VÉRIFICATION DES PRATIQUES DE GESTION DES RENSEIGNEMENTS PERSONNELS DE L'AGENCE DES SERVICES FRONTALIERS DU CANADA

CIRCULATION TRANSFRONTALIÈRE DES DONNÉES

TABLE DES MATIÈRES

SECTION I

MESSAGES PRINCIPAUX

1.1 Nous avons constaté que l'Agence des services frontaliers du Canada (ASFC) est dotée de systèmes et de procédures pour la gestion et l'échange de renseignements personnels avec d'autres pays. Il existe toutefois plusieurs moyens de gérer plus efficacement les risques d'atteinte à la vie privée et d'assurer une responsabilité, une transparence et un contrôle plus grand en ce qui a trait à la circulation transfrontalière des données, qui consiste à recueillir ou communiquer des renseignements personnels par-delà les frontières nationales.

1.2 Les demandes d'assistance pour obtenir des renseignements que les gouvernements étrangers font parvenir par écrit à l'ASFC sont traitées conformément aux exigences. Cependant, de nombreux échanges de renseignements entre l'ASFC et les États-Unis au niveau régional sont de nature verbale et ne se sont pas accompagnés de demandes écrites. Ces échanges ne sont pas enregistrées systématiquement et ne s'inscrivent pas dans le processus d'approbation établi en vertu des politiques de l'ASFC. En outre, ils ne sont pas conformes aux modalités de l'Accord d'assistance mutuelle en matière douanière (AAMD) entre le Canada et les États-Unis du mois de juin 1984.

1.3 L'ASFC doit se doter d'une méthode coordonnée d'identification et de suivi pour tout échange transfrontalier de données. L'Agence ne peut, avec une certitude raisonnable, rendre compte de l'étendue de ses échanges des renseignements personnels, de la quantité des renseignements échangés, ni de la fréquence de ces échanges avec les États-Unis. Par extension, elle ne peut pas affirmer avec certitude que toutes les activités d'échange de renseignements sont gérées de façon appropriées et en conformité avec l'article 107 de la *Loi sur les douanes* et l'article 8 de la *Loi sur la protection des renseignements personnels*.

1.4 En règle générale, les contrôles entourant le Système d'information sur les passagers (SIPAX) et le Système intégré d'exécution des douanes (SIED) sont satisfaisants. Ces deux systèmes clés contiennent des renseignements personnels de nature délicate sur des millions de voyageurs. Les gouvernements étrangers n'ont pas directement accès à ces systèmes et les communications électroniques vers les États-Unis, en vertu des initiatives sur les voyageurs à risque élevé et des initiatives communes d'avis de signalement, sont transmises par des voies de communication protégées. Il est toutefois possible de renforcer les contrôles pour réduire davantage le risque que des renseignements personnels soient utilisés ou communiqués indûment. Plusieurs moyens existent tels que :

- terminer la mise en place d'un nouveau cadre de gestion de la sécurité que l'ASFC a amorcé;
- actualiser et préciser les rôles et les responsabilités des fonctions de TI;
- mettre à jour les droits d'accès aux systèmes;
- appliquer des moyens de contrôle de la vérification pour les renseignements imprimés se rapportant à des avis de signalement;
- mettre en place un mécanisme pour le Canada et aux États-Unis, qui garantit aux deux parties que les contrôles des systèmes et de la protection des renseignements personnels échangés sont adéquats.

1.5 L’ASFC doit envisager des moyens d’améliorer la qualité et le contrôle des données qu’elle acquiert dans le cadre de l’Initiative d’information préalable sur les voyageurs et le dossier passager (IIPV/DP) pour garantir que les renseignements personnels sont aussi exacts et complets que possible.

1.6 L’ASFC n’a pas encore évalué l’efficacité de l’Initiative d’identification des voyageurs à risque élevé (IIVRE) avec les États-Unis, car ce projet n'a pas atteint sa pleine mise en oeuvre. L’ASFC devrait plus particulièrement évaluer l’incidence des données inexactes ou incomplètes sur les objectifs d’exécution et sur les voyageurs eux-mêmes. Tant qu’elle n’aura pas évalué l’Initiative, l’ASFC ne sera pas en mesure de démontrer qu’elle a atteint son objectif et, de ce fait, que la collecte et l’utilisation d’une grande quantité de renseignements personnels sur des millions de voyageurs sont justifiées.

1.7 L’ASFC est une nouvelle organisation. Par conséquent, le moment est favorable pour qu’elle définisse et mette en œuvre un cadre détaillé de gestion de la protection de la vie privée. L’ASFC devrait notamment mettre à jour et consolider ses accords avec les États-Unis en ce qui a trait à l’échange des renseignements personnels. Elle devrait également consolider ses rapports sur les incidents relatifs à la protection de la vie privée et trouver des façons d’améliorer le suivi des activités de communication des renseignements personnels.

1.8 En dernier lieu, les activités associées à l’échange transfrontalier de données devraient être plus transparentes. À ce titre, il n’existe pas encore de tableau exhaustif et complet de ces activités révélant la nature des renseignements échangés, avec qui ces renseignements sont échangés et à quelles fins. À l’instar d’autres ministères, l’ASFC ne rend pas compte en détail de ses échanges transfrontaliers de données. Elle doit donc faire preuve de plus de transparence pour mieux informer le Parlement et la population canadienne de ses activités dans ce domaine.

1.9 Il est dans l’intérêt public d’examiner de telles questions. Nous croyons qu’une gestion ferme et responsable de la protection de la vie privée est essentielle pour répondre aux préoccupations de la population à propos de la circulation des renseignements personnels entre le Canada et d’autres pays.

SECTION II

INTRODUCTION

Contexte de la vérification

2.1 L'économie canadienne dépend en grande partie de l'échange d'information avec ses partenaires du monde entier. Bien que le Canada ait de nombreux partenaires commerciaux, c'est avec son plus proche voisin – les États-Unis d'Amérique – qu'il entretient les liens les plus étroits.

2.2 Les avancées technologiques des deux dernières décennies ont permis d'éliminer un grand nombre d'obstacles à la communication en matière d'échange d'information. Les échanges de données entre les sociétés multinationales et les gouvernements nationaux ont augmenté en même temps que la capacité accrue des bases de données et de la création de systèmes et de réseaux de communication mondiaux pouvant transmettre de l'information.

2.3 La mondialisation a poussé les nations à adopter une approche plus concertée et coordonnée relativement à la réglementation des biens et des personnes, notamment la circulation transfrontalière des données. Cela a donné lieu à un accroissement des échanges de renseignements personnels entre les gouvernements nationaux, une situation qui s'est accélérée dans les domaines de l'exécution de la loi et de la sécurité nationale à la suite des événements tragiques du 11 septembre 2001.

2.4 En réponse aux attaques terroristes du 11 septembre, les gouvernements du monde entier – dont le gouvernement du Canada – ont instauré des mesures destinées à renforcer la sécurité nationale et internationale. De façon générale, de telles mesures semblent fondées sur le principe que plus les gouvernements détiennent de renseignements sur les personnes, mieux ils pourront assurer la sécurité de la société.

2.5 Depuis les événements du 11 septembre, on fait appel à un échange d'information plus efficace entre les organismes partenaires dans l'application de la loi à l'échelle nationale et internationale, pour parer à la menace terroriste. Tous les organismes d'exécution de la loi et les organismes du renseignement doivent trouver un juste équilibre entre les mesures qui augmentent la sécurité et celles qui protègent la vie privée. Il n'en reste pas moins qu'en général, les voyageurs ne seront pas surpris de constater que le niveau de protection de la vie privée à un bureau d'entrée au Canada ne sera plus le même par rapport à celui qui existe dans la vie de tous les jours. La surveillance qu'exercent des responsables de l'ASFC sur les personnes et les biens est prévisible et elle est prévue par la loi, afin de protéger le bien-être général du Canada. En conséquence, la surveillance et l'échange d'information effectués par l'ASFC afin de gérer des frontières se passe dans un contexte global de réduction de la protection de la vie privée.

2.6 Nous avons choisi de procéder à une vérification de l'ASFC après avoir pris en considération un certain nombre de critères. Les éléments essentiels du Programme de sécurité nationale du gouvernement du Canada sont axés sur le renforcement de la frontière canado-américaine, et l'ASFC est le principal organisme chargé de la sécurité de la frontière au Canada. En décembre 2001, le Canada et les États-Unis ont signé la « *Déclaration Manley/Ridge sur la frontière intelligente* et le *plan d'action en 30 points* visant à améliorer *notre* frontière commune » sans restreindre indûment les échanges commerciaux et les

déplacements légitimes. L'objectif principal du plan était de trouver des moyens d'accroître la coopération bilatérale et l'échange de renseignements pour l'exécution de la loi entre les deux gouvernements.

2.7 Dans le cadre de son mandat de protection des frontières, l'ASFC recueille des renseignements personnels de nature délicate sur des millions de voyageurs arrivant au Canada. Cette information peut comporter des données détaillées sur les finances, les antécédents familiaux, les déplacements ainsi que des identificateurs personnels comme les numéros d'assurance sociale et de passeport. Une grande partie de cette information est conservée dans un format identifiable – copie papier (dossiers) ou dans des bases de données électroniques – et elle peut être échangée avec des gouvernements étrangers en vertu de l'article 107(8) de la *Loi sur les douanes*.

2.8 Le *Plan d'action des douanes*, lancé le 7 avril 2000, proposait une nouvelle approche pour l'exécution des dispositions douanières fondée sur la gestion des risques. Le Plan veille surtout à affecter des ressources douanières là où elles produiront les meilleurs résultats. Cette nouvelle méthode d'exécution se traduit par la collecte et l'utilisation d'une grande quantité de renseignements personnels sur les voyageurs, lesquels renseignements sont susceptibles d'être transmis par-delà des frontières. Du coup, l'augmentation de la quantité de renseignements personnels recueillis, utilisés et communiqués entraîne inévitablement un accroissement des répercussions sur la vie privée.

2.9 En dernier lieu, la *Politique de sécurité nationale* du gouvernement du Canada, annoncée le 27 avril 2004, faisait état d'un financement additionnel destiné aux mesures de sécurité frontalière, notamment des ressources accrues pour la recherche de renseignements par l'ASFC et la création d'un Centre national d'évaluation des risques (CNER) afin de faciliter l'échange de données liées au renseignement et aux avis de signalement avec les États-Unis (voir le paragraphe 3.58 pour une brève explication du terme « avis de signalement ».

Pourquoi cette vérification est-elle importante?

2.10 Dans un contexte où la responsabilité de garantir le droit à la protection de la vie privée des personnes incombe aux gouvernements, et où un grand nombre de ceux-ci assurent à leurs citoyens des niveaux de protection variables, la circulation transfrontalière des renseignements personnels pose des défis particuliers en matière de protection de la vie privée. Comment, par exemple, le gouvernement du Canada peut-il, considérant les limites territoriales de l'application des lois, garantir que l'information qu'il partage avec un gouvernement étranger jouira du même niveau de protection qu'au Canada? Les principes généralement admis de protection des données seront-ils reconnus et respectés?

2.11 Cette vérification est particulièrement importante pour plusieurs raisons. Premièrement, la circulation transfrontalière de renseignements personnels comporte de sérieux risques d'incidence sur la vie privée liés aux différences juridictionnelles des pratiques sur la protection des renseignements personnels, la sécurité des données personnelles en transit, et la pertinence des outils qui gouvernent la gestion des renseignements personnels échangés. À cet égard, nous considérons que les modalités énoncées dans les accords bilatéraux d'échange d'information constituent des aspects importants de contrôle et de gestion pour la circulation transfrontalière des données.

2.12 Deuxièmement, tout indique que la population canadienne est préoccupée par l'échange transfrontalier des renseignements personnels les concernant avec les États-Unis. Selon une

étude du Commissariat commandée en 2004, 75 p. 100 des personnes interrogées croyaient que le gouvernement du Canada transférait les renseignements personnels des citoyens à des gouvernements étrangers aux fins de la sécurité nationale et 85 p. 100 des personnes indiquaient qu'elles étaient modérément ou très préoccupées par ces divulgations. Dans le même ordre d'idées, bon nombre d'entre elles se disaient inquiètes de l'exploration des données, du profilage racial, de l'accès direct des gouvernements étrangers aux bases de données canadiennes (notamment les États-Unis) et des utilisations secondaires de l'information personnelles.

2.13 Troisièmement, puisque les organismes responsables de l'application de la loi et de la sécurité nationale à l'échelle mondiale recueillent davantage d'information sur un plus grand nombre de personnes auprès d'une quantité accrue de sources, et comme ces organismes utilisent ces renseignements pour déceler les menaces potentielles, un risque subsiste que des données incomplètes ou inexactes entraînent des conséquences indésirables telles que la surveillance injustifiée des personnes.

À propos de l'Agence des services frontaliers du Canada

2.14 Une partie du portefeuille de l'Agence des services frontaliers du Canada (ASFC) a été créée le 12 décembre 2003 et fait partie du portefeuille de la Sécurité publique et Protection civile (SPPC). L'ASFC englobe le programme des douanes de l'ancienne Agence des douanes du revenu du Canada (ADRC); les fonctions liées à l'exécution de la loi, au renseignement et à l'interception relevant de Citoyenneté et Immigration Canada (CIC), et les principales fonctions d'inspection des aliments et des plantes de l'Agence canadienne d'inspection des aliments (ACIA).

2.15 Le mandat législatif de l'ASFC consiste à faciliter la circulation transfrontalière des personnes et des biens légitimes, au bénéfice de l'économie canadienne, tout en arrêtant les personnes et les biens représentant un risque potentiel à la sécurité du Canada, ou de ses alliés, ou qui ne se conforment pas aux lois canadiennes sur les douanes et l'immigration et à d'autres lois. L'ASFC administre plus de 90 lois qui régissent les échanges commerciaux et les voyageurs.

2.16 En étant la première ligne de défense en matière de gestion et de la circulation des personnes et des biens à destination ou en partance du Canada; les opérations de l'ASFC se font dans quelque 1 200 points de services à travers le Canada et dans 39 emplacements à l'étranger. Elle a une présence en tout temps dans plus de 119 postes frontaliers et 9 aéroports internationaux. Au cours du dernier exercice financier, les quelque 12 500 employés de ASFC ont traité plus de 12 millions d'expéditions et 95 millions de visiteurs arrivant au Canada – par voie terrestre, aérienne ou maritime. Durant cette période, l'ASFC a traité les dossiers d'immigration de plus de deux millions de personnes.

2.17 L'Administration centrale de l'ASFC est située à Ottawa. Ses différentes activités sont réparties dans les huit régions suivantes : Atlantique, Québec, Grand Toronto, Niagara Falls/Fort Erie, Windsor/St. Clair, Nord de l'Ontario, Prairies et Pacifique.

2.18 L'ASFC disposait d'un budget de 1,06 milliard de dollars pour l'exercice financier qui a pris fin le 31 mars 2005 pour exécuter son mandat lié aux frontières. Pour de plus amples renseignements sur l'ASFC, veuillez consulter les rapports publiés sur son site Web à l'adresse suivante : www.cbsa.asfc.gc.ca.

2.19 Au moment où nous avons effectué la vérification, l'ASFC se constituait en nouvel organisme, de sorte que les systèmes et les procédures nécessitaient des ajustements. Nous sommes conscients qu'il y a beaucoup à faire au cours d'une telle période de transformation, et que les gestionnaires ont dû travailler fort pour apprendre et s'adapter. Par ailleurs, il est possible qu'une certaine confusion ou une incertitude demeure au sein de la direction et du personnel de l'Agence quant aux rôles, aux responsabilités et au fonctionnement des systèmes de l'organisme. Il importe toutefois de comprendre que la circulation transfrontalière des données est essentielle à un grand nombre de programmes et activités quotidiennes de l'Agence. Cependant, ni l'Agence ni l'ensemble du gouvernement fédéral n'a encore envisagé cette question sous l'angle de la gestion collective et de la responsabilité.

Objectif, critères, portée et approche de la vérification

2.20 Les objectifs nationaux en matière de sécurité et de protection de la vie privée sont souvent considérés comme des valeurs qui se font contrepoids; par exemple lorsque une augmentation de la sécurité entraîne une diminution de la vie privée. La présente vérification se fonde sur l'hypothèse selon laquelle les objectifs nationaux liés à la sécurité et les saines pratiques de gestion des renseignements personnels, sont intimement liés.

2.21 Sous-jacente à cette hypothèse repose la conviction selon laquelle un cadre structuré de responsabilisation et de contrôle de la gestion des renseignements personnels limitera les risques d'atteinte à la vie privée et en même temps appuiera les objectifs se rapportant à la sécurité nationale et à l'exécution de la loi. Autrement dit, les mesures de sécurité qui respectent la protection de la vie privée n'en seront que plus efficaces.

Objectif :

Évaluer la mesure par laquelle l'ASFC contrôle et protège adéquatement les échanges transfrontaliers des renseignements personnels des Canadiennes et des Canadiens avec des gouvernements étrangers ou leurs institutions.

Critères :

2.22 Des critères précis ont été élaborés pour la vérification. Ils ont ensuite été transmis à l'ASFC, qui a indiqué son accord.

Les critères sont énoncés à l'annexe B du rapport.

Afin de déterminer les critères de vérification, nous nous sommes appuyés sur les outils suivants :

- Les pouvoirs stipulés dans la *Loi sur les douanes* (p. ex. l'article 107);
- Les dispositions sur la collecte, l'utilisation, la conservation et la destruction qui figurent dans les articles 4 à 8 de la Loi sur la protection des renseignements personnels;
- Les dix principes internationaux relatifs à l'équité dans le traitement des renseignements personnels, lesquels principes sont définis dans l'annexe 1 de la Loi sur la protection des renseignements personnels et les documents électroniques (*LPRPDÉ*); et

- Les politiques, lignes directrices et directives du Conseil du Trésor sur la gestion des renseignements personnels.

Portée :

2.23 En raison de l'ampleur et de la complexité de l'ASFC et de sa réorganisation qui était en cours lors de notre vérification, nous avons débuté notre travail en déterminant la portée des nombreux programmes et activités de gestion de l'information de l'Agence. Nous avons procédé avec cet exercice afin d'identifier les aspects du programme où l'incidence sur la vie privée de la population canadienne sera vraisemblablement la plus importante, pour ensuite y concentrer notre attention. Gardant à l'esprit les ressources dont nous disposions pour effectuer la vérification, les activités visant à identifier la portée des programmes et activités de gestion de l'information de l'Agence portaient principalement sur les programmes concernant les voyageurs plutôt que sur les programmes commerciaux de l'ASFC. Nous avons également concentré nos efforts sur les activités douanières et les activités de renseignements aux postes frontaliers et aux aéroports. L'examen ne portait pas sur les activités maritimes, ferroviaires ou postales de l'Agence.

2.24 Nos activités visant à déterminer la portée de la vérification nous ont amenés à choisir les quatre programmes et systèmes d'information suivants :

- Activités d'exécution des mesures douanières et les activités de renseignements (postes frontaliers et aéroports);
- Système intégré d'exécution des douanes (SIED);
- Système d'information sur les passagers (SIPAX);
- Centre national d'évaluation des risques (CNER).

2.25 Outre ces quatre domaines principaux, la vérification a porté sur le cadre de gestion en matière de protection de la vie privée à l'ASFC ainsi que sur la mesure par laquelle l'Agence fait rapport au Parlement et à la population canadienne de ses activités dans le domaine de la circulation transfrontalière des données.

2.26 Bien que les activités d'immigration liées à l'application de la loi, aux renseignements et à l'interdiction exigent également l'échange transfrontalier de renseignements personnels; les changements organisationnels pour favoriser l'intégration de ces activités à celles de l'ASFC n'avaient pas été menés à terme au moment de notre vérification. Il en va de même pour le principal programme d'inspection des plantes et des aliments, qui a été transféré de l'ACIA à l'ASFC. Par conséquent, ce programme ainsi que les autres cités ci-dessus n'ont pas été examinés lors de la vérification.

2.27 Par ailleurs, nous n'avons pas examiné le programme NEXUS. Dans le cadre de ce programme, les renseignements personnels des voyageurs sont assujettis à un examen approfondi, ce qui favorise leur entrée rapide au Canada et aux Etats-Unis. L'inscription au programme NEXUS est fait sur une base volontaire. En outre, la collecte, l'utilisation et la communication des renseignements personnels dans le cadre du programme NEXUS ne se fait qu'avec le consentement explicite du participant.

2.28 En terminant, il est à noter que la Commissaire à la protection de la vie privée ne dispose d'aucun pouvoir légal à l'extérieur du Canada. Par conséquent, nous n'avons pas effectué une vérification du contrôle et de l'utilisation des renseignements personnels une fois que ceux-ci ont franchi la frontière canado-américaine.

Approche :

2.29 Nous avons fait des entrevues avec 108 employés de l'ASFC. Parmi les personnes que nous avons interrogées, figuraient des cadres supérieurs et des agents de programme à l'Administration centrale de l'ASFC, des gestionnaires et des employés du Centre national d'évaluation des risques, des directeurs régionaux, des chefs de division, des surintendants des douanes, des agents des douanes, des agents régionaux du renseignement, des analystes régionaux du renseignement et des enquêteurs régionaux des douanes dans les trois régions où nous nous sommes rendus au cours de la vérification – Québec, Windsor-St.Clair, et Pacifique.

2.30 En plus d'interviewer certains employés choisis, l'équipe chargée de la vérification a examiné un échantillon des dossiers d'exécution des mesures douanières (p. ex., les rapports de saisie, les données des fichiers du Système de gestion du renseignement (SGR), les bloc-notes des agents, les fichiers de demande d'assistance et les mesures de surveillance communes entre le Canada et les États-Unis). Puisque l'ASFC n'est pas en mesure, à l'heure actuelle, d'identifier facilement tous les dossiers contenant des échanges transfrontaliers – plus particulièrement ceux qui comportent de l'information communiquée verbalement – l'équipe de vérification n'a pu choisir au hasard certains types de dossiers aux fins de la vérification. Nous avons dû nous fier aux responsables des programmes pour le choix des dossiers, en fonction des cas particuliers dont ils se souvenaient, basé sur des recherches qu'ils avaient effectuées dans leurs dossiers respectifs (p. ex., les bloc-notes). Ils nous ont ensuite présenté les dossiers pour notre examen.

