter qu'ils ne manquent à l'appel pendant leur période de stockage et à veiller à ce qu'ils soient détruits lorsqu'ils ne sont plus utiles.
- Certains consuls honoraires en poste à l'étranger font des copies superflues des demandes de passeport et des déclarations solennelles.
- Le MAECI n'a pas mis au point un calendrier commun de conservation et d'élimination des images de télévision en circuit fermé enregistrées dans les aires consulaires afin de veiller à ce qu'elles ne soient pas conservées plus longtemps que nécessaire.
- Dans certaines salles d'attente publiques, les clients n'ont pas accès à des installations sécuritaires pour jeter des demandes de passeport partiellement remplies contenant des renseignements personnels.

Mesures de sécurité essentielles

- **Écrans d'ordinateurs.** Dans quelques-unes des installations de Passeport Canada qui ont été visitées pendant la vérification, la disposition des écrans d'ordinateurs utilisés par les agents des passeports permettait aux membres du public ou à d'autres personnes non autorisées d'apercevoir des renseignements personnels de nature délicate.

  Nota : *Les commentaires qui suivent sont fondés sur une analyse du site Web public de Passeport Canada effectuée en 2007 par Watchfire, un fournisseur de services externe.*

- **Site Web de Passeport Canada (www.ppt.gc.ca).** Nous avons constaté que les formulaires en ligne « Plainte auprès de l'Ombudsman » et « Questionnaire – Rétroaction des clients » (versions française et anglaise) n'étaient pas chiffrés sur le site Web de Passeport Canada.
- La fonction de « remplissage automatique » du navigateur n'était pas désactivée pour tous les formulaires en ligne non protégés par l'application epass Canada.
- Un avis faisant état de tous les droits prévus dans la *Loi sur la protection des renseignements personnels* n'apparaissait pas sur tous les formulaires en ligne de Passeport Canada servant à recueillir des renseignements personnels.
- Aucun avis n'apparaît pour avertir les utilisateurs qu'ils s'apprêtent à quitter le site Web sécurisé de Passeport Canada pour entrer sur le site d'une tierce partie, qui pourrait ne pas comporter les mêmes caractéristiques de sécurité.

Établissement d'un cadre de gestion de la protection de la vie privée et de la sécurité

- Passeport Canada ne reçoit pas d'évaluations de la menace et des risques de la part des agents réceptionnaires, comme le prévoit le contrat qu'il a conclu avec eux.
- **Évaluations des facteurs relatifs à la vie privée.** Ce ne sont pas tous les résumés des évaluations des facteurs relatifs à la vie privée et des évaluations préliminaires des facteurs relatifs à la vie privée de Passeport Canada qui sont affichés sur son site Web, tel que l'exige la politique du Secrétariat du Conseil du Trésor sur les évaluations des facteurs relatifs à la vie privée.
- **Avis relatifs à la vie privée.** Les avis concernant la protection de la vie privée qui apparaissent sur les formulaires de demande de passeport de Passeport Canada n'informent pas les demandeurs de leurs droits d'accéder à leurs renseignements personnels, de les corriger, et de déposer une plainte concernant l'utilisation qui en est faite.