2.31 L'équipe de vérification a également examiné les protocoles d'entente (PA) et les traités qui établissent le cadre de divulgation des renseignements des douanes aux gouvernements étrangers, ainsi que les politiques et les procédures internes, le matériel didactique, les évaluations des facteurs relatifs à la vie privée (EFVP) et les outils d'élaboration des rapport de l'ASFC (p. ex., les rapports sur les plans et les priorités).

2.32 Notre vérification effectuée sur le terrain s'est terminée, pour l'essentiel, en novembre 2005. Par conséquent, les observations et les recommandations figurant dans ce rapport s'appliquent à partir de cette date.

2.33 Dans le cadre de notre approche, nous avons mis sur pied un Comité consultatif de vérification. Ce Comité, constitué de quatre personnes, a apporté sa vaste expertise dans les domaines de la protection de la vie privée, de l'exécution de la loi, de la sécurité, de la technologie de l'information et de l'administration publique. Le Comité a fourni des conseils et des orientations à l'équipe à plusieurs étapes de la vérification.

2.34 Après avoir terminé l'étape d'examen de la vérification, nous avons transmis verbalement nos conclusions à la direction de l'ASFC. Les ébauches de notre rapport ont été réviser par les gestionnaires de l'ASFC afin de s'assurer de l'exactitude des faits et pour obtenir les réponses de l'Agence sur nos observations et nos recommandations.

2.35 Quelques-unes de nos observations portent sur des questions qui sont particulièrement délicate de nature et elles ont été exclues de ce rapport public, dans le but de protéger l'information qui concerne l'ASFC. Ces observations et ces recommandations ont été communiqués séparément à l'ASFC dans une lettre adressée aux gestionnaires. Nous allons faire un suivi des efforts de l'ASFC afin de répondre à ces questions, dans le cadre de notre suivi à ce rapport de vérification.

2.36 Nous tenons à remercier les responsables de l'ASFC de leur collaboration durant la vérification et pour leur réceptivité à l'égard de notre travail.

Structure du rapport :

2.37 La section III de ce rapport – Observations et Recommandations – traite des quatre programmes et des systèmes d'information mentionnés précédemment, soit, le/les : Activités d'exécution des douanes et de renseignement (postes frontaliers et aéroports); Système intégré d'exécution des douanes (SIED); Système d'information sur les passagers(SIPAX) et Centre national d'évaluation des risques (CNER).

Nous donnons au besoin leur historique pour chaque programme, initiative ou système, ou nous en faisons une courte description. Nous formulons ensuite des observations sur la circulation transfrontalière des renseignements personnels et leurs échanges aux gouvernements étrangers. Enfin, nous présentons nos recommandations relativement à un ensemble d'observations spécifiques.

Équipe de vérification :

Trevor Shaw – directeur général, Vérification et revue

Tom Fitzpatrick
Michael Fagan
Robert Bedley
Douglas Marshall

Membres du Comité consultatif de vérification externe :

John L'Abbe :	Consultant à la sécurité, Services de consultation L'Abbe (Sous-commissaire de la GRC – à la retraite)
John Hopkinson :	Consultant en sécurité des systèmes informatiques (EWA Information and InfrastructureTechnologies Inc.)
David Flaherty :	Consultant à la protection de la vie privée et à l'accès à l'information (Ancien commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique)
Denis Morency :	Consultant à la protection de la vie privée (Ancien directeur général de la Commission d'accès à l'information du Québec)

SECTION III

OBSERVATIONS et RECOMMANDATIONS

ACTIVITÉS D'EXÉCUTION DE LA LOI ET LES RENSEIGNEMENTS DES DOUANES (POSTES FRONTALIERS ET AÉROPORTS)

Contexte :

3.1 Les principaux volets de l'ASFC se rapportant à l'exécution de la loi sont les enquêtes et les programmes de renseignement et d'interception conçus pour faire face aux cas présumés d'évasion fiscale, de contrebande, de fraude, de terrorisme, de blanchiment d'argent et autres infractions aux lois dont l'Agence est chargée d'assurer l'application.

3.2 La Direction générale de l'exécution de la loi à l'Administration centrale de l'ASFC est responsable de l'élaboration des procédures, des stratégies et des politiques opérationnelles nationales liées au programme d'exécution de l'Agence.

Elle a aussi les responsabilités suivantes :

- recueillir, analyser et diffuser de l'information concernant les menaces à la sécurité des frontières du Canada;
- fournir des services d'orientation et de soutien fonctionnel aux employés de l'ASFC des bureaux frontaliers et intérieurs au Canada;
- servir de point de convergence pour les relations de l'ASFC avec les organismes nationaux et étrangers de sécurité, d'application de la loi et du renseignement; et
- élaborer et gérer de nouveaux programmes en collaboration avec des partenaires internationaux

3.3 La Direction générale comporte quatre directions : la Direction de l'exécution, la Direction du renseignement et de la gestion du risque, la Direction de l'élaboration des politiques et des programmes et la Direction des services de gestion. Tandis que l'Administration centrale de l'ASFC fournit des services d'orientation fonctionnelle, la mise en application du programme relève, quant à elle, des régions. Les chefs régionaux de l'ASFC ont en effet la responsabilité de surveiller les activités liées au renseignement et à la sécurité à la frontière, dans leurs sphères de compétences respectives.

3.4 Les opérations d'exécution comprennent la gestion des points d'entrée aériens, maritimes et terrestres pour la circulation de voyageurs et de marchandises. Bien que la structure organisationnelle puisse varier légèrement d'une région à l'autre, les programmes d'exécution contiennent tous les mêmes volets généraux – c'est-à-dire les renseignements (douanes et immigration), les enquêtes (fraude douanière) et l'application de la loi en matière d'immigration.

Renseignements personnels :

3.5 La *Loi sur les douanes* définit le « renseignement douanier » comme un renseignement de toute nature et sous toute forme qui :

(a) soit concerne une ou plusieurs personnes et est obtenu, selon le cas, par le ministre ou pour son compte pour l'application de la *Loi sur les douanes* ou du *Tarif des douanes*;
(b) soit est tiré d'un renseignement visé à l'alinéa *a*).

3.6 Par définition, le renseignement douanier a une vaste portée. Sans être exhaustive, la liste suivante donne une idée du type de renseignements personnels que l'ASFC recueille et qui pourraient, par conséquent, faire l'objet d'une communication transfrontalière :

- renseignements biographiques – nom, date et lieu de naissance;
- adresse et numéros de téléphone (résidentiel, cellulaire);
- renseignements relatifs à une infraction;
- information sur les méthodes de dissimulation, *modus operandi* de l'individu, informations sur les marchandises les plus susceptibles d'être passées en contrebande, historique des déplacements, notes de surveillance; et
- autres renseignements tels que le numéro d'immatriculation d'un véhicule, de l'information préalable sur les voyageurs (IPV), le dossier passager (DP) ainsi que de l'information sur l'emploi et les finances.

Circulation transfrontalière de renseignements personnels :

3.7 En s'acquittant de son mandat au chapitre de la protection de la frontière, l'ASFC recueille des renseignements personnels de diverses sources. En plus de la collecte directe de renseignements – c'est-à-dire auprès de la personne que l'information concerne – l'Agence recueille des renseignements auprès des entreprises de transport aérien, d'autres ministères et organismes gouvernementaux, des organismes nationaux du renseignement et d'exécution de la loi, des gouvernements étrangers et de leurs établissements. L'ASFC obtient en outre des renseignements du grand public grâce à un service en ligne sans frais.

3.8 L'ASFC peut également recueillir de l'information grâce à des indices en provenance de points d'entrée douaniers, des activités de surveillance, de sources humaines et par l'exécution de mandats. De plus, l'ASFC a accès à l'information contenue dans un certain nombre de bases de données externes, incluant : le Centre d'information de la police canadienne (CIPC); le Système de soutien des opérations des bureaux locaux (SSOBL) – une base de données de Citoyenneté et Immigration Canada; le Système de rapports sur les renseignements judiciaires (SRRJ) – bientôt remplacé par le Système d'incidents et de rapports de police (SIRP); le National Crime Information Centre (NCIC) des États-Unis, soit l'équivalent américain du système canadien CIPC.

3.9 Les renseignements personnels recueillis en vertu du programme d'exécution des mesures douanières de l'ASFC sont conservés en formats papier et électronique. En plus des systèmes SIPAX et le SIED (examinés dans le cadre de la vérification), les membres du personnel de l'exécution peuvent, selon leur rôle et leur secteur de responsabilité, utiliser les systèmes suivants dans l'exercice de leurs fonctions :

Système de rapports des événements (SRE)	– un système de rapports électroniques permettant aux inspecteurs des douanes de transmettre de l'information au personnel du renseignement
Système de gestion des renseignements (SGR)	– le dépôt de toute information et dont l'accès est restreint au personnel du renseignement
Système de gestion de l'information des enquêtes des douanes (SGIED)	– un système de gestion du suivi des dossiers, utilisé par le personnel des enquêtes, qui saisit le résumé de conclusions d'enquête, des données de base (nom, adresse, date de naissance) ainsi que les dates de poursuites du bureau principal

Communication de renseignements à des gouvernements étrangers :

3.10 Selon le paragraphe 107(8) de la *Loi sur les douanes*, des renseignements douaniers peuvent être fournis à un gouvernement étranger, à une organisation internationale créée par les gouvernements de divers états, à une communauté d'états ou à une institution d'un tel gouvernement ou d'une telle organisation. Toute communication d'information doit se faire :

- conformément à une convention ou une entente internationale, ou à tout autre accord international écrit conclu entre le gouvernement du Canada ou l'une de ses institutions et le gouvernement de l'état étranger, l'organisation internationale ou la communauté d'états;
- seulement aux fins énoncées dans l'entente en question.

3.11 Il n'est pas nécessaire que les ententes internationales en matière d'échange d'information traitent uniquement de l'échange de renseignements douaniers. Toutefois, les ententes doivent permettre la communication ou l'échange de tels renseignements.

3.12 De nombreux accords bilatéraux entre les agences de douanes de différents pays ont pour objet d'établir des protocoles régissant leur coopération et leur entraide mutuelle. Le Canada a vingt accords écrits de collaboration internationale. Six d'entre eux sont des accords d'assistance mutuelle en matière douanière (AAMD). Les AAMD doivent être approuvés par décret du Gouverneur en Conseil; ils ont le caractère juridique d'un traité et sont exécutoires en vertu de la loi. Il s'agit d'accords entre les gouvernements. Le Canada a un accord d'assistance mutuelle en matière douanière (AAMD) avec les États-Unis, le Mexique, la Corée du Sud, l'Union européenne, la France et l'Allemagne. Les autres accords de collaboration écrits sont entre les administrations douanières.

3.13 Le Canada a en outre conclu des traités d'entraide juridiques (TEJ) avec 31 pays. Il convient de noter que les TEJ régissent l'aide juridique globale, en matière criminelle, entre les pays. Cependant, ces traités ne relèvent pas uniquement de la responsabilité de l'ASFC; ils sont gérés de concert avec le ministère des Affaires étrangères et du Commerce international et le ministère de la Justice du Canada.

3.14 Les fonctionnaires autorisés à approuver la communication de renseignements douaniers en vertu des autorités désignées en vertu de l'article 107 de la *Loi sur les douanes* sont désignés dans les politiques et lignes directrices de l'ASFC.

Il y aurait lieu de renforcer certains accords régissant l'échange de renseignements entre le Canada et les États-Unis afin de fournir des mesures accrues de protection des données.

3.15 Les AAMD et les TEJ entre le Canada et les États-Unis existent depuis longtemps. À notre avis, leur mise à jour est essentielle. Non seulement ces accords font référence à des organismes de douanes qui n'existent plus, mais ils n'abordent pas de manière satisfaisante la gestion des renseignements personnels. Pour appuyer ce point de vue, il suffit d'examiner des AAMD avec d'autres pays, lesquels accords contiennent, eux, des mesures de protection des données accrues. Toutefois, même ces accords, bien qu'ils soient plus acceptables, pourraient faire l'objet d'améliorations.

3.16 L'AAMD entre le Canada et les États-Unis établissant l'assistance mutuelle et la coopération entre leurs administrations douanières respectives a été signé le 20 juin 1984. L'accord d'assistance mutuelle en matière douanière définit l'« administration douanière » au Canada comme étant le ministère du Revenu national, Douanes et Accise. La preuve que le document n'est plus à jour est que le ministère a été remplacé depuis par l'Agence des douanes et du revenu du Canada (ADRC) et, plus récemment, par l'ASFC. De la même façon, l'administration douanière des États-Unis est définie comme le United States Customs Service, Department of Treasury (service des douanes américain, département du Trésor). Aux États-Unis, le service des douanes relève en grande partie de la Customs and Border Protection Agency rattachée au Department of Homeland Security (département de la Sécurité intérieure).

3.17 L'AAMD entre le Canada et les États-Unis stipule que les demandes de renseignements doivent se faire par écrit et inclure les éléments suivants :

- l'identité de l'organisme requérant;
- la nature de l'enquête;
- les noms et les adresses des parties concernées par la demande;
- l'objet de la demande et les questions juridiques en jeu; et
- le but et les motifs de la demande.

3.18 Il convient de noter que même si les demandes de renseignements douaniers doivent se faire par écrit, il existe une exception pour les demandes urgentes, c'est-à-dire lors de situations où il faut agir rapidement. L'accord requiert seulement que les demandes verbales d'assistance soient confirmées par écrit, à la demande de l'autre partie. L'accord stipule également que les documents, les renseignements et les communications doivent demeurer confidentiels et être protégés contre la divulgation en vertu des lois du pays receveur.

De plus, l'utilisation des documents, des renseignements et des communications à des fins autres que celles prévues dans l'accord nécessite le consentement écrit préalable de l'autre administration douanière.

3.19 Tel que mentionné précédemment, la vérification du Commissariat incluait une analyse comparative d'un certain nombre d'AAMD que le Canada a conclus avec d'autres pays. À titre

d'exemple, l'AAMD entre le Canada et l'Union européenne (UE) – qui est entré en vigueur en 1997 – accorde une attention accrue au traitement des renseignements personnels et offre en général une meilleure protection des données que l'AAMD entre le Canada et les États-Unis. À la différence l'AAMD entre les États-Unis et le Canada, celui entre le Canada et l'UE stipule que même si une demande verbale peut être faite dans certaines circonstances, une confirmation de cette demande est exigée. L'accord entre le Canada et l'UE inclut également le principe de la nécessité d'accès – c'est-à-dire que la communication de renseignements entre les représentants des douanes de chaque pays doit se faire seulement en fonction du principe du besoin de connaître. L'accord limite en outre les communications concernant les demandes aux fonctionnaires désignés spécifiquement.

3.20 De plus, l'article 16 de l'AAMD entre le Canada et l'UE stipule que les renseignements échangés seront traités de manière confidentielle. Il précise également que les renseignements fournis feront l'objet d'une protection similaire à celle qui est accordée non seulement en vertu des lois du pays receveur, mais aussi en fonction de celles du pays qui a fourni l'information. Cela signifie que les renseignements que le Canada fournit à un pays de l'UE doivent être traités conformément aux lois canadiennes relatives à la protection des renseignements personnels et aux lois du pays de l'Union européenne concerné.

3.21 À l'instar de l'AAMD entre le Canada et les États-Unis, l'accord entre le Canada et l'UE précise également que les renseignements ne peuvent être utilisés, sans consentement préalable, à des fins autres que celles précisées dans l'entente. De plus, l'article 16 stipule que le pays qui fournit l'information peut établir des restrictions supplémentaires se rapportant à un tel usage secondaire des renseignements.

3.22 Le TEJ entre le Canada et les États-Unis a été signé en mars 1985. En vertu de ce traité, les demandes d'assistance doivent inclure, entre autres, l'objet de l'enquête, une description ainsi que le but de la demande de renseignements, des éléments de preuve et de l'assistance recherchés, de même que toutes les exigences en matière de confidentialité. À moins d'y être autrement autorisé par le pays requérant, le pays répondant doit faire « de son mieux » afin de préserver la confidentialité des demandes et de leur contenu. Le traité stipule qu'un pays peut exiger que les renseignements demeurent confidentiels ou que leur communication ou leur utilisation fasse l'objet de certaines restrictions. De plus, il est interdit au pays requérant d'utiliser ou de communiquer les renseignements fournis, sans consentement préalable, à des fins autres que celles figurant dans la demande.

3.23 La vérification du Commissariat incluait un examen d'autres TEJ, dont le traité d'octobre 2004 entre le Canada et l'Allemagne. Comparativement au traité entre le Canada et les E.-U., le TEJ entre le Canada et l'Allemagne prévoit des mesures de protection accrues relativement à toute demande de renseignements. Selon ces mesures, les demandes de renseignements doivent inclure les éléments suivants :

- l'identité des personnes faisant l'objet de l'enquête et, si possible, une liste des questions et des précisions concernant tout droit de cette personne de refuser de fournir des éléments de preuve;
- une description de la présumée infraction et une mention des dispositions législatives y afférentes; et
- l'objet de l'examen auquel les personnes seront soumises.

3.24 Le TEJ entre le Canada et l'Allemagne stipule également que l'utilisation des renseignements personnels échangés dans le cadre du traité se limite aux fins pour lesquelles

ils sont transmis, à la prévention et à la sanction des infractions liées au traité, aux procédures administratives et aux procédures devant un tribunal civil, et pour éviter des menaces graves à la sécurité publique. Toute autre utilisation nécessite le consentement préalable du pays qui transmet l'information.

3.25 En vertu de ce même TEJ, le pays qui reçoit l'information doit informer le pays qui la transmet de toute utilisation secondaire de l'information. Les deux parties doivent traiter l'information soigneusement et garantir que les renseignements qu'ils fournissent sont exacts et complets. Si l'une des parties se rend compte que les renseignements qu'elle a fournis sont inexacts, elle doit en aviser l'autre pays qui est alors responsable de corriger l'information ou de la retourner. L'échange de renseignements se limite à ceux liés à la demande. Les parties doivent conserver un dossier approprié de la transmission et de la réception de renseignements personnels et protéger les renseignements contre tout accès, modification ou communication non autorisés.

3.26 Parmi les accords que nous avons examinés, un seul requiert que les processus de traitement des renseignements personnels fassent l'objet d'une vérification. La vérification de ces processus garantirait aux deux pays que les signataires respectent les conditions générales des traités. Le protocole d'entente sur l'échange automatisé d'avis de surveillance et l'échange d'information préalable sur les voyageurs – signé en mars 2005 – requiert que les participants s'assurent que des mécanismes de vérification et de suivi sont en place pour la protection des renseignements. Toutefois, le protocole d'entente n'oblige pas les organismes à échanger les résultats de la vérification avec l'autre partie dans le but de fournir la garantie que les obligations sont respectées en vertu du protocole d'entente.

3.27 Nous croyons que l'idée d'une garantie réciproque ou mutuelle concernant la protection des renseignements personnels est importante non seulement pour les renseignements des Canadiennes et des Canadiens échangés avec les États-Unis, mais aussi pour les Américains dont des renseignements personnels peuvent être communiqués au Canada. Un système d'assurance mutuelle pourrait exiger que chacun des pays fournissant de l'information à l'autre précise les mécanismes de contrôle internes au sein de son administration visant à protéger les renseignements personnels. En vertu d'un tel système, les parties pourraient en outre devoir effectuer des vérifications internes de la sécurité et des mesures de protection des renseignements personnels, et s'échanger les résultats obtenus. Ces pratiques permettraient à chaque pays de garantir à l'autre pays l'efficacité de son système de protection des données. Elles permettraient également aux parties de s'entraider en matière de pratiques et de principes adéquats de protection des données.

Recommandation 1 :

En vue de renforcer son cadre de gestion de la protection des renseignements personnels, il est recommandé que l'ASFC s'efforce de mettre à jour et de consolider ses protocoles d'entente sur l'échange de renseignements personnels avec les États-Unis, ce qui comprendrait la mise en place de processus offrant une garantie mutuelle que la circulation transfrontalière de renseignements personnels fasse l'objet de mesures de protection appropriées.

Réponse de l'ASFC :

À court terme, l'ASFC créera un cadre de gestion de la protection des renseignements personnels afin d'orienter l'élaboration de politiques; elle envisagera la création d'un plan pour mettre à jour les accords d'assistance mutuelle en matière douanière (AAMD). L'Agence examinera les éléments du cadre de gestion de la protection des renseignements personnels déjà en place et verra à préciser les rôles et les responsabilités liés à la protection des renseignements personnels. Nous élaborons actuellement des directives pour l'élaboration d'accords de collaboration écrits qui prennent en compte les avis fournis par le Commissariat à la protection de la vie privée (CPVP). À long terme, nous passerons en revue les directives afin d'orienter les activités d'accès, d'utilisation et de communication des renseignements personnels à des gouvernements étrangers.

Les demandes écrites d'assistance en provenance des gouvernements étrangers contiennent les éléments requis établis en vertu des accords d'assistance mutuelle en matière douanière (AAMD); les demandes ont été traitées conformément au paragraphe 107(8) de la* Loi sur les douanes *et aux politiques de l'ASFC.

3.28 La responsabilité de répondre aux demandes d'assistance d'autres pays en vertu des accords d'assistance mutuelle en matière douanière relève principalement de la Direction générale de l'exécution de l'ASFC. Selon la nature de l'aide recherchée, la Division des enquêtes douanières ou la Division de la contrebande et des services du renseignement traitera la demande. Sauf pour les requêtes en provenance des États-Unis, c'est l'Administration centrale de l'ASFC qui coordonne toutes les demandes d'assistance de l'étranger, en vertu des AAMD.

3.29 En novembre et décembre 2003, l'Agence des douanes et du revenu du Canada (ADRC) a émis des directives opérationnelles provisoires, soit les *Mémorandums provisoires D1-16-1 et D1-16-2*. En plus de présenter une description clause par clause de l'article 107 de la *Loi sur les douanes*, les directives fournissent des conseils sur l'utilisation des renseignements douaniers au sein de l'Agence. Elles couvrent également la communication de tels renseignements à des organismes externes, nationaux et étrangers. Les mémorandums complètent l'information comprise dans les AAMD et TEJ de l'ASFC.

3.30 Le *Mémorandum D1-16-2* identifie les fonctionnaires autorisés à communiquer des renseignements douaniers en vertu des nombreuses clauses de l'article 107 de la *Loi sur les douanes*. Ce mémorandum n'a pas été modifié depuis que l'ADRC l'a créé, et l'équipe de vérification a été informée que les dispositions demeuraient en vigueur comme politique opérationnelle de l'ASFC.

3.31 À titre d'échantillonnage exploratoire ou de dépistage, nous avons examiné 80 dossiers d'entraide internationale. Même si notre examen se concentrait sur la circulation transfrontalière de renseignements personnels entre l'ASFC et les États-Unis, il incluait également un échantillon de requêtes d'autres gouvernements étrangers. Notre examen des dossiers de demandes d'assistance écrites a confirmé que tous les échanges de renseignements ont reçu l'approbation des fonctionnaires mandataires en vertu de la politique de l'ASFC. Nous concluons que cet aspect fondamental du contrôle interne fonctionne bien.

3.32 La documentation comprise dans l'échantillonnage établissait le pouvoir en vertu duquel les demandes avaient été formulées, la nature de l'enquête que l'agence des douanes

étrangère effectuait et la nature exacte des renseignements communiqués. Nous sommes convaincus que les échanges de renseignements étaient autorisés en vertu de l'AAMD applicable, du paragraphe 107(8) de la *Loi sur les douanes*, et que l'information que l'ASFC a communiquée se limitait aux renseignements nécessaires pour satisfaire aux demandes. De plus, l'examen n'a permis de déceler aucun cas où l'Agence aurait communiqué à une tierce partie des renseignements provenant de bases de données externes – telles que le Système de rapports sur les renseignements judiciaires ou le Centre d'information de la police canadienne (CIPC). Nous notons que de tels renseignements ne peuvent être communiqués qu'avec l'autorisation de l'organisme chargé de leur contrôle.

Le cadre de responsabilisation et l'environnement de contrôle entourant les échanges verbaux transfrontaliers de renseignements personnels ont besoin d'être renforcés.

3.33 Notre évaluation a examiné les outils existants – les accords d'échange de renseignements et les politiques de l'ASFC – régissant les échanges transfrontaliers de renseignements personnels. Nos observations concernent le degré de conformité par rapport au cadre de responsabilisation lié aux outils. Il convient de noter que notre vérification n'incluait pas l'évaluation des mérites relatifs aux exigences prévues dans les AAMD entre le Canada et les États-Unis, dont l'exigence d'émettre une demande écrite préalable à tout échange de renseignements, sauf en cas de situations d'urgence.

3.34 De façon générale, voici nos observations :

- Dans bien des cas, l'ASFC a communiqué des renseignements aux États-Unis sans demande écrite de ce pays.
- La communication de renseignements a souvent lieu avant qu'un fonctionnaire désigné de l'ASFC ne l'ait autorisée, ce qui contrevient aux politiques de l'Agence.
- Nous avons découvert des lacunes dans la tenue de dossiers concernant la communication de renseignements.

3.35 En ce qui concerne la communication de renseignements en l'absence d'une demande écrite, nous avons interrogé des gestionnaires et des agents régionaux du renseignement (ARR) choisis au sein de la Division de la contrebande et des services du renseignement que nous avons visitée. Ceux-ci ont déclaré que de nombreux échanges de renseignements avec les États-Unis se faisaient à l'échelle régionale, sans demande écrite, contrairement à l'Accord d'assistance mutuelle en matière douanière (AAMD) entre le Canada et les États-Unis. Des 22 ARR interrogés, 14 d'entre eux (soit quelque 64 p. 100) ont reconnu qu'ils échangeaient verbalement, avec leurs homologues américains, des renseignements douaniers – y compris des renseignements personnels.

Des huit ARR qui ont affirmé ne participer aucunement aux échanges verbaux transfrontaliers, six provenaient de la même région. Ceux-ci ont expliqué que leur rôle et leur zone de concentration ne nécessitaient pas d'échanges verbaux avec les autorités américaines. Au cours des réunions de suivi avec trois gestionnaires de cette région, l'équipe de vérification a été informée que les ARR pouvaient échanger des renseignements avec les États-Unis. Un gestionnaire a affirmé que les échanges quotidiens entre certains ARR et les États-Unis se faisaient verbalement dans une proportion de 80 à 95 p. 100.

3.36 La fréquence des échanges verbaux avec les États-Unis variait chez les 14 agents régionaux du renseignement ayant rapporté participer aux échanges de renseignements

transfrontaliers et dépendait, en grande partie, de leur localisation et de leur rôle. Même si les estimations variaient, à peu près la moitié des répondants ont indiqué que les communications verbales de renseignements représentaient de 70 à 90 p. 100 de leurs échanges avec les autorités douanières américaines et qu'elles pouvaient inclure les éléments suivants :

- des renseignements sur le passage ou les déplacements d'une personne;
- un résumé des mesures d'exécution antérieures;
- la confirmation de l'existence d'un dossier à l'ASFC;
- la confirmation de l'existence d'un dossier chez un autre organisme d'application de la loi.

3.37 En ce qui a trait à l'ampleur des échanges verbaux, on a informé l'équipe de vérification qu'un échange n'avait pas lieu si cet échange risquait de compromettre des activités relatives au renseignement ou à des enquêtes en cours, ou s'il risquait d'identifier une source confidentielle de renseignements ou de dévoiler de l'information qu'un organisme externe (tierce partie) avait fournie à l'ASFC.

3.38 À l'exception d'un cas, les ARR ont rapporté qu'une demande écrite était exigée avant de communiquer des documents aux États-Unis. En utilisant l'exemple d'une mesure d'exécution antérieure, l'équipe de vérification a été informée que des détails généraux entourant une saisie aux douanes pouvaient être communiqués verbalement (à l'exception de la saisie de devises); une demande écrite serait nécessaire si les États-Unis souhaitaient obtenir une copie du rapport de saisie et des documents d'appui.

3.39 Nous avons également interrogé dix inspecteurs des douanes et quatre surintendants des douanes au point de passage frontalier que nous avons visité. Six des dix inspecteurs et deux des quatre surintendants ont indiqué qu'ils avaient (bien que rarement) échangé, avec les agents de la protection des frontières américains, des résultats se rapportant à des demandes de noms et de véhicules. Nous notons que la majorité des échanges transfrontaliers de renseignements concerne des renseignements sur des véhicules qui traversent la frontière. Quant aux activités des aéroports, nous avons interrogé huit inspecteurs des douanes et trois surintendants. Aucun n'a rapporté avoir participé à des échanges d'information avec les États-Unis. On nous a expliqué que les demandes d'assistance provenant des États-Unis étaient transmises à l'ARR sur place.

3.40 En ce qui concerne le processus d'approbation des demandes d'information, en vertu des *Mémorandums D-1-16-1 et D-1-16-2*, l'ASFC a identifié et désigné des fonctionnaires ayant l'autorité d'approuver les communications de renseignements en vertu des dispositions diverses de l'article 107 de la *Loi sur les douanes*. Selon cette politique, un fonctionnaire désigné doit autoriser la communication de renseignements à une tierce partie. Les situations de dangers imminents ou d'urgence où il est impossible d'obtenir une approbation préalable constituent les seules exceptions (par exemple, la communication de renseignements est nécessaire pour protéger la vie, la santé ou la sécurité d'une personne). Toutes ces exceptions doivent être rapportées à un fonctionnaire désigné, dès que possible, après l'événement.

3.41 À l'échelle régionale, le pouvoir de communiquer des renseignements douaniers à des gouvernements étrangers a été délégué au gestionnaire/directeur d'un secteur du programme des douanes. La vérification a permis de constater que cette politique était peu respectée. Dans bien des cas, les renseignements sont échangés verbalement avec les fonctionnaires douaniers américains sans approbation préalable. Bien qu'il y ait eu des exceptions, les ARR qui ont participé aux échanges avec les États-Unis ont généralement reconnu que les échanges

verbaux – les communications de renseignements en réponse à une demande d'assistance des États-Unis et les échanges continus liés à des dossiers d'intérêt commun – se produisent sans l'approbation préalable du gestionnaire ou du directeur. De la même façon, les inspecteurs des douanes qui ont rapporté échanger des renseignements avec leurs homologues américains ont admis que de tels échanges avaient lieu sans l'autorisation préalable d'un gestionnaire.

3.42 Selon nous, un manque de respect de la politique mine le cadre de responsabilisation et le contrôle général de l'Agence, de même que sa capacité à surveiller efficacement ses pratiques en matière d'échange de renseignements avec les entités étrangères afin de garantir que celles-ci sont conformes aux exigences de la *Loi sur les douanes* et de la *Loi sur la protection des renseignements personnels.*

3.43 Tel que mentionné précédemment, nous avons découvert des faiblesses dans la tenue de dossiers concernant la communication de renseignements personnels. Le droit d'une personne à la protection de la vie privée inclut le droit de connaître la nature des renseignements personnels la concernant que les institutions gouvernementales recueillent, les circonstances dans lesquelles ces renseignements peuvent être communiqués à une tierce partie, et avec qui ils seront échangés. En s'acquittant de cette obligation, il s'avère essentiel que les établissements créent et conservent les dossiers présentant toutes les communications à des organismes externes.

3.44 En vertu de la politique de l'ASFC, les fonctionnaires doivent conserver des dossiers contenant tous les renseignements douaniers demandés et ayant fait l'objet d'une communication à des organismes externes. Les dossiers doivent inclure le nom du requérant, la date de réception de la demande, le but dans lequel des renseignements douaniers sont requis, la nature des renseignements communiqués et le motif de la décision rendue. La vérification a révélé des lacunes quant au respect de cette politique. Des 14 ARR qui ont confirmé avoir participé à des échanges verbaux avec les États-Unis, moins de 50 p. 100 ont inscrit à leurs dossiers, pour tous les cas, de telles communications.

3.45 L'équipe de vérification a constaté que lorsqu'une demande de renseignements provenant des États-Unis est enregistrée dans le Système de gestion du renseignement (SGR) de l'ASFC, il existe habituellement une note dans le système concernant les échanges verbaux de renseignements. Cependant, lorsque aucun dossier ne se trouve dans le SGR, les mesures administratives prises relatives à d'autres échanges verbaux de renseignements personnels varient selon les répondants. Certains ont indiqué que les échanges verbaux sont enregistrés dans leur registre ou dans un Rapport sur la fourniture et l'utilisation des renseignements douaniers ou sur l'accès à ces renseignements (formulaire E675 de l'ASFC). D'autres ont répondu que la décision d'enregistrer les échanges varie en fonction du type de renseignements fournis. Les vérifications de noms, les questions concernant le passage de voyageurs et les renseignements généraux de saisie ont été donnés à titre d'exemples du type d'échanges qui ne sont pas enregistrés. Les autres agents régionaux du renseignement ont indiqué que les dossiers relatant des échanges verbaux ne sont pas conservés.

3.46 À propos du point de passage frontalier que l'équipe a visité, cinq des six inspecteurs des douanes qui ont échangé les résultats de vérification de noms ou de passages avec les États-Unis ont rapporté que de tels échanges de renseignements ne sont habituellement pas documentés. En résumé, la vérification a permis de constater que les échanges verbaux de renseignements personnels avec les États-Unis ne font pas l'objet d'un enregistrement de façon constante.

3.47 Le niveau de précision avec lequel les échanges verbaux sont rapportés dans le Système de gestion du renseignement (SGR) et les registres des agents est un domaine qui requiert plus d'attention. L'équipe de vérification a indiqué que le SGR ou les notes compilées dans les registres n'indiquaient pas toujours le nom du fonctionnaire qui requérait l'information, le but dans lequel les renseignements étaient demandés ou la nature exacte de la communication de renseignements, à savoir les renseignements spécifiques qui ont été transmis en réponse à la requête.

3.48 Il convient de noter que nos observations relatives aux enregistrements des échanges verbaux de renseignements reposent sur un échantillonnage limité d'inscriptions dans les registres et le SGR que l'ASFC a fourni pour notre examen. Étant donné la taille de l'échantillon, il est impossible de confirmer s'il existe un problème répandu et systémique. Toutefois, notre travail d'évaluation indique clairement qu'il est nécessaire d'améliorer l'enregistrement des échanges de renseignements. Sans une couverture satisfaisante, l'ASFC ne peut évaluer de manière objective si les activités transfrontalières d'échanges de renseignements respectent le droit à la protection de la vie privée des personnes.

3.49 Nous avons conclu qu'en l'absence d'une tenue adéquate de dossiers, l'ASFC se trouve dans l'impossibilité d'évaluer pleinement la mesure dans laquelle les échanges de renseignements ont lieu et si ces échanges sont appropriés dans tous les cas. De plus, en l'absence de dossiers, les personnes ne peuvent exercer leur droit d'accès à des renseignements personnels en vertu du paragraphe 12(1) de la *Loi sur la protection des renseignements personnels*.

Recommandation 2 :

Il est recommandé que l'ASFC formule un plan d'action pour aborder la question des échanges verbaux de renseignements personnels. Un tel plan devrait prendre en considération les activités suivantes :

- *déterminer l'ampleur des échanges verbaux de renseignements douaniers avec les autorités douanières des États-Unis et mettre en place des mesures afin de garantir que toute communication de renseignements personnels soit conforme, de façon continue, aux politiques et aux accords gouvernementaux;*
- *mettre en place des mesures afin de garantir que toutes les communications de renseignements personnels sont enregistrées, comme l'exige la politique de l'ASFC;*
- *diffuser un communiqué à tout le personnel concernant le processus d'approbation régissant la communication de renseignements personnels en vertu du paragraphe 107(8) de la* Loi sur les douanes *et renforcer les exigences de la politique en incluant un module spécifique pour les ateliers de formation relatifs à la mise en application de la* Loi sur la protection des renseignements personnels *et l'article 107;*
- *surveiller le respect des politiques régissant les échanges transfrontaliers de données afin de garantir la mise en place de contrôles de gestion adéquats pour protéger les renseignements personnels de toute communication non autorisée.*

Réponse de l'ASFC :

L'ASFC accepte ces recommandations et élaborera un plan d'action afin de revoir les

pratiques et les directives existantes concernant l'accès aux renseignements douaniers, l'utilisation et la communication de ceux-ci. L'Agence créera des normes et des outils pour rapporter les activités de communication de renseignements personnels qui prendront en compte à la fois les nécessités opérationnelles et les pratiques recommandées par la commissaire à la protection de la vie privée. L'ASFC appuie les nouvelles directives ainsi que les ateliers ciblés de formation et de sensibilisation; elle surveillera la mise en œuvre de la nouvelle orientation. De plus, nous passerons en revue le matériel de formation destiné au Programme de formation des recrues pour les points d'entrée (FORPE) (ancien nom : Programme de recrutement et de formation des inspecteurs des douanes (PRFID)) afin de nous assurer que le nouveau personnel comprend les exigences liées à la protection des renseignements personnels quant à l'accès aux renseignements douaniers ainsi que l'utilisation et la communication de ceux-ci. Nous nous efforcerons d'améliorer notre capacité de surveiller le respect des directives.

L'ASFC ne peut, avec un degré raisonnable de certitude, faire rapport de la mesure dans laquelle ont lieu les échanges de renseignements personnels avec les États-Unis, le volume ou la fréquence de ces échanges. En outre, l'ASFC ne peut être certaine que toutes ses activités d'échange de renseignements sont autorisées en vertu de l'article 107 de la* Loi sur les douanes *et de l'article 8 de la* Loi sur la protection des renseignements personnels*.

3.50 Pour évaluer à quel point les activités d'échange de renseignements avec les États-Unis sont conformes à la *Loi sur la protection des renseignements personnels,* à la *Loi sur les douanes* et aux accords bilatéraux entre les deux pays, l'ASFC doit avoir la capacité de suivre tous les échanges transfrontaliers de renseignements personnels. À l'heure actuelle, il s'agit d'une capacité nettement sous-développée.

3.51 Un des objectifs de la vérification consistait, dans la mesure du possible, à faire rapport sur la nature des renseignements concernant les Canadiennes et les Canadiens que l'ASFC communique aux États-Unis, les modalités et le but de ces communications. Les enquêtes initiales avaient pour objectif de préciser le matériel de référence que l'ASFC avait en main pour l'aider dans cette tâche, matériel incluant les diagrammes de cheminement des données et les descriptions de programmes. En plus de fournir des dossiers décrivant l'échange automatisé d'avis de surveillance et d'information préalable sur les voyageurs, l'ASFC a soumis un diagramme qui illustrait, de façon générale, le processus d'échange de renseignements, c'est-à-dire l'autorisation légale en matière d'échange de renseignements, le nom de l'accord international, le type de renseignements échangés (par exemple, des renseignements nécessaires pour renforcer les lois douanières) et le mode de transmission (papier ou électronique).

3.52 Même si la tâche d'établir les diagrammes de cheminement des données dans le cadre des initiatives d'information sur les voyageurs à haut risque et de l'Initiative IVRE peut s'effectuer assez facilement, tel n'est pas le cas en ce qui concerne les autres échanges continus entre les autorités douanières canadiennes et américaines, à l'échelle régionale.

3.53 Tel que mentionné précédemment, il s'agit, dans certains cas, de communications verbales non enregistrées. De plus, nous avons constaté que les documents relatifs aux communications verbales de renseignements se trouvent en différents endroits tels que les registres et les dossiers électroniques des agents, et que ces documents ne sont pas clairement identifiés comme documents se rapportant à un échange transfrontalier de

renseignements entre le Canada et les États-Unis. Cet état de fait a empêché l'équipe de vérification d'opter pour un échantillon aléatoire dans le cadre de l'examen des dossiers. Ainsi, tel que mentionné précédemment, nous avons dû recourir aux membres du personnel de l'ASFC pour déterminer - plus ou moins à partir de leur souvenir de cas spécifiques - quels dossiers seraient examinés. Une fois les choix effectués, les notations concernant les échanges verbaux dans certains de ces dossiers n'indiquaient pas clairement quels renseignements avaient fait l'objet d'une communication transfrontalière ni le but de cette communication.

3.54 En l'absence d'un mécanisme organisationnel d'enregistrement de tous les détails des échanges transfrontaliers de renseignements personnels qu'effectue l'ASFC, celle-ci a une capacité limitée d'évaluation de son niveau de conformité au cadre législatif et politique régissant les échanges de renseignements avec les gouvernements étrangers ou leurs institutions. De plus, les dirigeants de l'ASFC ne peuvent obtenir un compte rendu détaillé de la nature des renseignements personnels échangés et de l'ampleur des échanges. Enfin, la direction ne peut fournir ces renseignements à d'autres – par exemple, au Parlement, au commissaire à la protection de la vie privée et à la population canadienne.

Recommandation 3 :

Il est recommandé que l'ASFC mette en place des moyens de consigner tous les échanges transfrontaliers de données aux fins des programmes de gestion et de reddition de comptes. Il pourrait s'agir – sans s'y limiter – de l'élaboration de diagrammes indiquant la circulation des données, et de modifications apportées aux systèmes d'information existants afin d'identifier et d'enregistrer de manière fiable toutes les activités d'échanges avec les gouvernements étrangers.

Réponse de l'ASFC :

L'ASFC accepte la recommandation et reconnaît que les pratiques privilégiées en matière de communication de renseignements doivent être davantage documentées. Ce travail peut faire partie du plan de renforcement du cadre de gestion de la protection des renseignements personnels. Nous envisagerons des directives afin de renforcer les procédures conçues pour consigner la documentation relative aux communications de renseignements personnels et garantir une responsabilité de gestion appropriée afin d'assurer la conformité aux directives sur l'accès aux renseignements douaniers et sur l'utilisation et la communication de ces mêmes renseignements. Nous déploierons les efforts nécessaires afin de garantir que l'ensemble des directions et des régions sont au fait des directives révisées et des processus adoptés. Nous voulons que les directives répondent aux modalités du cadre légal de même qu'aux principes généralement reconnus en matière de renseignements personnels.

De plus, de tels échanges transfrontaliers de données seront identifiés et décrits dans la documentation narrative et schématique, et des vérifications rétrospectives de système seront intégrées aux systèmes de TI pour identifier et enregistrer les activités d'échanges de renseignements avec les gouvernements étrangers.

La stratégie de vérification rétrospective de l'ASFC est actuellement en cours d'élaboration et le cadre de travail sera terminé d'ici décembre 2006 de manière à garantir que les activités requises de vérification rétrospective et d'enregistrement des communications de renseignements personnels feront partie de notre cycle de développement de systèmes liés aux projets et aux systèmes.

SYSTÈME INTÉGRÉ D'EXÉCUTION DES DOUANES (SIED)

Contexte :

3.55 Les ministères et organismes gouvernementaux dépendent largement des bases de données, des programmes et des réseaux d'information pour réaliser leurs mandats respectifs. Comme les renseignements personnels qui sont sous le contrôle de l'ASFC se trouvent principalement dans des bases de données, notre vérification comprenait un examen et une évaluation des contrôles des principaux systèmes TI de l'Agence. Ces contrôles sont essentiels à la protection adéquate des renseignements personnels. Tout système comportant des lacunes entraînerait des risques non seulement sur le plan de la sécurité, mais aussi des risques à la protection de la vie privée.

3.56 Le Système intégré d'exécution des douanes (SIED) est un système automatisé d'appui à l'exécution des lois et règlements en matière de douanes. Selon un protocole d'entente, l'ASFC obtient l'infrastructure de ses services informatiques de l'Agence du revenu du Canada (ARC). Cette entente prolonge les modalités d'une entente de service qui existait à l'époque où les programmes des douanes et du revenu faisaient tous partie de l'ancienne Agence des douanes et du revenu du Canada (ADRC). L'ASFC est responsable pour tous les contrôles internes de sécurité du système SIED.

3.57 La base de données SIED est conçu pour appuyer les fonctions des inspecteurs de première ligne des douanes et du personnel des opérations du renseignement et des enquêtes en leur permettant de recueillir, d'analyser et de communiquer de l'information concernant les risques à la frontière. Le système sert également de lieu d'archivage commun pour les données sur l'exécution des mesures douanières, par exemple, les données sur les arrestations, les saisies et les enquêtes sur les douanes en cours.