Annexe C – Champs d'enquête et critères de vérification généraux

CHAMPS D'ENQUÊTE ET CRITÈRES DE VÉRIFICATION GÉNÉRAUX	OBSERVATIONS ET CONCLUSIONS
CHAMP D'ENQUÊTE N^{O} 1 : COLLECTE DES RENSEIGNEMENTS PERSONNELS *La collecte des renseignements personnels semble-t-elle être réalisée de façon sécuritaire et à la seule fin de la délivrance d'un passeport?* (Loi sur la protection des renseignements personnels*, articles 4, 5 et 7*)	
Les renseignements personnels recueillis l'ont-ils été à la seule fin de la délivrance d'un passeport et avec le consentement du demandeur?	
- Les renseignements personnels recueillis ne sont utilisés qu'aux fins de la détermination du droit d'obtenir un passeport, et de la délivrance subséquente de celui-ci.	
- Les renseignements personnels recueillis le sont avec le consentement éclairé du demandeur.	
Les renseignements personnels sont-ils recueillis de manière sécuritaire? (conformément à la Politique du gouvernement sur la sécurité et à la Norme de gestion de la sécurité des technologies de l'information)	
- La méthode utilisée pour la collecte des renseignements personnels, ainsi que le lieu de celle-ci, sont sécuritaires.	
- Les renseignements personnels sont conservés dans un endroit sécuritaire.	
- Le transport et la transmission des renseignements personnels ont lieu de façon sécuritaire.	
Des mesures et des contrôles appropriés ont-ils été mis en place pour protéger la collecte de renseignements personnels?	
- La collecte de renseignements personnels est régie par des procédures.	
- Les procédures sont observées par l'équipe chargée de recueillir les renseignements personnels.	
- Les activités liées à la collecte des renseignements personnels font l'objet d'une surveillance et d'un examen continus afin de cerner et d'atténuer les risques d'atteinte à la vie privée.	
CHAMP D'ENQUÊTE N^{O} 2 : UTILISATION DES RENSEIGNEMENTS PERSONNELS *Les renseignements personnels semblent-ils utilisés de façon sécuritaire et aux seules fins de la délivrance d'un passeport? (*Loi sur la protection des renseignements personnels*, articles 4 et 7)*	

CHAMPS D'ENQUÊTE ET CRITÈRES DE VÉRIFICATION GÉNÉRAUX	OBSERVATIONS ET CONCLUSIONS
L'utilisation des renseignements personnels est-elle limitée aux fins de délivrance d'un passeport ou aux fins prévues par la loi?	
- Les renseignements personnels sont utilisés seulement aux fins de la détermination du droit d'obtenir un passeport, et de la délivrance subséquente de celui-ci, ou aux fins prévues par la loi.	
Pendant leur traitement, les renseignements personnels sont-ils conservés de façon sécuritaire?	
- Le traitement des demandes a lieu dans un endroit sécuritaire.	
- Les renseignements personnels sont conservés dans un endroit sécuritaire.	
- Le transport et la transmission des renseignements personnels ont lieu de façon sécuritaire.	
Des mesures et des contrôles appropriés ont-ils été mis en place pour protéger les renseignements personnels?	
- Le traitement et l'utilisation des renseignements personnels sont régis par des procédures adéquates, qui sont observées par l'équipe chargée du traitement des renseignements personnels.	
CHAMP D'ENQUÊTE N^{O} 3 : COMMUNICATION DES RENSEIGNEMENTS PERSONNELS Des renseignements personnels sont-ils communiqués à des tiers sans le consentement du client, en dehors des exceptions autorisées*?* (article 8 de la *Loi sur la protection des renseignements personnels*)	
Passeport Canada communique-t-il des renseignements personnels à des organismes canadiens et/ou étrangers?	
- Tous les échanges de renseignements sont permis par la loi.	
- Des mesures de contrôle et des ententes appropriées sont en place pour chaque entente d'échange de renseignements.	
Des mécanismes de régulation de l'accès et de contrôle appropriés ont-ils été mis en place afin d'éviter la communication non autorisée de renseignements personnels?	
- L'accès aux renseignements personnels se fait uniquement en fonction du « besoin de connaître ».	
- Tous les cas de communication de renseignements à des tiers sont consignés.	
- Des mesures de contrôle appropriées ont été mises en place pour empêcher la communication de renseignements personnels à d'autres personnes que le demandeur ou les utilisateurs autorisés.	