3.58 Les inspecteurs des douanes et les agents du renseignement peuvent créer, consulter, mettre à jour ou supprimer des avis de signalement (voir l'encadré ci-dessous) dans les bureaux locaux, régionaux et nationaux. Le Système automatisé de surveillance à la ligne d'inspection primaire (SASLIP) aux bureaux d'entrées frontaliers (lecteur de plaque d'immatriculation) et la Ligne d'inspection primaire intégrée (LIPI) dans les aéroports (lecteur de documents de voyage) procurent aux inspecteurs des douanes de l'information issue du couplage de données effectué à partir du SIED, soit des avis de signalement, des mises en garde et de l'information sur l'exécution des mesures douanières. Les rapports opérationnels du système fournissent des détails sur les transactions liées aux avis de signalement, aux saisies et antécédents de passage des voyageurs et des véhicules de transport aux frontières et aux aéroports.

Un « avis de signalement » est un dossier électronique créé dans le SIED. Il permet de mettre un indicateur dans le système ou d'identifier des voyageurs ou des véhicules en fonction de différents indicateurs de risque ou d'autres renseignements disponibles.

Renseignements personnels :

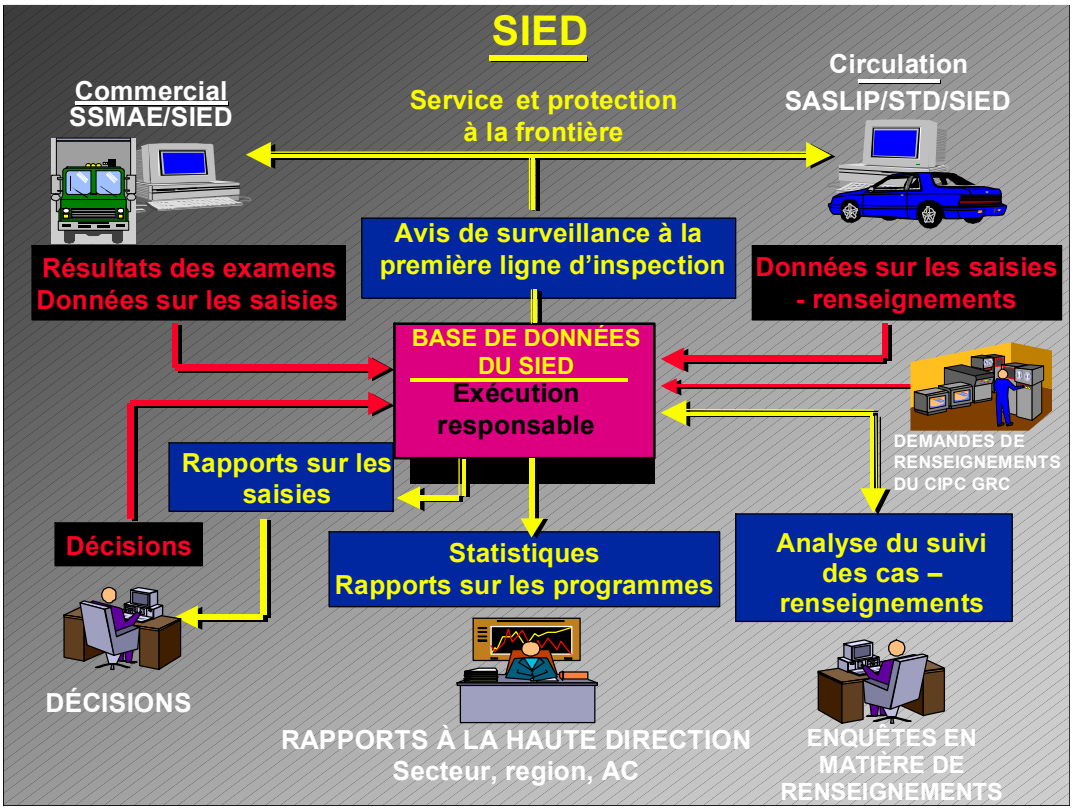
3.59 Tous les renseignements portant sur une mesure d'exécution prise à l'égard d'une personne ou d'une entreprise sont entrés dans la base de données SIED. Les renseignements personnels conservés dans le SIED comprennent entre autres :

- la ou les raisons pour lesquelles la personne doit faire l'objet d'un deuxième examen;
- les résultats de la recherche et les notes sur les entrevues menées pendant le deuxième examen;
- les renseignements de base – nom, âge, adresse, citoyenneté, numéro d'immatriculation et numéro de passeport;
- les mesures d'exécution prises (fouille, arrestation, détention, etc., de la personne) et les résultats de l'enquête;
- l'identité des compagnons de voyage.

3.60 Le système sert également à consigner d'autres détails relatifs aux moyens de transport, aux marchandises, aux méthodes de dissimulation et aux indicateurs. Les inspecteurs des douanes peuvent obtenir automatiquement de l'information sur une personne en consultant un système automatisé de renseignements sur les contrevenants dans lequel sont entrées toutes les saisies effectuées et tous les mises en garde concernant les droits de douane associés à une personne.

Circulation des renseignements personnels

Source – Description du SIED par l'ASFC le 21 janvier 2005.



Remarques :

À l'exception de la banque de données du Centre d'information de la police canadienne (CIPC), tous les programmes indiqués ci-dessus sont sous le contrôle de l'ASFC.

Dans le schéma, « circulation » fait principalement référence aux voyageurs de vols non commerciaux. Notre vérification s'est essentiellement concentrée sur eux.

Bien que le schéma ci-dessus n'y fasse pas référence, l'icône « circulation » inclut également le LIPI, le système utilisé pour le traitement des informations relatives aux passagers des transporteurs aériens entrant au Canada.

Les cas d'arbitrage renvoient à des appels faisant suite à des décisions administratives prises conformément à la *Loi sur les douanes*, un secteur que nous n'avons pas examiné dans le cadre de cette vérification.

Communication de renseignements à des gouvernements étrangers :

3.61 Tel que décrit dans le présent rapport, les renseignements personnels recueillis par l'ASFC peuvent être communiqués à des gouvernements ou des organismes étrangers conformément aux TEJ, des accords d'assistance mutuelle en matière douanière (AAMD), des protocoles d'entente (PE) ou d'autres accords ou arrangements. Le paragraphe 107(8) de la *Loi sur les douanes* prévoit les pouvoirs requis pour autoriser de telles communications.

3.62 Le 9 mars 2005, l'ASFC et la *U.S. Customs and Border Protection Agency* ont signé un PA en vue de faciliter les échanges automatisés d'information sur les avis de signalement et l'échange d'information préalable sur les voyageurs (IPV). Le Centre national d'évaluation des risques (CNER) – qui a fait l'objet d'un examen dans le cadre de notre vérification – et le *U.S. National Targeting Centre* (*NTC*) ont géré conjointement cette initiative.

3.63 Lorsque les agents et les analystes du renseignement et les autres employés autorisés de l'ASFC établissent un avis de signalement, ils ont la possibilité d'échanger l'information relative à cet avis avec les États-Unis. S'ils choisissent cette option, l'avis est électroniquement transmis au CNER pour examen. Lorsque le CNER confirme que l'avis satisfait aux critères d'échange de renseignements, cet avis est envoyé électroniquement du SIED au *U.S. Treasury Enforcement Communications System* (*TECS*). Une fois la transmission terminée, les autorités douanières des États-Unis aux points d'entrée ont accès à l'avis.

3.64 Dans le cadre de notre examen, nous avons évalué les contrôles visant à garantir l'intégrité des renseignements personnels que l'ASFC gère aux fins du programme d'échange des avis de signalement du SIED. L'examen de la TI servant aux contrôles de la base de données SIED est directement lié aux obligations de l'ASFC prévues aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*. La vérification a porté principalement sur les mesures de sécurité et de protection des renseignements personnels mises en place pour assurer l'intégrité des données, sur les avis de signalement qui sont utilisés ou communiqués via l'infrastructure de TI de l'ASFC, ou qui font l'objet d'échanges entre l'ASFC et les États-Unis. Nous avons aussi examiné la sécurité logique et physique des renseignements personnels, la gestion des changements à la TI, ainsi que les contrôles électroniques des opérations. L'équipe de vérification a examiné les activités du SIED ci-dessous :

- l'échange transfrontalier de renseignements sur les avis de signalement; et
- les contrôles spécifiques de TI pour le SIED.

3.65 Notre vérification de la TI de la base de données SIED a été effectuée parallèlement à la vérification des initiatives du Centre national d'évaluation des risques en matière d'échange d'information sur les avis de signalement et sur les voyageurs à risque élevé. Il est à noter que nous n'avons pas évalué les contrôles électroniques utilisé par le U.S. NTC pour protéger l'information une fois que l'ASFC l'a transmise aux États-Unis.

L'architecture de sécurité du Système intégré d'exécution des douanes (SIED) est bien conçue.

3.66 L'architecture du système comprend l'ordinateur central et les serveurs, ainsi que les lignes de communication, les pare-feu et les zones de sécurité dont le but principal est de protéger le système et son contenu des attaques externes. Une architecture de TI bien définie et bien construite sert de fondation aux autres contrôles électroniques effectués en vue d'assurer la sécurité et la protection des renseignements personnels.

3.67 Nous avons constaté que l'architecture de sécurité sur laquelle reposent les applications et systèmes du SIED est bien conçue. Elle offre plusieurs types de protection à chaque niveau important de TI ainsi qu'un contrôle central sur l'accès entre les zones contrôlées.

3.68 Le protocole d'entente (PE) entre le Canada et les États-Unis sur l' échange automatisé d'information sur les avis de signalement et l'échange d'information préalable sur les voyageurs oblige l'ASFC et la *U.S. Customs Border Protection Agency* à respecter les dates d'expiration, les annulations et les modifications de leurs avis de signalement respectifs. Toutefois, le PE renferme peu de détails sur les contrôles électroniques spécifiques qui servent à protéger les renseignements personnels conservés dans le *U.S. Treasury Enforcement Communications System* (*TECS*). Comme il est indiqué ci-dessus, notre vérification n'a pas porté sur les contrôles de la protection de ces renseignements une fois que ceux-ci ont été transmis aux États-Unis. Cependant, nous avons identifié des moyens d'améliorer le cadre de contrôle bilatéral.

Recommandation 4 :

Il est recommandé que l'ASFC collabore avec ses homologues des États-Unis en vue d'offrir l'assurance mutuelle que leurs contrôles de sécurité électroniques respectifs permettent de garantir la protection des renseignements personnels des citoyens relatifs aux avis de signalement échangés. À cet égard, il faudrait entre autres envisager d'étendre la portée des ententes sur les niveaux de service pour y inclure des descriptions des processus de suppression des données au moment de l'expiration de la période de conservation ou lorsqu'elles sont annulées, ainsi que l'obligation d'effectuer des vérifications périodiques de la sécurité et de la protection des renseignements personnels.

Réponse de l'ASFC :

L'obligation pour nos homologues des États-Unis d'assurer la protection des données sur les citoyens dans le cadre des échanges d'information sur les avis de signalement fait partie intégrante du PE conclu entre l'ASFC et la United States Customs and Border Protection (USCBP) concernant les échanges automatisés d'information sur les avis de

signalement et l'échange d'information préalable sur les voyageurs (IPV). Les États-Unis ont également mis en place un processus de suppression des avis de signalement expirés ou annulés.

Un examen des Ententes sur les normes de service (ENS) actuellement en cours sera effectué, et des améliorations seront apportées au cadre de contrôle bilatéral.

Les autorités douanières des États-Unis n'ont pas directement accès au SIED.

3.69 Notre vérification a confirmé que l'application SIED ne permet pas aux autorités des États-Unis d'accéder directement aux renseignements personnels. Les communications électroniques entre le Canada et les Etats-Unis s'effectuent en « poussant » plutôt qu'en « tirant », l'ASFC fournissant aux États-Unis l'information sélectionnée sur *avis de signalement* une fois qu'elle s'est assurée que cette information peut être communiquée.

3.70 Les échanges entre les systèmes SIED et le *TECS* sont chiffrés à l'aide d'algorithmes approuvés faisant appel à des dispositifs de chiffrement périphériques afin de protéger l'intégrité des données en transit. Ces dispositifs font l'objet de contrôles de défaillance.

L'impression des avis de signalement n'est pas consignée électroniquement.

3.71 Les registres des utilisateurs consistent en rapports informatisés sur les opérations que les utilisateurs effectuent dans un système donné. Ces rapports sont conservés dans le système et peuvent être imprimés à des fins de vérification. Ils renferment le nom d'usager et le code d'identification de l'ordinateur ainsi que les numéros des dossiers consultés, modifiés ou supprimés, avec la date et l'heure de l'opération. Les registres constituent d'importants outils de vérification parce qu'ils permettent de faire des suivis périodiques ou ponctuels des activités des différents utilisateurs. La consignation des activités est essentielle pour déterminer si les droits d'accès ont été adéquatement exercés, selon le principe de la nécessité d'accès. Les registres des utilisateurs – et leur utilisation comme outil de contrôle et de vérification sont nécessaires afin de garantir l'intégrité des données des programmes et de confirmer que l'utilisation et la communication des renseignements se font conformément aux principes régissant la protection de la vie privée et aux politiques organisationnelles. Toutefois, il serait essentiel d'informer les utilisateurs (employés), au moyen d'avis et de politiques, de l'existence de ces procédures de contrôle. L'accès aux registres doit être strictement contrôlé afin d'empêcher toute utilisation ou communication inappropriée.

3.72 Bien que le SIED consigne toutes les opérations effectuées avec le système, il n'enregistre pas l'impression des avis de surveillance qui peuvent renfermer des renseignements personnels. Il y a donc un risque de communication de renseignements personnels, accidentelle ou intentionnelle, qui ne laisse pas de piste de vérification ou d'historique qui permettrait d'identifier l'utilisateur responsable de la communication.

Recommandation 5 :

Il est recommandé que l'ASFC modifie son application SIED de manière à ce qu'elle permette de consigner les renseignements chaque fois qu'un imprimé est fait à partir du système.

Réponse de l'ASFC :

Actuellement, le message ci-dessous apparaît avant l'impression d'un avis de signalement dans le SIED :

Document protégé

Vous êtes sur le point d'imprimer un document protégé qui renferme des renseignements douaniers de nature délicate. Vous êtes responsable de l'utilisation et de la communication adéquates de ces renseignements. Vous ne devez en aucun cas les communiquer à des personnes non autorisées à les obtenir en vertu de l'article 107 de la *Loi sur les douanes* ou conformément à la directive D-1-16-2, « Lignes directrices administratives provisoires visant la fourniture de renseignements douaniers à quiconque, l'autorisation d'accès à ces renseignements à quiconque et l'utilisation de ces renseignements ».

Selon le paragraphe 107(2) de la *Loi sur les douanes*, il est interdit à quiconque de sciemment fournir à quiconque un renseignement douanier, de permettre qu'un tel renseignement soit fourni, de permettre à quiconque d'avoir accès à un renseignement douanier ou encore d'utiliser un renseignement douanier, à moins d'y être autorisé par l'article 107 de la Loi. Toute personne qui contrevient à ce paragraphe commet un acte criminel en vertu du paragraphe 160(1) de la *Loi sur les douanes* et est passible d'une amende maximale de cinq cent mille dollars ou d'un emprisonnement maximal de cinq ans, ou de ces deux peines. Toute infraction à l'article 107 ou aux Lignes directrices provisoires peut également entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement.

En imprimant le présent avis de signalement, vous acceptez les exigences et les obligations ci-dessus. Voulez-vous toujours imprimer le document?

Oui **Non**

En plus de l'avis d'impression, tous les systèmes de l'ASFC présentent, dès qu'on y accède, un avis général selon lequel les systèmes ne sont accessibles que pour des usages autorisés et des activités professionnelles officielles.

L'information requise sera ajoutée à la piste de vérification du SIED conformément à la stratégie de l'ASFC en matière de pistes de vérification et sera incluse dans le SIED d'ici décembre 2006.

Le cadre de gestion du changement dans la TI de l'ASFC est bien défini.

3.73 La gestion du changement dans le contexte de la TI est une démarche méthodique pour l'introduction et le contrôle de changements apportés à un système informatique donné, ainsi que pour l'adaptation à ces changements, de manière à ce que l'organisme puisse satisfaire à toutes les nouvelles exigences opérationnelles de ce système. La gestion du changement repose sur l'élaboration de procédures, de contrôles, de technologies et de logiciels qui vont permettre de modifier le matériel informatique et les logiciels. Une gestion efficace du changement est essentielle à la préservation des fonds de données d'un organisme, à l'amélioration de ses programmes et à la protection de l'intégrité des renseignements personnels qu'il utilise dans son processus décisionnel.

3.74 La vérification a révélé que l'ASFC – comme l'ARC – possède un cadre de gestion du changement bien défini et contrôlé, ainsi que l'est son processus de conception, d'élaboration et de mise à l'essai des nouvelles exigences de la TI. Ce processus est conforme à un processus normalisé approuvé pour l'intégration de changements technologiques, lesquels incluent notamment, les :

- modifications et les mises à niveau de la fonctionnalité de l'application;
- changements et les mises à niveau des bases de données;
- changements aux volumes de transactions; et
- retouches aux systèmes opérationnels.

3.75 Le processus de mise à l'essai de la gestion du changement permet de tester, dans un environnement conçu à cette fin, un plan de migration en vue de changements prévus, sans risque de conséquences négatives sur le programme ou le système opérationnel en cours ou sur l'intégrité des éléments d'information que celui-ci renferme.

3.76 L'approche de gestion du changement adoptée par l'équipe de l'ASFC repose sur une gamme plus vaste de capacités et des mécanismes régulateurs plus efficaces permettant de mieux garantir l'intégrité des changements et du code de programme, que si une seule personne était responsable de changements d'une telle importance. Cette approche permet également de réduire les risques de changements technologiques accidentels ou intentionnels ou l'insertion de « portes dissimulées » dans le code de programmation qui pourraient avoir une incidence sur la confidentialité et l'intégrité des données traitées et entreposées par les applications du SIED. Comme précaution supplémentaire, l'ASFC n'autorise pas les concepteurs de programmes informatiques à accéder à l'environnement de production final.

3.77 L'ARC exige que tous les changements aux environnements du SIED passent par un comité de 22 personnes qui se réunit chaque semaine. Chaque changement requiert cinq signatures avant de pouvoir être mis en œuvre. Lorsque des changements doivent être apportés aux données du SIED, un processus d'autorisation doit être suivi, et les changements doivent être consignés.

3.78 Nos enquêtes nous ont permis de déceler des problèmes mineurs que l'ASFC se doit d'examiner. Plus particulièrement, trois administrateurs de bases de données à l'ASFC ont le privilège d'apporter des changements aux bases de données du SIED. Des nouveaux préposés aux bases de données doivent être formés et doivent démontrer qu'ils sont en mesure d'effectuer des changements avant d'obtenir l'accès aux bases de données du SIED. Nous

avons rencontré un seul cas où, pendant un changement effectué dans une base de données, les procédures de suppression n'avaient pas été suivies parce qu'il était techniquement impossible de le faire.

3.79 Nous avons également constaté que l'ASFC n'a pas de documents de procédures pour le retrait d'un serveur de la production ou de la préproduction, ni pour l'exercice des contrôles appropriés de la confidentialité et de l'intégrité des données d'un serveur. Cette fois encore, cette situation ne s'est présentée qu'une seule fois, et les mesures appropriées ont été prises pour protéger les éléments d'information.

Les rôles et les responsabilités en matière de la TI doivent être clairement définis.

3.80 Il est important que les différents rôles et responsabilités en matière de la TI soient clairement définis et communiqués à tous les intéressés. À ce propos, la précision est essentielle à la gestion efficace des nombreux contrôles de la sécurité des TI qui doivent être effectués pour protéger les renseignements personnels et douaniers dans l'ensemble des organismes (ASFC et ARC), des programmes et des secteurs géographiques. Cette responsabilité comprendrait la définition des rôles de leadership (c'est-à-dire celui de l'agent de la sécurité du ministère et celui de l'expert en sécurité informatique) ainsi que la définition du rôle des gestionnaires, spécialistes et utilisateurs fonctionnels de la TI.

3.81 Au moment de la vérification, l'ASFC ne disposait pas d'organigrammes ni de listes de personnes-ressources à jour pour documenter les rôles et les responsabilités rattachés à son nouveau cadre de sécurité de la TI. Cette lacune est sous-jacente à plusieurs catégories de contrôle de la TI, et est due à la création plutôt récente de l'ASFC comme organisme indépendant.

3.82 Notre vérification a montré qu'à l'ASFC, les rôles liés à la sécurité sont très décentralisés afin de répondre aux besoins particuliers de chaque programme et application. Le risque peut d'entraîner un manque d'uniformité dans la façon dont chaque secteur de programmes se conforme aux normes, aux politiques et aux besoins en formation. Tout écart important à l'égard des normes fondamentales pourrait générer un maillon faible dans la chaîne de la sécurité de l'Agence. Toute faiblesse dans cette structure pourrait entraîner des atteintes à la sécurité, ce qui pourrait compromettre les renseignements personnels.

3.83 Nous avons constaté que l'ASFC et l'ARC ont signé des protocoles d'entente et des ententes sur les niveaux de service qui définissent les rôles et les attentes en matière de niveaux de service – y compris les attentes sur le plan de la sécurité – entre les organismes.

Recommandation 6 :

Il est recommandé que l'ASFC définisse et fasse connaître les rôles et les responsabilités de tous les responsables officiels de la TI au sein de l'organisme en faisant entre autres une mise à jour des descriptions d'emploi et des organigrammes.

Réponse de l'ASFC :

L'ASFC effectue actuellement un examen des rôles et responsabilités en matière de TI afin de les définir plus clairement. Elle a déjà fait d'importants progrès à cet égard quant à la sécurité de la TI et à l'agent de sécurité des ministères (ASM). Elle a aussi entrepris l'harmonisation de ces responsabilités avec la norme opérationnelle du SCT pour la GSTI, y compris la gouvernance et la structure des organismes. Les rôles et les responsabilités clarifiés seront mis en œuvre et annoncés d'ici décembre 2006.

L'ASFC élabore actuellement un cadre de gestion de la sécurité.

3.84 En 2004, l'ASFC a défini le rôle et la structure des fonctions de l'agent de sécurité du ministère (ASM). Récemment, l'ASM a été chargé d'élaborer et de mettre en place un cadre cohésif de gestion de la sécurité qui permettra de coordonner tous les aspects de la sécurité dans l'ensemble de l'Agence.