CHAMPS D'ENQUÊTE ET CRITÈRES DE VÉRIFICATION GÉNÉRAUX	OBSERVATIONS ET CONCLUSIONS
- Le traitement et la communication des renseignements personnels font l'objet d'une surveillance et d'un examen continus de façon à cerner et à atténuer les risques d'atteinte à la vie privée.	
CHAMP D'ENQUÊTE N^{O} 4 : CONSERVATION ET ÉLIMINATION DES RENSEIGNEMENTS PERSONNELS *Les renseignements personnels semblent-ils conservés pour la période appropriée et ensuite éliminés de manière appropriée?* (Loi sur la protection des renseignements personnels*, article 6*)	
Les renseignements sont-ils conservés seulement pendant la période prescrite appropriée?	
- Il existe une période prescrite pour la conservation des renseignements.	
- Quel est le calendrier fixé pour l'élimination des demandes de passeport rejetées?	
- Les renseignements sont éliminés à la fin de la période de conservation.	
Les renseignements sont-ils éliminés de manière appropriée?	
- Une méthode d'élimination sécuritaire des renseignements a été mise en place et est observée.	
CHAMP D'ENQUÊTE N^{O} 5 : CADRE DE GESTION DE LA PROTECTION DE LA VIE PRIVÉE *Un cadre efficace de gestion de la protection de la vie privée ou une infrastructure administrative efficace semble-t-il avoir été mis en place afin de soutenir le traitement et la délivrance des passeports?* (Loi sur la protection des renseignements personnels*, article 2, et premier principe de la LPRPDE, « Responsabilité »*)	
Passeport Canada a-t-il désigné une ou des personnes tenues de rendre des comptes quant au respect par l'organisme des obligations en matière de protection de la vie privée?	
- Des responsabilités en matière de protection de la vie privée précises sont établies au sein de l'organisme.	
- La structure organisationnelle relative aux processus liés à la protection de la vie privée est officiellement et efficacement soutenue.	
- Les politiques, les lignes directrices et les règlements en matière de protection de la vie privée sont cernés, évalués et incorporés aux activités opérationnelles.	
- Les employés reçoivent-ils une formation continue au sujet de leurs obligations et de leurs droits en matière de protection de la vie privée et de sécurité?	

CHAMPS D'ENQUÊTE ET CRITÈRES DE VÉRIFICATION GÉNÉRAUX	OBSERVATIONS ET CONCLUSIONS
- Les objectifs des processus liés à la protection de la vie privée sont clairement définis, officiellement approuvés et communiqués de manière efficace.	
- Des activités et des mécanismes de contrôle relatifs aux processus liés à la protection de la vie privée pertinents et exhaustifs ont été mis en place et permettent d'atténuer des risques connus.	
- L'organisme a établi des mesures de sécurité appropriées en ce qui a trait aux renseignements personnels transférés à des tiers, y compris des ententes et des contrats appropriés, ainsi que des mesures de surveillance efficaces.	

Annexe D – Critères de vérification détaillés

Nota :

Les critères d'évaluation utilisés dans cette vérification découlent principalement des obligations énoncées aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*, dans la Politique du gouvernement sur la sécurité, ainsi que dans les politiques, les lignes directrices et les documents connexes du Conseil du Trésor qui régissent la gestion des renseignements personnels.

En outre, certains critères relatifs aux pratiques exemplaires ont été extraits et adaptés de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

Responsabilité (premier principe de la LPRPDE)

Critères :

- L'organisation doit désigner une ou plusieurs personnes qui surveilleront et coordonneront les activités de l'organisation afin de garantir que celle-ci respecte ses obligations relatives à la protection de la vie privée.

- Les personnes désignées pourront déléguer des rôles et des responsabilités spécifiques dans l'ensemble de l'organisation afin de garantir la protection de la vie privée et la sécurité des fonds de renseignements personnels que l'organisation a en sa possession.

- L'organisation doit, par voie contractuelle ou autre, s'assurer que les tierces parties à qui sont confiés des renseignements personnels fournissent un degré de protection comparable à celui qu'elle garantit.