3.85 Ce cadre devrait comprendre les outils, les méthodes et les structures nécessaires pour la mise en œuvre d'un réseau de sécurité allant d'un secteur de programmes à un autre et couvrant tous les aspects de la sécurité à l'ASFC, y compris la sécurité et la protection des renseignements personnels. Le cadre devrait également constituer pour l'Agence une base solide qui lui garantira qu'aucun secteur du contrôle de la sécurité ne devienne le maillon faible de la structure globale de la sécurité de l'organisme. À notre avis, un des éléments clés de ce cadre serait une évaluation de son efficacité sur le plan de la protection des renseignements personnels.

Recommandation 7 :

Il est recommandé que l'ASFC poursuive ses efforts en vue de créer un cadre cohésif de gestion de la sécurité. L'Agence devrait effectuer une vérification de ce cadre un an après sa mise en œuvre afin de s'assurer que celui-ci protège efficacement les renseignements douaniers et personnels. Nous demandons aussi à l'ASFC de fournir les résultats de cette vérification au Commissariat à la protection de la vie privée.

Réponse de l'ASFC :

L'ASFC prévoit mettre en œuvre un cadre complet de gestion de la sécurité d'ici la fin de l'exercice financier 2007. Nous étudierons à ce moment la possibilité d'effectuer une vérification ou un examen de la mise en œuvre. Tout élément concernant la protection de la vie privée découlant d'une vérification ou d'un examen du cadre de gestion de la sécurité sera communiqué au Commissariat à la protection de la vie privée du Canada.

Les droits d'accès au SIED sont accordés conformément au principe de la « nécessité d'accès ».

3.86 Le contrôle des droits d'accès à un système informatique et à ses différents éléments de données constitue une mesure de sécurité essentielle parce qu'il limite l'utilisation et la communication de renseignements personnels aux personnes qui ont besoin d'accéder à ces données. La limitation de l'accès à un petit nombre d'utilisateurs s'avère un moyen efficace de réduire les risques d'utilisation et de communication non autorisées de renseignements personnels.

3.87 La création de nouveaux profils d'utilisateur du SIED fait l'objet d'un contrôle strict grâce à des processus amorcés dans les unités opérationnelles et au service de dépannage. Seules les personnes ayant besoin de consulter des données obtiennent l'accès au SIED. De plus, leur accès se limite au niveau nécessaire à l'exécution des fonctions rattachées à leur poste.

3.88 Un profil d'utilisateur est créé sur production d'une demande de compte d'usager signée par l'employé et autorisée par son gestionnaire. En signant le formulaire de demande, l'employé accepte la responsabilité d'assurer la confidentialité des données. De plus, un changement récemment introduit exige que les utilisateurs confirment qu'ils ne divulgueront pas leur nom d'usager ou leur mot de passe. Le niveau d'accès dont l'employé a besoin lui est attribué et confirmé par son gestionnaire avant que la demande soit envoyée au service de dépannage, qui crée le profil d'utilisateur et active le droit d'accès de l'employé.

3.89 On nous a avisés que les nouveaux utilisateurs du SIED reçoivent de leur gestionnaire de programme une formation sur la sensibilisation à la sécurité. Dans le cadre de cette formation, on insiste sur la nécessité d'assurer la confidentialité des renseignements obtenus de la banque de données SIED. La formation porte aussi sur les procédures de gestion des comptes et des mots de passe afin d'empêcher les utilisateurs non autorisés d'accéder au système.

3.90 Pour faciliter la gestion générale des profils d'utilisateur et des comptes, l'ARC a récemment lancé un projet d'examen continue sur la nécessité, pour l'ARC et l'ASFC, de maintenir les comptes du système de « gestion du risque lié aux utilisateurs privilégié » (GRUP). Il a pour but d'améliorer à la fois l'intégrité de l'attribution des comptes d'utilisateurs et les avantages et la gestion des mots de passe correspondant aux rôles des utilisateurs. L'application de politiques de gestion des mots de passe efficaces garantit que les mots de passe sont souvent changés, qu'ils ne sont pas réutilisés et qu'ils sont formés de manière à ne pas être dévoilés. De récentes mises à niveau du système exclusif « Active Directory », utilisé par l'ARC et l'ASFC, faciliteront la gestion des comptes d'utilisateur à l'échelle de l'organisme.

3.91 Bien que l'accès à la base de données du SIED soit généralement bien contrôlé, le processus de demande d'accès à l'information relatives aux pistes de vérification était jusqu'à récemment mis à jour par les mêmes personnes qui effectuent l'examen des pistes de vérification. L'ASFC a pris des mesures correctrices pour rétablir la situation et a délégué des responsabilités à des personnes distinctes pour le maintien et la surveillance des pistes de vérification. Nous avons également remarqué au moment de notre vérification que les comptes des gestionnaires des bases de données du SIED ne faisaient pas l'objet de surveillance ou de vérification.

Recommandation 8 :

Il est recommandé que l'ASFC consigne et surveille l'accès des administrateurs de la base de données du SIED et les opérations qu'ils y effectuent sur le système.

Réponse de l'ASFC :

L'ASFC a procédé à l'examen des procédures et processus visant à consigner et surveiller l'accès des administrateurs aux bases de données du SIED. L'Agence a également mis en œuvre des mesures de contrôle additionnelles. La stratégie en matière de pistes de vérification appliquée par l'ASFC améliorera davantage ses capacités de vérification du SIED d'ici décembre 2006.

SYSTÈME D'INFORMATION SUR LES PASSAGERS (SIPAX)

Contexte :

3.92 Le Système d'information sur les passagers (SIPAX) est une banque de données, une application et un système informatique que l'ASFC utilise à l'appui de sa stratégie de gestion des risques pour le filtrage des millions de passagers du transport aérien qui entrent au Canada chaque année. Le système a été élaboré et mis en œuvre en 2002-2003 afin de gérer l'information préalable sur les voyageurs/dossiers du passager (IPV/DP) – voir l'encadré intitulé « Renseignements personnels » ci-dessous – qu'elle reçoit des compagnies aériennes, des agents de voyage et des billetteries automatisées. L'ASFC a annoncé qu'elle prévoit étendre l'utilisation de l'application SIPAX à d'autres modes de transport.

3.93 L'autorisation légale de recueillir de l'information IPV/DP est prévue dans la *Loi sur les douanes* et la *Loi sur l'immigration et la protection des réfugiés* et ses règlements. Le *Règlement sur les renseignements relatifs aux passagers (douanes)* de l'ADRC prévoit que les transporteurs commerciaux et les affréteurs, les agents de voyage et les propriétaires et exploitants d'un système de réservation sont tenus de fournir au ministre du Revenu national (maintenant l'ASFC) des renseignements personnels spécifiques sur tous les passagers et membres d'équipage à bord d'un vol commercial à destination du Canada au moment du départ du moyen de transport, ou de donner au ministre l'accès à ces renseignements.

3.94 L'ASFC utilise la base de données SIPAX pour entreposer des données IPV/DP sur les passagers et les membres d'équipage des vols internationaux à destination du Canada avant que ces personnes arrivent au pays. Le système facilite la comparaison de l'IPV envoyée par les systèmes du transporteur aérien au moment du départ avec l'information conservée dans les banques de données de l'ASFC et de Citoyenneté et Immigration Canada – p. ex., l'information sur les infractions antérieures aux lois et règlements sur les douanes, ou sur les personnes qui font l'objet de mandats de l'Immigration ou de mandats pour infractions criminelles.

3.95 L'application SIPAX facilite le couplage des données IPV et DP se rapportant à un individu ou à l'ensemble des passagers de certains vols, de façon à ce que les équipes de ciblage des passagers de l'ASFC puissent mener des analyses poussées des risques. Les équipes de ciblage des passagers sont réparties dans huit aéroports du Canada. Elles comparent les renseignements des DP aux différentes sources de données sur l'application de la loi et le renseignement afin d'évaluer les risques que présentent certains passagers. Selon cette évaluation, un avis électronique de surveillance peut être créé. Si c'est le cas, le voyageur doit généralement subir un deuxième examen.

3.96 Le système d'acquisition de données (SAD) pour accéder à l'information IPV/DP utilisé par l'ASFC est le logiciel de messagerie iDetect, un outil électronique fourni par un tiers, la Société internationale de transport aéronautique (SITA), qui est sous contrat avec l'ADRC (maintenant l'ASFC). Cet outil se trouve encore sur le réseau informatique de l'Agence du revenu du Canada. La SITA a aussi la responsabilité d'assurer la sécurité de la transmission au SIPAX des données sur les voyageurs provenant des compagnies aériennes et des agents de voyage.

3.97 Le 7 octobre 2002, l'ASFC a commencé à recueillir électroniquement de l'IPV auprès du premier groupe de transporteurs aériens participant à l'initiative. À la fin de janvier 2003, l'Agence recevait des données IVP d'environ 70 p. 100 des transporteurs aériens. L'ASFC nous

a indiqué qu'actuellement tous les transporteurs aériens fournissent des données IPV. Nous avons cependant constaté que l'Agence ne reçoit pas toujours toutes les données IPV pour tous les vols.

3.98 L'Agence a commencé à recueillir des DP auprès des transporteurs aériens le 8 juillet 2003. La quantité et la qualité des données que reçoit l'ASFC demeurent problématiques. Comme réponse à des problèmes de qualité des données décelés lors d'un examen de l'application SIPAX postérieur à sa mise en œuvre, une fonction d'analyse des données a été créée avec le mandat de repérer et d'analyser ces problèmes. L'ASFC poursuit ses travaux avec les différents transporteurs aériens en vue d'élaborer et de mettre en œuvre des solutions.

Renseignements personnels :

3.99 L'information IPV/DP consiste en divers éléments de données, comme le montre l'encadré ci-dessous. Tous les voyageurs et les membres d'équipage qui arrivent au Canada par vol commercial sont visés par cette initiative.

ÉLÉMENTS DE DONNÉES IPV/DP

Information préalable sur les voyageurs (IPV)

L'IPV figure dans la zone de lecture automatique (ZLA) des documents de voyage des passagers et des membres d'équipage (p. ex., passeport ou carte de résidant permanent). Les éléments de données IPV comprennent le nom complet, la date de naissance, le sexe, la citoyenneté ou la nationalité et le numéro du document de voyage du passager. L'IPV qui figure dans la base de données SIPAX n'inclut pas la citoyenneté ni la nationalité, mais elle comprend le pays d'origine du document de voyage.

Dossier passager (DP)

L'information du DP comprend les données personnelles liées à la réservation faite par le voyageur et à son itinéraire qui sont enregistrées dans le système de réservation du transporteur commercial. Voici en quoi consistent ces éléments de données :

Code de localisation du DP	Agence de voyage	Information sur le siège
Date de réservation	Agent de voyage	Billets aller seulement
Dates de voyage prévues	Information DP divisée	IPV recueillie
Nom du passager	Information sur le billet	En attente
Autres noms dans l'IPV	Numéro du billet	Information sur l'enregistrement
Information sur toutes les formes de paiement recueillie	Numéro de siège	
Adresse de facturation	Information sur les passagers sans billet « Go show »	
Numéros de téléphone des personnes-ressources	Date d'émission du billet	
Tous les itinéraires pour le DP particulier	Numéro des étiquettes a bagage (information sur les bagages)	
Information sur les grands voyageurs	Information sur les passagers défaillant « No show »	

Circulation des renseignements personnels :

3.100 Les étapes ci-dessous illustrent la circulation des renseignements personnels concernant les passagers d'un vol international typique à destination du Canada.

- Un voyageur réserve un billet d'avion pour le Canada par l'entremise d'un agent de voyage, d'un représentant ou d'une compagnie aérienne ou encore par le biais d'un système de réservation sur Internet.

- L'agent qui fait la réservation demande les renseignements nécessaires et crée un dossier du passager (DP) à partir de l'information que lui fournit le voyageur.

- L'agent de réservations transmet le DP au Système de contrôle des départs (SCD).

- Lorsque le voyageur se présente au comptoir d'enregistrement, l'agent consigne l'information préalable sur les voyageurs (IPV), laquelle comprend les renseignements sur les bagages et le siège attribué; et délivre une carte d'embarquement.
- Les éléments de données mis à jour sont entrés dans le dossier du voyageur du SCD.
- Après le décollage de l'avion, le SCD de la compagnie aérienne transmet les données contenues dans l'IPV/DP à la base de données du SIPAX à l'ASFC.
- Les données de l'IPV/DP que l'ASFC a reçues sont évaluées en les comparant à l'information des bases de données d'exécution de la loi et des renseignements, et se voient attribuer une cote de risque permettant de déterminer si un voyageur doit se soumettre à un examen supplémentaire.
- Si un voyageur est sélectionné pour un examen supplémentaire, un avis de signalement est transmis au SIED et mis en liaison avec le Système de la ligne d'inspection primaire intégrée (LIPI) que les inspecteurs de première ligne des douanes utilisent dans les aéroports.
- Lorsque le voyageur arrive à la première ligne d'inspection, l'inspecteur des douanes scanne son document de voyage (passeport) à l'aide du lecteur de carte du système LIPI ou entre manuellement de l'information dans le système.
- Le système LIPI recherche alors des correspondances dans les avis de signalement et les mesures d'exécution figurant dans le SIED et le Système de soutien des opérations des bureaux locaux (SSOBL).
- Lorsqu'il y a correspondance d'un avis de signalement ou des mesures d'exécution avec l'information contenue dans les bases de données des douanes ou de l'immigration, le voyageur doit se soumettre à un deuxième examen.
- Lorsqu'un voyageur visé par un avis de signalement est intercepté, les résultats du deuxième examen sont communiqués à l'agent qui a créé l'avis de signalement au moyen d'un message électronique ou d'un rapport d'inspection.

- Il y a lieu de remarquer qu'en plus des personnes auxquelles un avis de signalement est attribué, les agents des douanes peuvent aussi, à leur discrétion, soumettre d'autres passagers à un examen secondaire. Ils choisissent également des voyageurs au hasard.

Communication de renseignements à des gouvernements étrangers :

3.101 Le fondement légal pour l'échange des données IPV/DP est prévu par les engagements pris par le Canada et les *États-Unis aux termes de la Déclaration entre le Canada et les États-Unis sur leur frontière intelligente et le plan d'action en 30 points*, l'article 107 de la *Loi sur les douanes*, la *Loi sur l'immigration et la protection des réfugiés,* ainsi que le *Protocole d'entente sur l'échange automatisé des avis de signalement et l'échange de l'information préalable sur les voyageurs*.

3.102 Ci-après, une liste de contrôles de la TI de la banque de données SIPAX jugés adéquats suite à la vérification:

- la gestion et la sécurité des liaisons de données entre le Canada et les États-Unis;
- l'accès aux bureaux et aux centres de données hébergeant l'information du SIPAX;
- la gestion des données dans le SIPAX;
- les contrôles relatifs à la création des comptes; et
- la documentation technique détaillée sur le SIPAX.

Aucune entente officielle sur les niveaux de service n'existe entre les États-Unis et le Canada quant à la sécurité et à l'exactitude des données.

3.103 Lors des entrevues que nous avons menées auprès des employés et des gestionnaires des services de TI de l'ASFC, nous avons constaté que, bien que le Canada et les États-Unis aient conclu un protocole d'entente (PE) sur l'échange de renseignements, il n'existe entre ces deux pays aucune entente officielle sur les niveaux de service qui précise ce qui suit :

- les normes de sécurité communes;
- le niveau acceptable d'exactitude des données; et
- le responsable de l'exactitude des données échangées entre les deux partenaires.

3.104 Si aucune norme de sécurité n'a été définie, mise en œuvre et examinée, le système n'est peut-être pas en mesure de protéger les renseignements personnels de la population canadienne et des voyageurs venant d'autres pays. Une fois de plus, tel que signalé ci-dessus, sans responsabilités et normes clairement définies en vue de garantir un niveau d'exactitude acceptable pour les renseignements personnels échangés entre les partenaires, il y a un risque que des données inexactes donnent lieu à des mesures administratives qui auraient des conséquences défavorables sur les voyageurs.

Recommandation 9 :

Il est recommandé qu'une entente officielle sur les niveaux de service soit mise en place entre le Canada et les États-Unis, entente qui prévoira des normes de sécurité approuvées par les deux parties (en fonction des normes de sécurité et des normes sur la qualité et le filtrage des données selon la norme de la Gestion de la sécurité des technologies de l'information (GSTI) du gouvernement du Canada), de manière à ce que chacun des pays puisse prendre des mesures qui garantiront que les renseignements personnels échangés sont complets, à jour et exacts.

Réponse de l'ASFC :

L'ASFC examine actuellement les données qu'elle communique aux États-Unis afin de s'assurer qu'elles sont bien celles qu'on recherche avant que le voyageur n'arrive à destination et qu'elles satisfont aux exigences en matière de protection de la vie privée, de communication à des tiers et autres exigences législatives, ainsi qu'aux exigences liées à des programmes.

L'ASFC travaillera en collaboration avec ses homologues des États-Unis en vue d'élaborer des ententes détaillées sur les niveaux de service qui vont prévoir l'application de normes de sécurité adéquates à tous les échanges de renseignements personnels entre les deux pays.

En outre, l'ASFC met actuellement en œuvre un cadre de gestion des risques en réponse à la nécessité d'examiner périodiquement les vulnérabilités éventuelles qui auraient une incidence sur la confidentialité, l'intégrité et la disponibilité de ces renseignements.

Les droits d'accès individuels à la base de données SIPAX n'ont pas été examinés et validés assez souvent pour garantir leur validité à long terme.

3.105 La gestion des droits d'accès aux systèmes de TI exige une bonne coordination et des communications efficaces entre les utilisateurs, leurs gestionnaires et le personnel de la TI et des Ressources humaines.

3.106 Selon une politique de TI de l'ASFC, un examen des droits d'accès des différents utilisateurs doit être fait tous les trimestres. Toutefois, notre vérification a indiqué que l'examen et la validation des listes d'accès à l'application SIPAX n'ont pas été faits régulièrement au cours des deux dernières années. Des documents examinés dans le cadre de notre vérification ont révélé que l'Agence avait effectué un examen en avril 2005, et un autre dix mois plus tôt en juin 2004. Nous avons fait part de ces observations à l'ASFC. Depuis, l'Agence a effectué un examen dont les résultats nous ont été communiqués en septembre 2005.

3.107 Nous avons également constaté que les rôles et les responsabilités concernant le service de dépannage du SIPAX, comme il est indiqué dans la version 3.0 du *Document sur le service de dépannage du SIPAX*, ne comprennent pas de lignes directrices sur la révocation des droits d'accès au système des utilisateurs.

3.108 Nous avons examiné un échantillon de comptes d'utilisateur et nous les avons comparés aux dossiers de ressources humaines de ces personnes. Même si beaucoup de comptes avaient été supprimés dans le cadre du dernier examen trimestriel, certains comptes n'avaient pas encore été supprimés un an après que l'employé avait quitté l'Agence.

3.109 En l'absence d'un processus clairement défini pour l'administration des droits d'accès visant l'ensemble de l'organisme, y compris des examens périodiques des listes d'accès et des procédures de suppression des droits d'accès dès que l'emploi, le poste ou le rôle d'un employé change, il subsiste un risque accru que les droits d'accès de certains utilisateurs du système ne correspondent pas à leurs rôles et responsabilités. Il y a également un risque accru d'accès non autorisé lorsque des comptes ne sont pas désactivés dès qu'ils ne sont plus requis.

3.110 Une liste de contrôle devrait être rigoureusement suivie dans tous les cas, et pourrait être générée par n'importe laquelle des situations suivantes : un examen des droits d'accès; un gestionnaire prend note d'un changement dans le rôle ou dans le statut d'emploi d'un de ses employés; un responsable des ressources humaines prend note d'un changement dans le rôle ou les responsabilités d'un de ses employés suite à un changement dans la classification des emplois; l'équipe de soutien du SIPAX prend note d'un changement dans un rôle ou des responsabilités résultant d'une demande de niveau d'accès plus élevé; la production de rapports trimestriels sur l'accès afin de garantir que les doits d'accès sont correctement attribués en fonction du principe de la nécessité d'accès.

Recommandation 10 :

Il est recommandé qu'une « liste de contrôle normalisée des droits d'accès » au système soit utilisée lorsqu'un changement dans le rôle, les responsabilités ou le statut d'emploi d'un employé exige que son gestionnaire réévalue les droits d'accès dont cet employé a besoin, les autorisations d'accès requises et les autorisations à révoquer.

Recommandation 11 :

Il est recommandé que le document du service de dépannage du SIPAX soit mis à jour de manière à inclure des lignes directrices sur la révocation des droits d'accès au système. Nous recommandons également que les ressources humaines de l'ASFC consultent la liste de contrôle afin de s'assurer que les droits d'accès des employés qui changent de poste, qui sont en congé à long terme ou qui ont quitté l'organisme soient examinés et révisés ou révoqués en conséquence.

Réponse de l'ASFC aux recommandations 10 et 11 :

L'ASFC procédera à l'examen des processus et procédures d'attribution de droits d'accès et d'autorisation actuellement en cours, et élaborera une liste de contrôle à utiliser dès qu'un changement dans le statut d'un employé survient. La mise en oeuvre du Système de gestion du risque lié aux utilisateurs privilégiés (GRUP) permettra également d'améliorer l'intégrité générale du processus d'attribution des comptes d'utilisateurs et des mots de passe.

Les administrateurs du SIPAX n'effectuent pas de contrôle du registre de vérification des activités de consultation, d'extraction ou de modification de l'information se rapportant au serveur ou aux bases de données du SIPAX.

3.111 Dans le cadre des entrevues que nous avons menées auprès des principaux responsables de la TI de l'équipe de gestion des données de l'ASFC et du groupe de l'infrastructure de l'ARC, nous avons constaté que même si l'information sur le registre de vérification est disponible et peut être extraite, l'ASFC ne contrôle pas rigoureusement l'accès au SIPAX par les administrateurs de bases de données et les administrateurs de serveurs.