  Nota : *Il existe des critères applicables aux ententes sur l'échange de renseignements et à l'impartition. Pour les renseignements détenus par une institution fédérale, il convient d'offrir un niveau de protection équivalent ou supérieur à ce que recommandent la* Loi sur la protection des renseignements personnels*, les politiques du gouvernement en matière de sécurité ainsi que les lignes directrices du CT.*

- Les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris : la mise en œuvre des procédures visant à protéger les renseignements personnels; la mise en place des procédures pour recevoir et traiter les plaintes et les demandes de renseignements; la formation du personnel et la transmission au personnel de l'information relative aux politiques et aux pratiques de l'organisation et la rédaction des documents explicatifs concernant leurs politiques et procédures.

  Nota : *Voir aussi les « Rôles et responsabilités » du SCT dans la Politique sur la protection des renseignements personnels pour connaître les exigences précises liées au cadre de gestion de la protection de la vie privée.*

Notification des fins auxquelles les renseignements personnels sont recueillis (paragraphe 5(3) de la *Loi sur la protection des renseignements personnels*)

Critère :

- Sous réserve des exceptions prévues au paragraphe 5(3) de la *Loi sur la protection des renseignements personnels*, les institutions fédérales sont tenues d'informer les personnes auprès de qui elles recueillent des renseignements personnels des fins auxquelles ils sont destinés.

Détermination des fins de la collecte des renseignements (deuxième principe de la LPRPDE)

Critères :

- L'organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis.
- Il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ils sont destinés.
- Avant de se servir de renseignements personnels à des fins non précisées antérieurement, les nouvelles fins doivent être précisées avant l'utilisation. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant d'utiliser les renseignements à cette nouvelle fin.
- Les personnes qui recueillent des renseignements personnels devraient être en mesure d'expliquer à la personne concernée à quelles fins sont destinés ces renseignements.

Nota : *Il peut y avoir des exceptions à ce principe lorsque la collecte des renseignements est conforme à la loi et que le fait d'indiquer à la personne concernée les fins auxquelles ces renseignements sont destinés risquerait d'avoir pour résultat la collecte de renseignements inexacts ou incomplets.*

Collecte des renseignements personnels (articles 4 et 5 de la *Loi sur la protection des renseignements personnels*)

Critères :

- Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités.
- Chaque fois que possible, les institutions fédérales doivent recueillir auprès de l'individu lui-même les renseignements personnels destinés à des fins administratives.

Consentement (troisième principe de la LPRPDE)

Critères :

- Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon à ce que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.
- Une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait.

Limitation de la collecte (quatrième principe de la LPRPDE)

Critères :

- Les organisations ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées.
- Conformément au principe de la transparence (huitième principe de la LPRPDE), les organisations doivent préciser la nature des renseignements recueillis comme partie intégrante de leurs politiques et pratiques concernant le traitement des renseignements personnels.

  Nota : *Voir aussi : Lignes directrices sur l'usage et la communication de renseignements personnels du SCT*

Utilisation des renseignements personnels (paragraphe 6(2), article 7 et paragraphe 9(4) de la *Loi sur la protection des renseignements personnels)*

Critères :

- Les institutions fédérales sont tenues de veiller, dans la mesure du possible, à ce que les renseignements personnels qu'elles utilisent à des fins administratives soient exacts, complets et à jour. (Voir également la rubrique Exactitude – sixième principe de la LPRPDE).
- À défaut du consentement de la personne concernée, une institution fédérale ne doit utiliser des renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis, ou pour des usages compatibles avec ces fins, ou encore à des fins pour lesquelles les renseignements peuvent être communiqués à l'intérieur ou à l'extérieur de l'institution conformément au paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*.
- Lorsque des renseignements personnels sont utilisés régulièrement à une fin qui ne figure pas dans la description des fichiers de renseignements personnels d'*Info Source*, une telle utilisation doit être signalée à la commissaire à la protection de la vie privée et incluse dans le prochain énoncé des utilisations régulières dans *Info Source*.