3.112 L'absence d'un contrôle strict de l'accès au SIPAX par des administrateurs pourrait donner lieu à des utilisations non autorisées des bases de données ou des serveurs. En outre, comme les activités inhabituelles et les tendances qui découlent de cette absence de contrôle strict ne font pas l'objet d'une surveillance, les activités non autorisées risquent de ne pas être décelées, ce qui nuirait à l'intégrité du système. Le risque est encore plus grand si un intrus entre dans le système, manipule des données et efface toute trace de l'intrusion.

Recommandation 12 :

Il est recommandé d'effectuer périodiquement un contrôle rigoureux de l'accès des administrateurs au serveur et à la base de données du SIPAX afin de garantir des contrôles adéquats de leur utilisation du système.

Réponse de l'ASFC :

La stratégie de l'ASFC en matière de pistes de vérification est en cours d'élaboration, et le cadre de vérification sera terminé d'ici décembre 2006 afin que les pistes de vérification requises et les activités liées à l'échange de registres fassent partie de notre cycle de développement de logiciels pour les projets et les systèmes. L'ASFC procédera également à l'examen des procédures et processus actuels qui permettent de surveiller l'accès des administrateurs au serveur et à la base de données du SIPAX, et mettra en œuvre les mesures de contrôle adéquates.

CENTRE NATIONAL D'ÉVALUATION DES RISQUES

Description du programme :

3.113 En janvier 2004, le gouvernement du Canada a créé le Centre national d'évaluation des risques (CNER) au sein de la Direction générale de l'exécution de l'ASFC. Le Centre administre plusieurs initiatives et programmes concernant les voyageurs, incluant les échanges automatisés d'information sur les avis de signalement et l'échange d'information préalable sur les voyageurs à risque élevé, réalisé conjointement avec les États-Unis. La ligne téléphonique de surveillance à la frontière est aussi administrée par le Centre.

3.114 Le CNER et les initiatives ci-dessus ont été mis en place suite aux événements du 11 septembre 2001 et aux recommandations formulées dans le Plan des douanes d'avril 2000, qui recommande de se fier davantage aux renseignements et aux évaluations basées sur les risques pour guider les mesures d'exécution en matière de douanes.

3.115 Comme il est indiqué ci-dessus, le CNER est responsable de la ligne de surveillance à la frontière (ligne 1 800 pour les dénonciations). En composant un numéro de téléphone sans frais, le grand public peut signaler des activités transfrontalières criminelles ou douteuses. Les appels sont acheminés à l'unité opérationnelle régionale de l'ASFC appropriée afin que les mesures nécessaires soient prises. Bien que l'identité de l'auteur de l'appel demeure confidentielle; les renseignements fournis peuvent être transmis à des organismes canadiens et à des administrations douanières à l'étranger, selon le principe de la nécessité d'accès, après que l'ASFC vérifie la fiabilité de l'information reçue.

3.116 Des procédures normales d'exploitation (PNE) gouvernent les activités quotidiennes du CNER. Pour les activités d'échange d'information, toutes les communications, tant à l'intérieur qu'à l'extérieur de l'ASFC, sont assujetties aux restrictions énoncées à l'article 107 de la *Loi sur les douanes*, dans la politique de l'ASFC et dans le Protocole d'entente entre le Canada et les États-Unis sur les échanges automatisés d'information sur les avis de signalement et l'échange d'information préalable sur les voyageurs.

Initiative d'échange automatisé d'information sur les avis de signalement

Contexte :

3.117 Un « avis de signalement » est un dossier électronique créé, dans le Système intégré d'exécution des douanes (SIED) pour des voyageurs ou des véhicules particuliers, en fonction d'indicateurs de risque ou d'autres renseignements disponibles. Le Canada et les États-Unis échangent des avis de signalement depuis déjà plusieurs années. Ce genre d'échange automatisé a commencé le 6 février 2004. Cette initiative ne comprend pas d'échanges d'information sur les avis de signalement d'entreprises (activités commerciales) ni les avis postaux.

3.118 Il y a trois catégories d'avis de signalement. L'ASFC considère qu'il s'agit d'information protégée. Ces catégories sont liées généralement aux menaces à la sécurité nationale ou contre le bien-être économique ou sociale du Canada.

3.119 Le PE entre le Canada et les États-Unis pour l'échange automatisé d'information sur les avis de signalement et l'échange d'information préalable sur les voyageurs a été signé le 9 mars 2005.

Voici un sommaire des modalités du PE :

- les parties doivent accuser réception des avis de signalement;
- les parties doivent s'informer mutuellement de l'acceptation ou du rejet des avis de signalement;
- si un avis de signalement est rejeté, son rejet doit être justifié et communiqué;
- le pays qui reçoit l'avis doit se conformer aux règles du pays expéditeur en ce qui concerne l'expiration, l'annulation et l'archivage des avis de signalement;
- un avis de signalement visant un tiers ne peut pas être communiqué tant que le pays expéditeur n'obtient pas l'autorisation du tiers;
- les parties ne doivent pas échanger les avis de signalement avec des personnes non autorisées, ni donner accès aux avis à des personnes non autorisées;
- les avis de signalement échangés porteront un en-tête à cet effet;
- le pays destinataire ne peut pas arbitrairement annuler ou modifier un avis de signalement ni en modifier la date; et
- les résultats des examens effectués à la suite de la création d'un avis de signalement doivent être communiqués au pays qui a établi l'avis.

3.120 Tel qu'indiqué ci-dessus, les renseignements sur les avis de signalement sont entreposés dans le Système intégré d'exécution des douanes de l'ASFC.

Renseignements personnels :

3.121 Les avis de signalement renferment des données qui permettent d'identifier une personne. En plus du nom de la personne, la date de naissance et le sexe, l'avis peut comprendre une description physique de la personne et d'autres renseignements spécifiques sur l'individu.

3.122 L'avis de signalement comprend également une section réservée à la justification de la création de l'avis ainsi que des renseignements qui peuvent améliorer son efficacité.

3.123 En vertu de l'entente entre le Canada et les États-Unis, plusieurs types d'avis de surveillance peuvent être échangés, dont les avis de signalement concernant des menaces à la sécurité nationale et des activités criminelles transfrontalières.

Circulation transfrontalière des renseignements personnels :

3.124 La circulation des données commence avec l'entrée d'un avis de signalement par l'ASFC (habituellement par un agent régional du renseignement) ou par la *U.S. Customs and Border Protection Agency* (*CBP*). Lorsqu'un avis de signalement créé par l'ASFC est sélectionné aux fins d'échange par l'autorisateur des avis (p. ex., un agent régional du renseignement), on demande à celui-ci s'il veut échanger l'avis avec la *U.S. CBP*. On lui demande aussi si les renseignements figurant dans l'avis de signalement proviennent d'un tiers (p. ex., un service de police) et, le cas échéant, s'il a obtenu l'autorisation du tiers d'échanger l'information.

3.125 Le CNER a la responsabilité d'examiner les avis de signalement échangés par l'ASFC avant la transmission aux É-U. Néanmoins, tel qu'indiqué ci-dessous (3.132), le CNER n'examine pas tous les avis de signalement avant que ceux-ci soient transmis aux États-Unis.

3.126 Les avis de signalement reçus des États-Unis sont révisés par le CNER afin de s'assurer que ceux-ci sont conformes aux critères d'échange et qu'ils renferment suffisamment de renseignements pour que les inspecteurs des douanes puissent prendre les mesures qui s'imposent au moment d'intercepter un voyageur.

3.127 Selon des renseignements obtenus des responsables du CNER, l'Agence a reçu en mars 2003 un transfert massif de 17,500 dossiers (des avis de signalement déjà existants) concernant la sécurité nationale en provenance de la *CBP* des É.U. Ces enregistrements ont été versés dans le Système canadien d'avis de signalement sans aucun filtrage préalable. À la suite d'un exercice de filtrage, 5 000 de ces avis ont été annulés, et les 12,500 autres ont été jugés valides et conservés dans le système.

3.128 Après la mise en œuvre de l'initiative d'échange automatisé d'avis de signalement en février 2004, le *U.S. CBP* a effectué un autre transfert massif à l'intention du système canadien des avis de signalement en vue d'améliorer et de mettre à jour l'information. Effectué en fonction d'exigences précises, ce second transfert visait à remplacer les dossiers d'avis de signalement reçus préalablement. Nous avons été informés que 4 000 avis satisfaisaient à ces exigences. Ils ont été vérifiés en détails et individuellement par le personnel du CNER, entre autres fins pour en assurer la qualité et l'utilité pratique. Cet exercice a finalement permis de retirer une centaine d'avis de signalement du système canadien. Les agents du CNER ont de surcroît recommandé que la date d'échéance des avis de signalement restants (environ 3 900) soit fixée à un an, tout au plus, de la date à laquelle ils avaient été transférés, avec la possibilité de prorogation si jugé nécessaire. À ce jour, moins de dix de ces avis de signalement demeurent actifs, nous a-t-on informés.

3.129 En ce qui concerne les avis dont le transfert n'a pas été accepté, comme il est indiqué ci-dessus, les responsables du CNER ont expliqué que les rejets étaient dus au manque de précisions permettant de garantir la qualité, l'utilité ou la pertinence de ces avis de signalement.

3.130 Les résultats obtenus constituent un moyen de mesurer l'efficacité du programme des avis de signalement. L'ASFC appelle « résultats » les mesures d'exécution prises une fois qu'un indicateur a été apposé à l'avis de signalement d'un voyageur et que ce dernier a été intercepté. Les mesures d'exécution comprennent notamment l'arrestation et la détection ou la saisie de marchandises de contrebande. Il est également possible qu'un avis de signalement soit créé uniquement pour surveiller les habitudes de voyage d'une personne et de ses compagnons de voyage.

Même si les interceptions liées au renseignement ne donnent pas nécessairement lieu à des mesures d'exécution, elles sont toutefois efficaces sur le plan de la collecte de renseignements. En outre, les résultats ne tiennent pas compte du facteur de dissuasion des avis de signalement. Par exemple, à la suite de l'établissement d'un avis de signalement, une personne peut éviter de traverser la frontière ou de se livrer à certaines activités.

Les avis de signalement ne sont pas tous filtrés ou examinés avant que l'ASFC ne les transmettent aux États-Unis.

3.131 La vérification a révélé que certains agents du renseignement, qu'ils soient affectés à une région ou à l'administration centrale, sont autorisés à échanger des avis de signalement sur une base locale avec les autorités des États-Unis en cas d'urgence – p. ex., lorsqu'il y a un risque imminent à la sécurité nationale ou à la santé et à la sécurité publique. De tels avis de signalement sont transmis par téléphone à un agent des douanes des États-Unis. Lors de la vérification, nous avons constaté que les échanges locaux d'avis de signalement ne se font pas toujours en raison d'une situation d'urgence ou d'un risque imminent.

3.132 Un des rôles du CNER est d'examiner les avis de signalement canadiens avant qu'ils ne soient transmis aux É-U, afin de s'assurer qu'ils satisfont aux critères d'échange établis, qu'ils renferment suffisamment de précisions pour être efficaces et qu'ils ne comportent pas de renseignements que la loi interdit de communiquer. Bien qu'il ne semble pas y avoir de problème systémique, certains agents du renseignement régionaux (ARR) ont indiqué qu'ils avaient contacté ou qu'ils contacteraient directement leurs homologues des États-Unis pour créer un avis de signalement plutôt que de le faire électroniquement via le CNER. Puisque les avis de signalement peuvent être échangés en temps réel par un échange automatisé, il est étonnant de constater que les agents contournent le processus d'examen du CNER lorsqu'il n'y a pas de situation d'urgence. En plus d'offrir un mécanisme d'examen de la qualité des données, l'intervention du CNER dans le processus garantit la saisie de tous les avis de surveillance échangés aux fins de contrôle et de vérification.

Recommandation 13 :

Il est recommandé que l'ASFC prenne des mesures afin de s'assurer que tous les avis de signalement échangés avec les États-Unis soient transmis au Centre national d'évaluation des risques pour faire l'objet d'un contrôle de qualité, d'une surveillance continue et d'une vérification.

Réponse de l'ASFC :

L'ASFC effectuera un examen de ses processus d'échange des avis de signalement. À noter toutefois que les échanges effectués via le CNER et le NTC *se limitent aux catégories d'avis de signalement sur des voyageurs à risque élevé. Le plan d'action relatif à la recommandation 2 traitera des échanges qui ne se font pas entre le CNER et le NTC.*

Dans un avis de signalement, les renseignements personnels permettant d'identifier une personne se limitent à son nom, ce qui crée le risque que la mauvaise personne pourrait faire l'objet d'un examen secondaire inutile à la frontière.

3.133 La date de naissance de la personne dont le nom apparaît sur l'avis ne constitue pas un élément d'information obligatoire en vertu de l'initiative d'échange des avis de signalement entre le Canada et les États-Unis. Cela pourrait accroître le nombre de voyageurs assujettis à un deuxième examen uniquement en fonction de leur nom. Ainsi, les avis de signalement portant seulement le nom d'une personne pourraient faire augmenter le nombre de recherches ayant comme résultat « non-correspondance » ou « faux positif » - c'est-à-dire lorsqu'on constate, après un deuxième examen, que la personne interceptée n'est pas celle qui est visée par l'avis de signalement. Aucune étude ou analyse de la méthode utilisée pour confirmer l'identité des personnes aux fins d'échange des avis de signalement n'a encore été faite. Par conséquent, il y a toujours le risque qu'une personne soit réputée présenter un risque élevé ou inconnu selon des données minimales – seulement par son nom.

3.134 Dans le cadre de notre vérification, nous avons sélectionné 125 avis de signalement au hasard pour examen. L'échantillon comportait différents types d'avis – p. ex., monnaie, narcotiques, propagande haineuse, alcool, kidnapping, enfants disparus, contrebande générale et terrorisme. Les avis examinés comprenaient ceux établis par l'ASFC, mais aussi ceux ayant fait l'objet d'un échange, lesquels avaient été créés par l'Agence pour le compte d'autres services Canadiens chargés d'application de la loi. Environ 20 p. 100 des avis de l'échantillon avaient été établis par les États-Unis et transmis au Canada dans le cadre de l'entente d'échange de renseignements.

3.135 Les 125 avis examinés, qui visaient 309 personnes, satisfaisaient tous les critères du programme d'échange automatisé d'information sur les avis de signalement Canada-États-Unis. Toutefois, nous avons relevé un avis établi par le Canada où les renseignements sur l'identification de l'individu se limitaient au nom de la personne. Nous avons également trouvé des avis sur lesquels figuraient une liste de noms de personnes. En résumé, 16 avis identifiaient 27 personnes comme des sujets d'intérêt. De ce nombre, 10 avaient comme unique renseignement le nom des individus. Il n'y avait pas d'autre élément d'information comme l'adresse, le numéro de permis de conduire ou la date de naissance. On a associé ces dix personnes à d'autres objets, véhicules, adresses ou encore à d'autres sources d'information qui les reliaient à ces avis de signalement. Néanmoins, il demeure possible qu'une personne doive se soumettre à un examen secondaire uniquement en fonction de leur nom.

Aucun examen de l'efficacité de l'initiative d'échange des avis de signalement entre le Canada et les États-Unis n'a encore été effectué.

3.136 Les statistiques que l'ASFC a fournies à l'équipe de vérification pourraient suggérer que le taux des résultats des avis de signalement est faible (voir le paragraphe 3.130 ci-dessus) au Canada. Nous ne savons pas exactement si ce pourcentage constitue un taux acceptable ou utile compte tenu de la nature et des attributs des voyageurs à risque élevé. De plus, les statistiques sur les avis de signalement annulés n'établissent pas de distinction entre les avis annulés parce que périmés et les avis annulés parce qu'ils ont obtenu « faux positif » comme résultat.

3.137 Toute méthode utilisée pour identifier des voyageurs à risque élevé reposant sur l'intuition, les indicateurs physiques ou la cote du renseignement ou du risque – ou d'une combinaison de ces éléments d'information – peut faire en sorte que des voyageurs soient assujettis à un deuxième examen qui indiquera que ceux-ci représentent un faible risque ou aucun risque du tout. Nous croyons qu'il est dans l'intérêt autant de l'ASFC que des voyageurs de réduire au minimum les possibilités que de telles situations se présentent.

3.138 Aucun examen approfondi de l'efficacité de l'initiative d'échange des avis de signalement entre le Canada et les États-Unis n'a encore été effectué. Il est donc impossible de déterminer pour le moment si l'initiative donne de meilleurs résultats que les méthodes d'échange des avis de signalement utilisées auparavant.

> *Recommandation 14 :*
>
> *Il est recommandé que l'ASFC évalue le système d'échange des avis de signalement en vue de déterminer son efficacité à identifier les voyageurs à risque élevé qui entrent au Canada, ainsi que la mesure dans laquelle le système améliore les résultats sur le plan de l'exécution et des renseignements, tout en réduisant au minimum les renvois inutiles pour un deuxième examen.*

Réponse de l'ASFC :

Une évaluation des méthodes de ciblage utilisées par l'ASFC débutera en 2006 et, entre autres choses, l'utilisation des avis de signalement fera partie de cette évaluation.

Initiative d'identification des voyageurs à risque élevé – (IIVRE)

Description du programme :

3.139 Dans le cadre de la Déclaration entre le Canada et les États-Unis sur la frontière intelligente et le plan d'action en 30 points, le Canada et les États-Unis se sont engagés à utiliser la technologie et l'échange de renseignements afin d'identifier plus efficacement les voyageurs à risque élevé.

3.140 Au moment de la vérification, l'Initiative IVRE prévoyait l'échange de l'information préalable des voyageurs (IPV), de renseignements sur les avis de signalement et sur l'historique des voyageurs, entre l'ASFC et son homologue aux États-Unis, la *U.S. CBP*. Plus précisément, l'Initiative IVRE facilite l'échange de données IPV tirés du Système d'information sur les passagers (SIPAX) et du *U.S. Automated Targeting System-Passenger (ATS-P) system* par le biais d'une voie de communication électronique protégée. On nous a informés que l'échange de données DP dans le cadre de l'Initiative IVRE ne commencerait pas avant juin 2006.

3.141 Le SIPAX de l'ASFC a deux composantes – une première composante « d'acquisition des données » et une composante secondaire « d'analyse des données ». La composante d'acquisition des données sert à la collecte de l'IPV et des données DP des passagers et de l'équipage de la compagnie aérienne à partir du système de réservation et de contrôle des départs du transporteur. Lorsque les éléments d'IPV sont reçues, le système extrait automatiquement des données requis du DP pour chaque personne à bord de l'avion.

3.142 La composante secondaire d'analyse sert à comparer les modèles de risque, établis conjointement par l'ASFC et la *U.S. CBP*, en fonction de tendances, d'analyses et d'indicateurs connus, lesquels sont comparés à l'information IPV/DP d'un voyageur pour déterminer le risque qu'il présente. Les modèles de risque comportent divers éléments des DP, mais les cotes et les niveaux de risque attribués varient selon le modèle qu'on leur assigne. La cote de risque sert à déterminer si un voyageur satisfait au seuil de risque établi pour un modèle particulier, ce qui, en théorie, l'identifierait comme un voyageur pouvant nécessiter un examen plus approfondi ou présentant un risque élevé ou inconnu.

3.143 Une fois qu'un modèle de risque est créé, il est possible d'apporter des modifications à ses composantes en fonction de l'analyse des résultats découlant de l'utilisation des données à la frontière. L'information sur les mesures d'exécution et des renseignements peuvent donner lieu à une modification.

3.144 La gestion des données échangées dans le cadre de l'Initiative IVRE Canada-É.-U. est définie dans le protocole d'entente (PE) concernant l'échange automatisé d'information sur les avis de signalement et l'échange d'information préalable sur les voyageurs, signé en mars 2005. Certains éléments du PE appuient la protection de la vie privée et la sécurité, dont les éléments qui suivent :

- l'information ne doit pas être communiquée de manière à permettre à un participant d'accéder directement au système d'information de l'autre;
- l'accès doit être administré en fonction de la nécessité d'accès;
- les responsabilités générales relatives à la sécurité et à la protection de l'information, y compris l'établissement de mécanismes de vérification et de suivi, sont énoncées dans le PE; et
- toute autre communication de données reçues dans le cadre du PE est assujettie à « la règle du tiers », selon laquelle le tiers qui expédie des données doit d'abord obtenir l'autorisation de celui qui les a transmises.

Renseignements personnels :

3.145 Dans le cadre de l'Initiative IVRE, les éléments de données de l'information préalable sur les voyageurs (IPV) et du dossier du passager (DP) sont utilisés à des fins de cotation des risques.

3.146 Les éléments de données IPV sont les suivants : nom, date de naissance, sexe, type de document, numéro du document, pays qui a délivré le document et la date et heure prévue de l'arrivée. Le DV renferme l'information sur un voyageur telle qu'elle apparaît dans les registres de contrôle des réservations et des départs du transporteur. Une liste des éléments de données DV se trouve dans l'encadré sous le paragraphe 3.99 du présent rapport.

Circulation transfrontalière des renseignements personnels :

3.147 Voici comment circulent les renseignements personnels dans le cadre de l'Initiative IVRE :

- Lorsque des données IPV/DP sont reçues d'un transporteur aérien commercial en route pour le Canada, elles sont automatiquement cotées selon des modèles de risque élaborés conjointement par le CNER et le *U.S. National Targeting Centre* (*NTC*). Le sous-système de cotation des risques fait partie du Système d'Information sur les passagers (SIPAX).

- Lorsque le profil d'un voyageur correspond au seuil prescrit, les données ci-dessous sont automatiquement envoyées au *U.S. NTC* pour être comparées à ses bases de données :

  - le prénom et le nom de famille du voyageur;
  - le sexe et la date de naissance;
  - le type de document de voyage;
  - le numéro du document de voyage;
  - le pays qui a délivré le document de voyage;
  - la date du vol et l'heure prévue de l'arrivée;
  - les modèles de risque établis; et
  - le seuil de risque du voyageur.

- Le CNER examine tous les renseignements concernant tout voyageur qui satisfait à un seuil donné, y compris le calcul de la cote de risque, les renseignements IPV/DP, les renseignements extraits des bases de données de l'ASFC et toute information reçue du *NTC*.

- À l'aide des renseignements recueillis, le CNER détermine s'il y a lieu de créer un avis de signalement ou de prendre d'autres mesures nécessaires.