  Nota : *Voir aussi : Lignes directrices sur l'usage et la communication des renseignements personnels du SCT*

Limitation de l'utilisation, de la communication et de la conservation des renseignements personnels (cinquième principe de la LPRPDE)

Critères :

- Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis, à moins que la personne concernée n'y consente ou que la loi ne l'exige.
- Les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation.
- On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès à l'information après que la décision a été prise.
- On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées.
- Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

Utilisation – Couplage de données (Politique du Conseil du Trésor sur le couplage des données)

Critère :

- Les institutions fédérales doivent s'assurer que leurs programmes de couplage de données sont conçus et réalisés conformément aux principes relatifs à l'équité dans le traitement des renseignements prévus dans la *Loi sur la protection des renseignements personnels* et à la Politique du Conseil du Trésor sur le couplage de données.

Communication de renseignements personnels (article 8 de la *Loi sur la protection des renseignements personnels*)

Critère :

- Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent pas être communiqués à des tiers sans le consentement de la personne qu'ils concernent, sauf dans les cas particuliers énoncés au paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*.

Communication — Impartition (critères établis par le Commissariat à la protection de la vie privée du Canada)

Critères :

- Les renseignements personnels qui sont recueillis, utilisés, traités, communiqués, conservés ou détruits pour le compte d'une institution fédérale, ou dans le cadre d'un contrat avec une institution fédérale, doivent être gérés conformément aux principes relatifs à l'équité dans le traitement des renseignements prévus dans la *Loi sur la protection des renseignements personnels* et dans son *Règlement*.

- Lorsqu'un organisme ou un entrepreneur du secteur privé gère des renseignements personnels pour le compte d'une institution fédérale, le contrat doit préciser que les renseignements personnels sont réputés être sous le contrôle de l'institution fédérale et qu'ils sont assujettis à la *Loi sur la protection des renseignements personnels*.
- Le contrat doit également préciser, s'il y a lieu, de quelle manière le fournisseur de services ou l'entrepreneur vont satisfaire aux exigences de la *Loi* en matière de gestion des renseignements personnels qu'ils vont traiter pour réaliser le contrat.
- Le contrat doit aussi reconnaître le droit de la commissaire à la protection de la vie privée d'accéder aux renseignements personnels à des fins de vérifications et d'enquêtes.

Conservation et élimination (paragraphes 6(1) et 6(3) de la *Loi sur la protection des renseignements personnels* et paragraphes 4(1) et 4(2), ainsi que l'article 7, du *Règlement sur la protection des renseignements personnels*)

Critères :

- Les renseignements doivent être conservés et détruits selon les calendriers de conservation et d'élimination approuvés.
- À moins que la loi ne le prévoie autrement, ou que la personne concernée n'aie déjà donné son consentement, les renseignements personnels recueillis à des fins administratives, c'est-à-dire dans le cadre d'un processus de prise de décision concernant directement une personne, doivent être conservés pendant une période minimale de deux ans après la date de leur dernière utilisation à des fins administratives.
- Les dossiers doivent être éliminés ou détruits conformément à leur cote de sécurité.

Exactitude (paragraphe 6(2) de la *Loi sur la protection des renseignements personnels*)

Critère :

- Une institution fédérale est tenue de veiller, dans la mesure du possible, à ce que les renseignements personnels qu'elle utilise à des fins administratives soient exacts, à jour et complets.

Exactitude (sixième principe de la LPRPDE)

Critères :

- Les renseignements doivent être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient utilisés pour prendre une décision au sujet d'une personne.
- Une organisation ne doit pas systématiquement mettre à jour les renseignements personnels, à moins que cela ne soit nécessaire pour atteindre les fins auxquelles ils ont été recueillis.

Protection des renseignements personnels (articles 6, 7 et 8 de la *Loi sur la protection des renseignements personnels*)

Critères :

- Les institutions fédérales sont tenues de mettre en place des mesures de sécurité appropriées afin de garantir que, pendant toute la durée de leur cycle de vie, les renseignements personnels sous leur contrôle sont protégés et qu'ils ne sont pas vulnérables à la consultation, à l'utilisation, à la communication, à la modification ou à la destruction non autorisée.

Courriels et télécopies

Critères :

- Les renseignements personnels permettant d'identifier des personnes ne devraient pas être envoyés par courrier électronique, à moins d'être chiffrés, ni par télécopieur, sauf si le télécopieur est sécurisé et qu'il se trouve dans un lieu protégé.

  Nota : *L'envoi de renseignements personnels par courrier électronique ou par télécopieur présente des risques sur le plan de la sécurité pour plusieurs raisons. S'ils ne sont pas envoyés ou reçus de façon sécuritaire, les renseignements peuvent être interceptés ou utilisés, ou encore reçus par erreur par une personne qui n'est pas autorisée à les recevoir.*

Mesures de sécurité (septième principe de la LPRPDE)

Critères :

- Les mesures de sécurité doivent protéger adéquatement les renseignements personnels contre la perte ou le vol, ainsi que contre la consultation, la communication, l'utilisation, la modification ou la reproduction non autorisée.
- Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

  Nota : *La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements, ainsi que des méthodes de conservation.*
- Les méthodes de protection devraient comprendre des mesures adéquates : des moyens matériels, par exemple, le verrouillage des classeurs et la restriction de l'accès aux bureaux; des mesures administratives, par exemple, des autorisations sécuritaires; des mesures techniques, par exemple, l'usage de mots de passe et du chiffrement.
- Les droits d'accès aux renseignements personnels devraient être déterminés en fonction du « besoin de connaître ».

  Nota : *La nature des mesures de sécurité appropriées varie en fonction du degré de sensibilité, de la quantité, de la répartition et du format des renseignements, ainsi que des méthodes de conservation..*
- Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.
- Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès.

Accès (articles 12 à 28 de la *Loi sur la protection des renseignements personnels*)

Critères :

- Les institutions fédérales doivent donner aux citoyens et aux résidants du Canada l'accès aux renseignements personnels les concernant, lorsqu'une demande par écrit a été présentée par la personne, dans les délais prévus dans la *Loi sur la protection des renseignements personnels*, sous réserve des exceptions énoncées aux articles 18 à 28 de la *Loi*.
- Il est possible de donner accès à ses renseignements personnels à une personne en lui permettant de consulter les documents pertinents, ou en lui en remettant une copie.
- Lorsqu'une demande d'accès est rejetée, l'institution doit informer la personne que les renseignements n'existent pas ou lui indiquer l'exception prévue dans la *Loi sur la protection des renseignements personnels* en vertu de laquelle la décision a été prise. Il faut également informer, en même temps, la personne de son droit de déposer une plainte concernant le rejet de sa demande d'accès au Commissariat à la protection de la vie privée.

Accès aux renseignements personnels (neuvième principe de la LPRPDE)

Critères :

- Une organisation doit informer la personne qui en fait la demande du fait qu'elle possède des renseignements personnels à son sujet, le cas échéant. Les organisations sont invitées à indiquer la source des renseignements.
- Une organisation peut exiger que la personne concernée lui fournisse suffisamment de renseignements pour qu'il lui soit possible de la renseigner sur l'existence, l'utilisation et la communication de renseignements personnels. L'information ainsi fournie doit servir à cette seule fin.
- Une organisation qui fournit le relevé des tiers à qui elle a communiqué des renseignements personnels au sujet d'une personne devrait être la plus précise possible. S'il lui est impossible de fournir une liste des organisations à qui elle a communiqué des renseignements au sujet d'une personne, l'organisation doit fournir une liste des organisations à qui elle pourrait avoir communiqué de tels renseignements.
- Lorsque des renseignements personnels ont été transmis à un tiers, l'organisation doit s'assurer d'obtenir du tiers des copies des documents relatifs à la demande d'accès.
- Lorsque des renseignements personnels ont été communiqués dans le cadre d'une entente d'échange de renseignements, l'organisation doit s'assurer de conserver les documents originaux dans l'éventualité d'une demande d'accès à l'information.
- Une organisation qui reçoit une demande de communication de renseignements doit répondre dans un délai raisonnable et ne peut exiger, pour ce faire, que des droits minimes. Les renseignements demandés doivent être fournis sous une forme généralement compréhensible. Par exemple, l'organisation qui se sert d'abréviations ou de codes pour l'enregistrement des renseignements doit fournir les explications nécessaires.
- Lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets, l'organisation doit apporter les modifications nécessaires à ces renseignements. Les modifications peuvent exiger des corrections ou le retrait de l'information, ou l'ajout de

renseignements. S'il y a lieu, l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question.