3.148 Le processus que suit le CNER pour le traitement des demandes de renseignements provenant des États-Unis est similaire aux démarches décrites ci-dessus. Le CNER fait un examen manuel de tous les renseignements (mesures d'exécution, historique des passages voyageurs transfrontaliers et avis de signalement) avant de les transmettre au *U.S. NTC* pour examen.

Aucun échange de données ne se fait dans les circonstances suivantes :

- IPV correspond aux données d'une demande de renseignements sur un voyageur, mais il n'existe aucune information DP ou des données du système de contrôle des départs (SCD); ou les
- Informations DP ou du SCD correspondent à un voyageur visé par une demande de renseignements, mais il n'y a aucun dossier IPV qui est associé.

L'initiative IVRE n'a pas encore fait l'objet d'une évaluation visant à déterminer son efficacité à identifier les voyageurs à risque élevé.

3.149 La *Loi sur la protection des renseignements personnels* exige que la collecte de renseignements personnels se limite à l'information nécessaire à l'organisme pour réaliser son mandat législatif. Compte tenu du volume et de la nature délicate des renseignements personnels échangés entre le Canada et les États-Unis dans le cadre de l'initiative IVRE, l'ASFC doit –il s'agit en effet selon nous d'une obligation – déterminer si les avantages de cette initiative justifient l'ingérence dans la vie privée de millions de voyageurs sur qui des données IPV/DP sont recueillies.

3.150 Au moment de notre vérification, la Direction de l'évaluation de l'ASFC n'avait toujours pas mené d'étude sur l'Initiative IVRE, puisque l'étape de l'évaluation des risques des données contenues dans le DP n'était toujours pas commencé. La mise en œuvre complète est prévue d'ici juin 2006.

3.151 En l'absence d'une évaluation détaillée, l'efficacité de l'Initiative IVRE à accroître le taux d'interception et de résultats positifs (p. ex., empêcher l'entrée de personnes interdites sur le territoire et de marchandises prohibées, et recueillir des données du renseignement utiles) demeure spéculative. De plus, l'efficacité des éléments de données et de l'algorithme utilisés pour le traitement des données n'a pas encore été validée et n'a pas fait l'objet de tests de fiabilité. En outre, le nombre de faux positifs obtenus dans les résultats de l'Initiative IVRE demeure, à ce jour, inconnu.

3.152 Deux études produits par l'ASFC concernant l'utilisation de IPV/DP par les unités de ciblage des passagers (UCP) ont été examinés lors de notre vérification. Ces études ont suscité des préoccupations au sujet de la qualité et de la quantité des données IPV que l'Agence reçoit des transporteurs aériens. Notre examen des rapports sur ces études et les entrevues que nous avons menées auprès de responsables des unités de ciblage des passagers (UCP) dans le cadre de notre vérification ont produit des éléments de preuve anecdotiques appuyant l'idée que des données IPV inexactes ou incomplètes peuvent fausser les résultats de l'évaluation des risques. Bien qu'on nous ait dit qu'aucune mesure d'exécution ne serait amorcée uniquement en fonction de données IPV/DP, il n'en demeure pas moins que

des données DP incorrectes pourraient faire en sorte qu'un voyageur corresponde à un seuil de risque établi.

Même si un « faux négatif » (survenant lorsqu'un outil d'évaluation des risques ne permet pas d'identifier un voyageur à risque élevé) soulève des préoccupations légitimes en matière de sécurité, un « faux positif » est tout aussi inquiétant sur le plan de la protection de la vie privée.

3.153 Le commencement d'un examen détaillé de son système automatisé d'évaluation des risques afin de mesurer les résultats obtenus, y compris les conséquences non intentionnelles sur les voyageurs, pourra aider à déterminer si la collecte, l'utilisation et la communication de si grandes quantités de renseignements personnels peuvent être justifiées, autant sur le plan de la sécurité que sur celui de la protection de la vie privée.

Recommandation 15 :

Il est recommandé que l'ASFC entreprenne le plus tôt possible un examen de l'initiative IVRE comprenant une analyse des éléments de données spécifiques utilisés dans l'algorithme afin de déterminer si le système :

- *donne lieu à une augmentation du taux d'interception ou à d'autres résultats positifs;*
- *entraîne une augmentation du nombre de « faux positifs »;* et
- *produit des résultats qui justifient la collecte de renseignements personnels sur des millions de voyageurs, comparativement aux anciennes méthodes utilisées pour cibler les voyageurs à risque élevé.*

Réponse de l'ASFC :

L'initiative IVRE n'est pas encore entièrement mise en œuvre. Elle le sera en juin 2006, et une évaluation approfondie est prévue pour l'année suivante. Cette évaluation portera sur tous les aspects de l'Initiative, y compris la détermination des données et des techniques d'analyse qui génèrent des résultats positifs. En attendant que cette évaluation soit entreprise, et en réponse aux problèmes de qualité des données décelés au moment de l'examen suivant la mise en œuvre du SIPAX, l'ASFC a créé une fonction d'analyse détaillée des données afin d'assurer un suivi et d'analyser les problèmes d'exactitude et d'intégralité des données sur les passagers qui peuvent avoir une incidence sur l'efficacité des activités d'analyse et de ciblage.

L'ASFC prend très au sérieux sa responsabilité de protéger les renseignements personnels des millions de voyageurs qui arrivent au Canada. Elle a recours à des mesures extraordinaires pour garantir que les données personnelles des passagers sont protégées, en dépersonnalisant de plus en plus l'information de manière à ce que les responsables de l'ASFC ne puissent pas voir les noms des voyageurs lorsqu'ils font des analyses en vue de repérer des tendances et des modèles qui pourraient aider à améliorer le taux d'interception des personnes à risque élevé.

CADRE DE GESTION DE LA PROTECTION DE LA VIE PRIVÉE

Contexte :

3.154 Le concept et l'élaboration d'un cadre de gestion de la protection de la vie privée pour les ministères et organismes gouvernementaux sont relativement nouveaux. En règle générale, les organismes n'ont pas encore de cadre détaillé et cohésif pour la gestion des renseignements personnels qu'ils détiennent. Afin de combler cette lacune, la commissaire à la protection de la vie privée a récemment recommandé que le Secrétariat du Conseil du Trésor (SCT) élabore un modèle de cadre afin d'orienter la gestion de la protection de la vie privée dans l'administration fédérale (page 33 du Rapport annuel 2004-2005 au Parlement du Commissariat à la protection de la vie privée du Canada sur la *Loi sur la protection des renseignements personnels*).

3.155 Généralement, un cadre de gestion de la protection de la vie privée devrait :

- conscientiser de façon efficace l'organisme à l'importance de la gestion des renseignements personnels et promouvoir l'engagement à intégrer la protection de la vie privée dans les activités de gestion des programmes;

- établir des objectifs et des normes claires en matière de collecte, exactitude, sécurité, utilisation, communication, transmission, conservation et destruction des renseignements personnels ainsi que d'accès à ces renseignements;

- clarifier les structures, les rôles et les responsabilités de l'organisme relativement à la protection de la vie privée, et fournir des renseignements de base pour identifier les ressources et les savoir-faire nécessaires en vue d'acquérir des pratiques efficaces en matière de gestion de la protection de la vie privée;

- appliquer de saines approches de gestion des risques, plus particulièrement des évaluations des facteurs relatifs à la vie privée et des évaluations de la menace et des risques;

- inclure dans le cadre de gestion des pratiques exemplaires et des mesures de contrôle efficaces afin de promouvoir la conformité aux lois et règlements – intégrer les meilleures technologies disponibles pour améliorer la protection de la vie privée ainsi que les mécanismes qui permettront de régler efficacement les différends; repérer et combler les lacunes du système et les incidents liés à la protection de la vie privée;

- promouvoir la responsabilisation et l'amélioration continue des pratiques de traitement des renseignements personnels par les moyens suivants : présentation de rapports sur les programmes, évaluation et vérification; surveillance continue des pratiques de traitement des renseignements personnels; formation continue en matière de protection de la vie privée pour les employés.

3.156 Notre vérification n'avait pas la portée nécessaire pour viser l'ensemble des programmes et activités de sécurité de l'ASFC, ni pour repérer des cas précis d'utilisation inappropriée ou de perte de renseignements personnels. Toutefois, les considérations en matière de protection de la vie privée sont étroitement liées à la sécurité et à la protection des

renseignements personnels et sont susceptibles d'être affectées par la sécurité dans son ensemble. C'est pourquoi nous avons examiné les politiques et les procédures de sécurité de l'Agence, ses processus de signalement des incidents de sécurité et la mesure dans laquelle les manquements à l'égard de la protection de la vie privée sont signalés à l'interne.

3.157 En menant les entrevues et en examinant les documents, nous avons pu constater que l'ASFC comprend généralement bien les concepts de protection de la vie privée et souhaite améliorer ses pratiques de gestion en cette matière. Les enjeux relatifs à la gestion de la protection des renseignements personnels et de la vie privée sont exposés dans divers documents de l'ASFC sous forme d'ébauches ou de documents finaux. La plus grande partie de la documentation que nous avons examinée avait, soit été récemment créée par l'ASFC, soit été transmise par l'organisme qui l'a précédée, l'Agence des douanes et du revenu du Canada (jadis l'ADRC). La documentation comprenait, entre autres :

- Politiques et procédures en matière de sécurité – Manuel des finances et de l'administration de l'ADRC
    - Désignation des biens et des renseignements classifiés et protégés
    - Entreposage, transmission et destruction des biens et des renseignements de nature délicate
    - Protection des biens et des renseignements classifiés et protégés à l'extérieur des lieux de travail
    - Triage de sécurité du personnel
    - Contrôle de l'accès
    - Signalement des incidents de sécurité
    - Accès aux systèmes informatiques de l'Agence
    - Normes et pratiques de sécurité de la TI
    - Accès à distance aux systèmes informatiques de l'Agence et accès à distance à partir de ces systèmes
    - Évaluation de la menace et des risques (EMR) pour les systèmes de TI
    - Examens et inspections de sécurité des systèmes informatiques
    - Utilisation d'ordinateurs personnels aux résidences des employés
    - Consignation et surveillance de l'accès des employés aux données des clients
    - Enquêtes internes sur des cas d'inconduite, présumée ou soupçonnée, par des employés

- Politiques régissant l'utilisation et la communication de renseignements douaniers

- Instruments de délégation de pouvoirs pour l'administration des obligations de l'ASFC conformément à la *Loi sur l'accès à l'information* et à la *Loi sur la protection des renseignements personnels*

- Trousses de formation pour les employés régionaux, incluant un guide d'apprentissage, pour la communication de renseignements douaniers conformément à l'article 107 de la *Loi sur les douanes*

- Évaluations des facteurs relatifs à la vie privée et évaluation de la menace et des risques effectuées par l'ASFC

- Protocoles d'entente ou ententes écrites concernant l'accès à des renseignements détenus par l'ASFC ou l'utilisation de ces renseignements

- Ébauche d'un nouveau guide sur l'élaboration d'ententes écrites de collaboration avec les provinces, les territoires et d'autres ministères et organismes fédéraux

3.158 L'ASFC se fonde également sur les directives, les politiques et les instructions du Conseil du Trésor pour garantir la conformité à la *Loi sur la protection des renseignements personnels*. Elle se réfère aussi à des liens informels établis par des personnes pour répondre à un besoin immédiat ou local. Enfin, nous avons été informés que l'ASFC a l'intention d'élaborer ses propres politiques et lignes directrices en matière de sécurité et de protection de la vie privée pour remplacer et mettre à jour celles que lui a léguées l'ADRC. Ces politiques et lignes directrices reflèteront les pratiques et les besoins des programmes dont l'ASFC est responsable.

Le moment est opportun pour l'ASFC d'élaborer et de mettre en œuvre un cadre de gestion de la protection de la vie privée.

3.159 Malgré l'existence des documents mentionnés ci-dessus et le fait que l'Agence a l'intention d'élaborer des politiques et des lignes directrices relatives à la protection de la vie privée, notre vérification a démontré que l'Agence n'a pas de cadre détaillé et cohésif de la gestion de la protection de la vie privée – un cadre qui serait étroitement intégré aux opérations de l'ensemble de l'organisme. Plusieurs éléments importants d'un cadre de gestion efficace sont inexistants, incomplets ou périmés.

3.160 Un des éléments clés d'un cadre de gestion de la protection de la vie privée est la capacité de repérer, d'enquêter et de signaler les infractions à la protection de la vie privée relatives à la collecte, l'utilisation, la communication ou la destruction présumée de renseignements personnels. Il s'agit d'un des éléments que nous avons examinés et pour lequel nous avons fourni des résultats détaillés. L'information que nous avons obtenue pendant la vérification ne nous a pas permis de bien comprendre comment l'ASFC décèle et signale les infractions à la protection de la vie privée dans l'ensemble de l'organisme. Voici ce que nous avons appris et observé lors de nos entrevues avec des responsables de la sécurité et par notre examen des dossiers et des documents stratégiques relatifs à l'identification et au signalement d'infractions à la protection de la vie privée.

- Le président de l'ASFC est informé mensuellement des incidents relatifs à la sécurité qui sont signalés à l'Administration centrale de l'ASFC, ainsi que de tous les cas exigeant une enquête sur les allégations de mauvaise conduite d'un employé.

- Les politiques et les procédures qui étaient en place pour la gestion et le signalement d'incidents relatifs à la sécurité au moment de notre examen portaient principalement sur des points précis, notamment :

    - vol, perte ou destruction de recettes, de fonds, de marchandises saisies, de biens détenus ou d'autres biens;
    - abus, menaces, harcèlement criminel et voies de fait à l'égard d'employés;
    - compromission soupçonnée ou réelle de renseignements protégés ou classifiés;
    - codes malveillants et alertes/attaques de virus à l'endroit des systèmes de TI ou de communication;

- destruction, détérioration, modification ou falsification de dossiers;
- perte, vol ou utilisation malveillante de cartes d'identification/d'accès, de laissez-passer; et
- incidents ayant des répercussions sur la sécurité physique d'un immeuble ou d'une installation.

- L'ASFC compte 14 catégories d'incidents relatifs à la sécurité. Néanmoins, dans les politiques, procédures et formulaires de signalement de l'Agence se rapportant directement à des questions relatives à la protection de la vie privée, rien n'indique la manière dont l'Agence traite les cas de collecte, d'utilisation ou de communication inappropriée (accidentelle ou autre) de renseignements personnels que pourraient effectuer ses employés.

- Depuis que la création l'ASFC en décembre 2003, 30 rapports d'incidents relatifs à la sécurité (RIS)ont été produits auprès de la Section de la sécurité de l'Administration centrale de l'ASFC. Cependant, nous n'avons pas pu déterminer si les bureaux régionaux ont signalé à l'Administration centrale tous les incidents se rapportant à des infractions dans le traitement des renseignements personnels.

- Parmi les RIS que nous avons examinés :

    - 50 p. 100 ne se rapportaient pas à des renseignements personnels.

    - Des 50 p. 100 des incidents où des renseignements personnels avaient été dévoilés ou mis à risque :

- quatre se rapportaient à des ordinateurs perdus ou volés, surtout des ordinateurs portatifs (les rapports indiquent que ces ordinateurs auraient pu contenir des renseignements personnels, mais un des ordinateurs était équipé d'un dispositif de cryptage);
- deux se rapportaient à la perte d'un cahier de notes d'un inspecteur de douanes ou à l'accès inapproprié à un tel cahier;
- trois se rapportaient à la perte de courrier en transit;
- trois se rapportaient à l'accès physique non autorisé à des secteurs de travail à accès restreint;
- deux concernaient l'accès inapproprié à la TI par l'entremise d'un employé partageant un compte d'utilisateur avec un collègue; et
- un incident se rapportait à la communication d'un mot de passe.

- Nous avons noté certains cas où les rapports sur des incidents relatifs à la sécurité soulevaient des questions sur la possibilité que les ordinateurs aient contenu des renseignements personnels, mais la section narrative du rapport ne donnait pas de réponse à ces questions.

- Nous avons aussi constaté lors de nos entrevues que l'ASFC ne pouvait pas nous indiquer facilement le nombre d'employés qui se sont engagés dans l'organisation du travail « flexible » (faisant du télétravail), ni le nombre et le type d'ordinateurs qui avaient été assignés aux personnes travaillant à l'extérieur des locaux de l'ASFC. Le travail à l'extérieur des bureaux de l'ASFC impliquant la manipulation de renseignements douaniers et personnels à l'aide de nouvelles technologies (p. ex., les « Blackberry »)

pose des défis sur le plan des installations physiques, de la TI, des opérations et de la protection de la vie privée. Les assistants numériques personnels (ANP) exigent des mesures de protection spéciales afin de réduire des risques qui diffèrent de ceux que présente le cadre de travail habituel.

3.161 Nous avons également constaté en faisant notre vérification que l'Agence n'a aucune politique interne officielle qui détermine le moment où la Division de l'accès à l'information et de la protection des renseignements personnels doit être informée des situations suivantes :

- tout incident relatif à la sécurité et toute enquête interne sur des actes répréhensibles qui concernent des renseignements personnels; ou
- les plaintes que les unités opérationnelles de l'ASFC (un poste frontalier ou un aéroport, par exemple) reçoivent ou déposent relativement à des personnes qui allèguent que leur droit à la vie privée a été enfreint.

L'Agence nous a informés qu'un processus officiel sera établi et inclus dans les politiques qu'elle élabore actuellement.

3.162 En outre, les nouveaux documents destinés aux formations sur la protection de la vie privée que nous avons examinés ne précisent pas en quoi consiste une « atteinte à la vie privée ». Ces documents ne présentent pas non plus les procédures d'enquête et de présentation de rapport se rapportant aux atteintes à la vie privée (p. ex. : utilisation, communication ou perte inappropriées de renseignements personnels).

3.163 Enfin, il n'y a pas eu de vérification du processus qu'utilise l'ASFC pour signaler les incidents relatifs à la sécurité. Par conséquent, l'Agence n'est pas en mesure de certifier que son processus est complet et exact, ni de confirmer qu'elle est au fait de tous les incidents concernant des renseignements personnels, que ces incidents résultent d'écarts de conduite ou qu'ils soient considérés accidentels.

3.164 Nous estimons que le moment serait opportun pour l'ASFC de définir et mettre en œuvre un cadre de gestion de la protection de la vie privée. Elle pourrait ainsi améliorer les systèmes et les processus d'exercice et de renforcement du contrôle de la collecte, de l'utilisation, de la communication, de la conservation et de la destruction des renseignements personnels généraux et des renseignements personnels qui sont transmis à d'autres pays.

3.165 Nous suggérons que l'ASFC tienne compte des points ci-dessous dans l'élaboration et la mise en œuvre de son cadre de gestion de la protection de la vie privée :

- Nommer un Chef de la protection de la vie privée (CPVP) et lui donner un mandat clairement défini et un rôle central visant à promouvoir la sensibilisation et la conformité aux lois en matière de protection de la vie privée et aux pratiques établies de gestion de l'information. (Au moment de notre vérification, un fonctionnaire avait été nommé CPVP. Cependant, sa nomination n'avait pas encore été rendue officielle au moyen d'une délégation formelle de pouvoirs et par l'assignation d'un mandat défini.)

- Créer un comité de cadres supérieurs qui superviseront l'élaboration d'un cadre de gestion de la protection de la vie privée et qui planifieront, surveilleront et coordonneront les mesures prises pour renforcer les pratiques de gestion de la vie privée, y compris l'élaboration de politiques à cet égard. Ce comité aurait aussi pour rôle de s'assurer que des « évaluations des facteurs relatifs à la vie privée » soient effectuées lorsque

nécessaire, que l'orientation et la formation demandées soient fournies aux secteurs de programme chargés des questions de protection de la vie privée, et que les diverses ententes qui régissent l'échange de renseignements personnels soient à jour et qu'elles soient respectées par l'ensemble de l'ASFC.

- Créer une politique ministérielle de protection de la vie privée qui définit clairement les rôles et les responsabilités et détermine les situations où les pratiques en matière de protection de la vie privée sont essentielles à l'évaluation du rendement des employés. La politique devrait également définir les attentes en matière de gestion et de contrôle de la circulation transfrontalière des renseignements personnels pendant sa durée de vie. Nous avons constaté que l'ASFC n'a pas encore émis de politique portant exclusivement sur la protection de la vie privée.

- Instaurer un mécanisme de contrôle périodique du rendement par des moyens comme l'identification automatisée et des rapports sur les opérations informatiques irrégulières, une analyse des modèles d'utilisation des systèmes et des vérifications internes de la protection des renseignements personnels. Ces vérifications permettraient à la fois de garantir l'utilisation de pratiques normalisées et de fournir à la haute direction l'assurance que les renseignements personnels sont gérés conformément à la *Loi sur les douanes*, à la *Loi sur la protection des renseignements personnels* et aux politiques internes et ententes applicables en matière d'échange d'information. De tels mécanismes ne semblent pas exister actuellement à l'ASFC.

- Offrir régulièrement des ateliers de formation sur l'application – et le respect – de la *Loi sur la protection des renseignements personnels*. Pendant notre vérification, l'ASFC a commencé à donner ce type de formation. Bien qu'aucune formation n'ait été donnée pendant l'exercice 2004-2005, des ateliers ont eu lieu depuis dans six régions. L'ASFC prévoit donner des cours sur la protection des renseignements personnels au moins une fois dans chaque région d'ici mars 2006. Grâce à ces efforts sur le plan de la formation et à l'introduction d'une stratégie et d'un plan de formation continue, le niveau de sensibilisation et de conformité à la protection de la vie privée devrait augmenter.

- Établir un système détaillé fiable pour la consignation des plaintes et des incidents relatifs à la protection des renseignements personnels dans l'ensemble de l'ASFC (y compris les régions et les points d'entrées) afin de garantir que les plaintes et incidents sont signalés et que les mesures nécessaires sont prises.

3.166 Une fois qu'un cadre aura été établi, l'ASFC pourra prioriser la mise en œuvre des différents éléments de ce cadre et utiliser celui-ci comme point de référence dans la prise de décisions et l'élaboration de mesures futures.