Plaintes (article 29 et 34 de la *Loi sur la protection des renseignements personnels*)

Critères :

- Les institutions doivent coopérer avec le Commissaire à la protection de la vie privée dans ses enquêtes découlant de plaintes du public, ou d'une plainte de l'initiative du Commissaire lui-même en vertu de la *Loi sur la protection des renseignements personnels*.
- Les institutions doivent permettre à leurs représentants de témoigner verbalement ou par écrit devant le Commissaire à la protection de la vie privée.
- Les institutions doivent permettre aux représentants délégués par le Commissaire de pénétrer dans les locaux occupés par une institution fédérale, à condition de satisfaire aux normes de sécurité établies par l'institution pour ces locaux.
- Les institutions doivent permettre aux représentants délégués par le Commissaire de s'entretenir en privé avec toute personne se trouvant dans les locaux occupés par elles dans le cadre de la compétence conférée au Commissaire par la *Loi sur la protection des renseignements personnels*, selon que le Commissaire l'estime nécessaire.
- Les institutions doivent permettre aux représentants délégués par le Commissaire d'obtenir des copies ou des extraits des livres ou d'autres documents contenant des éléments utiles à l'enquête et trouvés dans les locaux.
- Les institutions doivent permettre aux représentants du Commissaire d'accéder à tous les renseignements à l'exception des renseignements confidentiels du Conseil privé de la Reine pour le Canada (paragraphe 70(1) de la *Loi sur la protection des renseignements personnels*).

Possibilité de porter plainte à l'égard du non-respect des principes (dixième principe de la LPRPDE)

Critères :

- Toute personne doit être en mesure de se plaindre du non-respect des principes (Annexe 1, LPRPDE) en communiquant avec la ou les personnes responsables de les faire respecter au sein de l'organisation concernée.
- Les organisations doivent établir des procédures pour recevoir les plaintes et les demandes de renseignements concernant leurs politiques et pratiques de gestion des renseignements personnels et y donner suite. Les procédures relatives aux plaintes devraient être facilement accessibles et simples à utiliser.
- Les organisations doivent informer les personnes qui présentent une demande de renseignements ou déposent une plainte de l'existence de procédures de recours pertinentes (y compris le droit de déposer une plainte auprès du Commissariat à la protection de la vie privée du Canada).
- Une organisation doit faire enquête sur toutes les plaintes. Si une plainte est jugée fondée, l'organisation doit prendre les mesures appropriées, y compris la modification de ses politiques et de ses pratiques au besoin.

AUTRES CRITÈRES DE VÉRIFICATION

Connaissance de la *Loi sur la protection des renseignements personnels*

Critères :

- Les employés du gouvernement qui traitent des renseignements personnels doivent connaître leurs obligations en vertu de la *Loi sur la protection des renseignements personnels*, y compris les restrictions en matière de communication des renseignements personnels.
- L'institution fédérale doit fournir aux employés la formation et la documentation appropriées sur la *Loi sur la protection des renseignements personnels* afin de garantir que les employés sont au fait de leurs obligations en matière de protection de la vie privée.

  Nota : *La conformité à l'esprit de la Loi et aux exigences particulières énoncées dans les articles 4 à 8 de la* Loi sur la protection des renseignements personnels *dépend largement du niveau de compréhension de la Loi qu'ont les personnes chargées de l'administrer pour le compte de l'institution et, dans une moindre mesure, les employés de l'institution. Le premier principe de la LPRPDE (Responsabilité) contient des dispositions semblables.*

Info Source (articles 9, 10 et 11 de la *Loi sur la protection des renseignements personnels*)

Critères :

- Les institutions fédérales doivent s'assurer que toutes les descriptions sont les plus complètes, à jour et exactes possible.

  Nota : *Comme complément des articles 4 à 8 de la* Loi sur la protection des renseignements personnels*, les articles 9, 10 et 11 de la* Loi *exigent que tous les fonds de renseignements personnels soient décrits et publiés dans* Info Source *comme fichiers de renseignements personnels ou comme catégories de renseignements personnels.*

Annexe E – Sommaire des systèmes de renseignements relatifs au passeport

Nota : *Passeport Canada est responsable du stockage et de la gestion des renseignements personnels contenus dans les trois fichiers de renseignements personnels suivants :*

Fichiers de renseignements personnels	Fonds de renseignements
Passeports réguliers et officiels	IRIS PMP Microfilm
Certificats d'identité et titres de voyage pour réfugiés	IRIS Microfilm
Fichiers de la Liste des signalements	IRIS ForeMost Stockage secondaire du SCC Interface C-41 Fichiers de sécurité

Système IRIS : Principal système électronique d'émission de passeports de Passeport Canada qui est utilisé pour la gestion du droit d'obtenir un passeport et pour la production des passeports.

Le système IRIS est un système intégré composé des bases de données électroniques suivantes :

- **Répertoire central (RC)** : index principal des documents liés aux passeports qui comprend des images numérisées de formulaires de demande de passeport et de documents justificatifs.
- **Passeport en direct (PED)** : base de données contenant les renseignements relatifs aux demandes de passeport présentées par des membres du public sur Internet au moyen de la Voie de communication protégée du Gouvernement en direct.
- **Travaux en cours (TC)** : bases de données utilisées pour le traitement et le stockage des demandes de passeport; les données sont transférées au répertoire central après l'étape de la production (c'est-à-dire une fois que les passeports ont été délivrés).
- **Liste des signalements (LS)** : base de données contenant des détails biographiques indexés (nom, date de naissance) au sujet des personnes dont la détermination du droit d'obtenir un passeport pourrait exiger un examen plus approfondi ou une enquête en vertu du Décret sur les passeports canadiens.

Système PMP : Composante relative aux passeports du système des TI COSMOS du MAECI, qui contient le système consulaire intégré. Le système PMP est utilisé pour l'enregistrement et le traitement des demandes de passeport et des documents justificatifs à l'étranger. Les données sont copiées dans le répertoire central (au Canada) de Passeport Canada une fois que le passeport a été délivré à l'étranger.

Microfilm : Des copies des demandes de passeport et des documents justificatifs étaient conservées sur microfilm jusqu'en 2002, année où le système IRIS a été conçu.

Stockage secondaire du SCC : Base de données électronique contenant des renseignements personnels sur les délinquants et les libérés conditionnels qui ont été fournis par le Service correctionnel du Canada (SCC) au sujet des personnes dont le nom apparaît dans la base de données de la Liste des signalements de Passeport Canada.

Interface C-41 : Base de données électronique contenant des renseignements personnels fournis par le ministère de la Justice du Canada en vue de l'administration de la *Loi d'aide à l'exécution des ordonnances et des ententes familiales* (projet de loi C-41) – personnes dont le nom apparaît dans la base de données de la Liste des signalements de Passeport Canada.

Fichiers de sécurité : Documents papier contenant des renseignements supplémentaires sur le droit d'obtenir un passeport et la gestion des cas – personnes dont le nom apparaît dans la base de données de la Liste des signalements, qui est utilisée par un petit nombre de fonctionnaires de la Direction générale de la sécurité de Passeport Canada.

ForeMost : Système de gestion des documents électroniques utilisé pour la conservation des documents organisationnels, y compris les documents électroniques, dont ceux concernant les personnes dont le nom apparaît dans la base de données de la Liste des signalements.