3.167 Bien que nous recommandions à l'Agence d'établir un cadre de gestion de la protection de la vie privée, nous tenons à souligner que pendant notre vérification nous n'avons relevé aucune preuve de mauvaise utilisation de renseignements personnels. Il faut toutefois reconnaître que, du fait qu'un grand nombre d'échanges transfrontaliers avec les États-Unis se font verbalement et du fait qu'il manquait des dossiers détaillés sur les communications, il y a lieu de se demander si l'Agence gère toujours les renseignements personnels de manière appropriée.

Recommandation 16 :

Il est recommandé que l'ASFC élabore un cadre détaillé de gestion de la protection de la vie privée adapté spécifiquement à ses besoins. L'agence devrait se fonder sur ce cadre pour améliorer ses politiques, systèmes, procédures et pratiques en matière de protection de la vie privée. Dans le cadre de cet exercice, l'ASFC devrait établir clairement et consolider les procédures de signalement des incidents relatifs à la vie privée et chercher des façons de renforcer le contrôle de la collecte, de l'utilisation et de la communication de renseignements personnels dans le cadre de ses opérations quotidiennes.

Réponse de l'ASFC :

Nous approuvons cette recommandation. L'ASFC travaillera en collaboration avec le Secrétariat du Conseil du Trésor (SCT) et le Commissariat à la protection de la vie privée à identifier les lacunes de notre cadre de gestion de la protection de la vie privée; nous accueillerons favorablement leurs conseils.

RAPPORTS PUBLIC SUR LA CIRCULATION TRANSFRONTALIÈRE DES DONNÉES

Contexte :

3.168 Comme prolongement de notre examen des activités de l'ASFC dans le secteur de la circulation transfrontalière des données, nous avons examiné de quelle manière et dans quelle mesure l'ASFC informe le Parlement et la population canadienne de la communication transfrontalière de renseignements personnels.

3.169 Notre examen a porté sur les documents suivants :

- *Info Source*
    - Sources d'information du gouvernement fédéral pour 2004-2005
- Rapports officiels
    - Rapports sur les plans et priorités
    - Rapports ministériels sur le rendement
    - Rapports annuels au Parlement
    - Rapports annuels sur l'application de la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*
- Documents sur le site Web

3.170 Nous avons examiné les banques de renseignements personnels listées et décrites dans *Info Source* afin de trouver des mentions d'échanges ou de communications de renseignements avec les États-Unis ou d'autres pays. Pour les rapports officiels et les documents sur le Web, nous avons utilisé des fonctions de recherche globale en vue de trouver des références à « la mise en commun » ou à « l'échange » de renseignements dans des contextes où l'intervention des États-Unis ou de juridictions étrangères est mentionnée ou peut être raisonnablement supposée.

L'ASFC pourrait améliorer l'information figurant dans ses documents visant à informer les Canadiennes et les Canadiens ainsi que le Parlement de la circulation transfrontalière des renseignements personnels.

3.171 Essentiellement, les Canadiennes et les Canadiens devraient pouvoir trouver de l'information adéquate dans des documents destinés au grand public (sur support papier ou électronique) concernant les renseignements personnels que l'ASFC échange avec d'autres pays. Toutefois, bien que nous ayons trouvé certaines exceptions dans des rapports publics, les renvois aux activités de l'ASFC relatives à la circulation transfrontalière des données sont plutôt brefs. Ils sont peu détaillés et n'indiquent pas clairement la mesure dans laquelle les renseignements personnels sont échangés avec d'autres pays.

Dans certains cas, l'Agence fournit plus de renseignements sur son site Web que dans les rapports au Parlement ou dans *Info Source* (la publication qui énumère les catégories de renseignements personnels détenus par l'Agence et utilisés dans des programmes connexes).

Voici un résumé de nos observations :

3.172 *Info Source :*

- Onze des descriptions de banques de renseignements personnels de l'ASFC font mention d'échange d'information avec des organismes étrangers. De ce nombre, seulement trois fournissent des détails importants sur ces activités d'échange.
- Les organismes étrangers avec lesquels se font les échanges de renseignements étaient identifiés dans seulement trois des banques de renseignements personnels. Dans d'autres cas, les références étaient générales et imprécises – p. ex., autorités des États-Unis, organismes d'exécution et d'enquêtes en matière de droit étranger.
- Les pouvoirs de communication de renseignements à des gouvernements étrangers étaient mentionnés en termes généraux dans cinq cas comme étant établis conformément à une entente ou à un arrangement afin de mener une enquête licite ou d'appliquer ou d'exécuter une loi.
- Il n'y a aucune référence spécifique à des échanges de renseignements personnels avec les États-Unis ou d'autres gouvernements étrangers dans les descriptions des banques des renseignements personnels pour les systèmes SIPAX (i.e. information IPV/ DP) et Système intégré d'exécution des douanes (SIED).
- La banque de renseignements personnels des dossiers du renseignement des douanes (CBSA PPU 015) n'a pas été désignée comme ajout à la prochaine version d'*Info Source*. Cette banque de renseignements personnels renferme l'information utilisée par l'ASFC et par les organismes d'exécution de la loi et les organismes d'enquête canadiens et étrangers.

3.173 Rapports officiels :

(1) *Rapport sur les plans et priorités 2005-2006*

- Ce document mentionne, dans quatre rubriques, l'échange d'information avec des organismes étrangers. Toutefois, les mentions sont peu détaillées et n'indiquent pas clairement la mesure dans laquelle des renseignements personnels sont échangés.

(2) Rapport ministériel sur le rendement pour la période se terminant le 31 mars 2004

- Le rapport mentionne dans onze rubriques l'échange d'information et/ou du renseignement avec des organismes étrangers. Encore une fois, les mentions sont peu détaillées et ne précisent pas la mesure dans laquelle les renseignements personnels sont utilisés. Dans cinq cas, l'échange de renseignements est mentionné lorsqu'on parle du Centre national d'évaluation des risques (CNER) et des unités conjointes d'analyse des passagers (UCAP). À noter que les UCAP du Canada et des États-Unis qui partageaient des locaux ne sont plus opérationnelles. L'échange de renseignements est aussi mentionné en termes généraux relativement à la Déclaration sur la frontière intelligente Canada/États-Unis.

(3) *Rapport annuel au Parlement sur les plans et les priorités 2005-2006*

- Au moment de la vérification, l'ASFC n'avait pas encore publié son Rapport annuel au Parlement.

(4) *Rapport annuel sur l'application de la* Loi sur l'accès à l'information *et de la* Loi sur la protection des renseignements personnels

- Au moment de la vérification, l'ASFC n'avait pas encore publié de rapport annuel sur son application de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*.

3.174 Site Web de l'ASFC :

- Huit documents faisaient mention de l'échange de renseignements avec des gouvernements étrangers. Seulement un document – une fiche d'information sur l'IPV/DP et la base de données SIPAX – décrivait la pratique en détail. Les autres mentions apparaissaient dans des fiches d'information concernant la Déclaration sur la frontière intelligente, le Centre national d'évaluation des risques, le Programme d'expéditions rapides et sécuritaires (Programme EXPRES), le renseignements sur l'Immigration, le renforcement des examens des douanes dans les aéroports et le ciblage des conteneurs en transit dans les ports maritimes.
- Sauf peut-être la fiche d'information aux bases de données IPV/DP et le SIPAX, aucun des documents figurant sur le site Web de l'ASFC ne fournissait suffisamment d'information sur la circulation transfrontalière de données pour que nous ayons une image précise de la nature, du moment et des motifs des échanges de renseignements.

Recommandation 17 :

Il est recommandé que l'ASFC examine ses fonds de renseignements personnels afin de s'assurer que toutes les banques de renseignements personnels soient énumérées dans la prochaine version d'Info Source, comme l'exige l'article 11 de la Loi sur la protection des renseignements personnels*.*

Recommandation 18 :

Il est également recommandé que l'ASFC examine toutes les descriptions de banques de renseignements personnels afin de s'assurer que toutes les utilisations des renseignements de ces banques — y compris l'échange de renseignements avec des gouvernements étrangers – y soient correctement mentionnées.

Réponse de l'ASFC aux récommandations 17 et 18 :

L'ASFC continuera à travailler en collaboration avec le Secrétariat du Conseil du Trésor afin de s'assurer que toutes les banques de renseignements personnels existantes et proposées indiquent avec précision avec qui et pourquoi l'Agence échange ces renseignements, y compris les activités avec ses partenaires internationaux.

3.175 Nous sommes également d'avis que l'ASFC, conjointement avec le Secrétariat du Conseil du Trésor et d'autres ministères gouvernementaux, devrait envisager d'autres stratégies afin de mieux informer le Parlement et le grand public des échanges de renseignements personnels avec d'autres pays. Cet exercice devrait comprendre un examen sur les moyens de rendre l'information contenue dans les rapports annuels actuels plus intelligible. Une autre stratégie à envisager consiste à publier périodiquement (p. ex., au moment de l'examen de la *Loi antiterroriste*) un rapport spécial et du gouvernement fédérale sur cette question, ou à utiliser collectivement la publication *Info Source*, les rapports annuels et les sites Web des ministères pour accroître la transparence des activités de l'Agence liées au traitement des renseignements personnels et en faciliter la compréhension pour les Canadiennes et les Canadiens, ainsi que pour le Parlement. La transparence favorise une responsabilisation à l'égard du public et constitue l'un des dix principes d'équité dans le traitement de l'information que l'on retrouve dans la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)*.

3.176 Notre examen des rapports de quatre autres entités a donné des résultats similaires. Il a confirmé que l'ASFC n'est pas le seul organisme qui doit fournir de meilleurs renseignements sur ses activités dans le secteur de la circulation transfrontalière des données. En conséquence, nous allons également continuer de discuter de cette question avec le Secrétariat du Conseil du Trésor.

Recommandation 19 :

Il est recommandé que l'ASFC, conjointement avec le Secrétariat du Conseil du Trésor, évalue d'autres stratégies et moyens pour mieux informer le Parlement et le grand public sur l'échange de renseignements personnels avec d'autres pays.

Réponse de l'ASFC :

L'ASFC a noté que la question des rapports ministériels sur le circulation transfrontalière des données est un dossier que le bureau du Commissariat à la protection de la vie privée va poursuivre avec le Secrétariat du Conseil du Trésor.

L'ASFC va, d'une manière indépendante, consulter le Secrétariat du Conseil de Trésor afin de discuter des stratégies possibles qui pourraient être employées par nous – et peut-être par d'autres institutions fédérales – afin d'améliorer la transparence concernant la nature de nos relations internationales, tout en respectant nos engagements internationaux sur la confidentialité. L'ASFC va aussi explorer avec le Secrétariat du Conseil du Trésor toutes les suggestions faites par le bureau du Commissariat à la protection de la vie privée du Canada à cet égard.

ANNEXE A

LISTE DES RECOMMANDATIONS

Exécution des dispositions douanières :

1. ***En vue de renforcer son cadre de gestion de la protection des renseignements personnels, il est recommandé que l'ASFC s'efforce de mettre à jour et de consolider ses protocoles d'entente sur l'échange de renseignements personnels avec les États-Unis, ce qui comprendrait la mise en place de processus offrant une garantie mutuelle que la circulation transfrontalière de renseignements personnels fasse l'objet de mesures de protection appropriées.***

2. ***Il est recommandé que l'ASFC formule un plan d'action pour aborder la question des échanges verbaux de renseignements personnels. Un tel plan devrait prendre en considération les activités suivantes :***

   - ***déterminer l'ampleur des échanges verbaux de renseignements douaniers avec les autorités douanières des États-Unis et mettre en place des mesures afin de garantir que toute communication de renseignements personnels se conforme, de façon continue, aux politiques et aux accords gouvernementaux;***

   - ***mettre en place des mesures afin de garantir que toutes les communications de renseignements personnels sont enregistrées, comme l'exige la politique de l'ASFC ;***

   - ***diffuser un communiqué à tout le personnel concernant le processus d'approbation régissant la communication de renseignements personnels en vertu du paragraphe 107(8) de la* Loi sur les douanes*, et renforcer les exigences de la politique en incluant un module spécifique pour les ateliers de formation relatifs à la mise en application de la* Loi sur la protection des renseignements personnels *et l'article 107; et***

   - ***surveiller le respect des politiques régissant les échanges transfrontaliers de données afin de garantir la mise en place de contrôles de gestion adéquats pour protéger les renseignements personnels de toute communication non autorisée.***

3. ***Il est recommandé que l'ASFC mette en place des moyens de consigner tous les échanges transfrontaliers de données aux fins des programmes de saine gestion et de reddition de comptes. Il pourrait s'agir – sans s'y limiter – de l'élaboration de diagrammes indiquant la circulation des données, et des modifications apportées aux systèmes d'information existants afin d'identifier et d'enregistrer de manière fiable toutes les activités d'échanges avec les gouvernements étrangers.***

Système intégré d'exécution des douanes (SIED) :

4. ***Il est recommandé que l'ASFC collabore avec ses homologues des États-Unis en vue d'offrir l'assurance mutuelle que leurs contrôles de sécurité électroniques respectifs permettent de garantir la protection des renseignements personnels des citoyens relatifs aux avis de signalement échangés. À cet égard, il faudrait entre autres envisager d'étendre la portée des ententes sur les niveaux de service, pour y inclure des descriptions des processus de suppression des données au moment de l'expiration de la période de conservation ou lorsqu'elles sont annulées, ainsi que l'obligation d'effectuer des vérifications périodiques de la sécurité et de la protection des renseignements personnels.***

5. ***Il est recommandé que l'ASFC modifie son application SIED de manière à ce qu'elle permette de consigner les renseignements chaque fois qu'un imprimé est fait à partir du système.***

6. ***Il est recommandé que l'ASFC définisse et fasse connaître les rôles et les responsabilités de tous les responsables officiels de la TI au sein de l'organisme, en faisant une mise à jour des descriptions d'emploi et des organigrammes.***

7. ***Il est recommandé que l'ASFC poursuive ses efforts en vue de créer un cadre cohésif de gestion de la sécurité. L'Agence devrait effectuer une vérification de ce cadre un an après sa mise en œuvre afin de s'assurer que celui-ci protège efficacement les renseignements douaniers et personnels. Nous demandons aussi à l'ASFC de fournir les résultats de cette vérification au Commissariat à la protection de la vie privée.***

8. ***Il est recommandé que l'ASFC consigne et surveille l'accès des administrateurs de la base de données du SIED et les opérations qu'ils y effectuent sur le système sur le système.***

Système d'information sur les passagers (SIPAX) :

9. ***Il est recommandé qu'une entente officielle sur les niveaux de service soit mise en place entre le Canada et les États-Unis, entente qui prévoira des normes de sécurité approuvées par les deux parties (en fonction des normes de sécurité et des normes sur la qualité et le filtrage des données selon la norme de la Gestion de la sécurité des technologies de l'information (GSTI) du gouvernement du Canada), de manière à ce que chacun des pays puisse prendre des mesures qui garantiront que les renseignements personnels échangés sont complets, à jour et exacts.***

10. ***Il est recommandé qu'une liste de contrôle normalisée des droits d'accès au système soit utilisée lorsqu'un changement dans le rôle, les responsabilités ou le statut d'emploi d'un employé exige que son gestionnaire réévalue les droits d'accès dont cet employé à besoin, les autorisations d'accès requises et les autorisations à révoquer.***

11. Il est recommandé que le document du service de dépannage du SIPAX soit mis à jour de manière à inclure des lignes directrices sur la révocation des droits d'accès au système. Nous recommandons également que les ressources humaines de l'ASFC consultent la liste de contrôle afin de s'assurer que les droits d'accès des employés qui changent de poste, qui sont en congé à long terme ou qui ont quitté l'organisme soient examinés et révisés ou révoqués en conséquence.

12. Il est recommandé d'effectuer périodiquement un contrôle rigoureux de l'accès des administrateurs au serveur et à la base de données du SIPAX afin de garantir des contrôles adéquats de leur utilisation du système.

<u>Centre national d'évaluation des risques (CNER)</u> :

13. Il est recommandé que l'ASFC prenne des mesures afin de s'assurer que tous les avis de signalement échangés avec les États-Unis soient transmis au Centre national d'évaluation des risques pour faire l'objet d'un contrôle de qualité, d'une surveillance continue et d'une vérification.

14. Il est recommandé que l'ASFC évalue le système d'échange des avis de signalement en vue de déterminer son efficacité à identifier les voyageurs à risque élevé qui entrent au Canada, ainsi que la mesure dans laquelle le système améliore les résultats sur le plan de l'exécution et des renseignements, tout en réduisant au minimum les renvois inutiles pour un deuxième examen.

15. Il est recommandé que l'ASFC entreprenne le plus tôt possible un examen de l'initiative IVRE comprenant une analyse des éléments de données spécifiques utilisés dans l'algorithme afin de déterminer si le système :

- ***donne lieu à une augmentation du taux d'interception ou à d'autres résultats positifs;***
- ***entraîne une augmentation du nombre de « faux positifs »; et***
- ***produit des résultats qui justifient la collecte de renseignements personnels sur des millions de voyageurs, comparativement aux anciennes méthodes utilisées pour cibler les voyageurs à risque élevé.***

<u>Cadre de gestion de la protection de la vie privée</u> :

16. Il est recommandé que l'ASFC élabore un cadre détaillé de gestion de la protection de la vie privée adapté spécifiquement à ses besoins. L'agence devrait se fonder sur ce cadre pour améliorer ses politiques, systèmes, procédures et pratiques en matière de protection de la vie privée. Dans le cadre de cet exercice, l'ASFC devrait établir clairement et consolider les procédures de signalement des incidents relatifs à la vie privée et chercher des façons de renforcer le contrôle de la collecte, de l'utilisation et de la communication de renseignements personnels dans le cadre de ses opérations quotidiennes.

<u>Rapport public sur la circulation transfrontalière des données</u> :

17. Il est recommandé que l'ASFC examine ses fonds de renseignements personnels afin de s'assurer que toutes les banques de renseignements personnels soient énumérées dans la prochaine version d'Info Source, comme l'exige l'article 11 de la Loi sur la protection des renseignements personnels.

18. Il est également recommandé que l'ASFC examine toutes les descriptions de banques de renseignements personnels afin de s'assurer que toutes les utilisations des renseignements de ces banques – y compris l'échange de renseignements avec des gouvernements étrangers – y soient correctement mentionnées.

19. Il est recommandé que l'ASFC, conjointement avec le Secrétariat du Conseil du Trésor, évalue d'autres stratégies et moyens pour mieux informer le Parlement et le grand public sur l'échange de renseignements personnels avec d'autres pays.

ANNEXE B

CRITÈRES D'ÉVALUATION DE LA VÉRIFICATION

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

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

Responsabilité (principe 1 de la *LPRPDÉ*)

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 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.

Remarque : Il existe des critères applicables aux ententes sur l'échange de renseignements et à l'impartition. Pour les renseignements détenus par une institution gouvernementale, la norme de protection devrait 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 mettre en œuvre des politiques et des pratiques destinées à : donner suite aux principes, y compris la mise en œuvre de procédures visant à protéger les renseignements personnels; la mise en place de 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; la rédaction des documents explicatifs concernant leurs politiques et procédures.

Transparence (principe 8 de la *LPRPDÉ*)

Critères :

Les organisations doivent faire preuve de transparence au sujet de leurs politiques et pratiques de gestion des renseignements personnels. Une personne doit pouvoir obtenir sans efforts déraisonnables de l'information au sujet de leurs politiques et pratiques. Ces renseignements doivent être fournis sous une forme généralement compréhensible.

Les renseignements fournis doivent comprendre le nom ou le titre et l'adresse de la personne responsable de la politique et des pratiques de l'organisation ainsi que le nom de la personne à qui il faut acheminer les plaintes et les demandes de renseignements; le moyen d'accès aux renseignements personnels que possède l'organisation; la description du genre de renseignements personnels que possède l'organisation, y compris une explication générale de l'usage auquel ils sont destinés; une copie de toute brochure ou autre document d'information expliquant la politique, les normes ou les codes de l'organisation; et la définition de la nature des renseignements personnels communiqués aux organisations connexes (p. ex., les filiales).

Remarque : Une organisation peut prendre divers moyens pour rendre accessible l'information concernant sa politique et ses pratiques. La méthode choisie est fonction de la nature de ses activités et d'autres considérations. Par exemple, l'organisation peut offrir des brochures à son établissement, envoyer des renseignements à ses clients par la poste, offrir un accès en ligne ou un service téléphonique sans frais.

Détermination des fins de la collecte des renseignements (principe 2 de la *LPRPDÉ*)

Critères :

L'organisation doit documenter les fins auxquelles des renseignements personnels sont recueillis.

Les fins auxquelles les renseignements personnels sont recueillis doivent être précisées à la personne de qui ils sont obtenus avant la collecte ou au moment de celle-ci.

Lorsque des renseignements personnels recueillis doivent être utilisés à des fins qui n'ont pas été déterminées avant la collecte, les nouvelles fins auxquelles ils sont destinés doivent être déterminées avant l'utilisation. À moins que ces nouvelles fins 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.

Remarque : Il peut y avoir des exceptions à ce principe lorsque la collecte des renseignements se fait conformément 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. Voir l'article 5 de la *Loi sur la protection des renseignements personnels*.

Collecte de 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 gouvernementale sont ceux qui ont un lien direct avec ses programmes ou ses activités.

Sous réserve des exceptions énoncées au paragraphe 5(3) de la *Loi sur la protection des renseignements personnels*, l'institution gouvernementale est tenue d'informer la personne concernée des fins auxquelles les renseignements sont destinés.

Dans la mesure du possible, les institutions gouvernementales doivent recueillir elles-mêmes auprès des personnes concernées les renseignements personnels qu'elles ont l'intention d'utiliser à des fins administratives.

Consentement (principe 3 de la *LPRPDÉ*)

Critères :

Les organisations doivent faire un effort raisonnable pour que la personne visée par des renseignements personnels recueillis soit informée des fins auxquelles ces renseignements sont destinés. Pour que le consentement soit valide, 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 des 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.

Limite de la collecte (principe 4 de la *LPRPDÉ*)

Critères :

Les organisations ne doivent pas recueillir des renseignements personnels de façon arbitraire. Elles doivent 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 (principe 8 – *LPRPDÉ*), les organisations doivent préciser la nature des renseignements recueillis comme partie intégrante de leurs politiques et pratiques de traitement des renseignements personnels.

L'exigence selon laquelle les organisations sont tenues de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis. Cette obligation suppose que le consentement à la collecte de renseignements ne doit pas être obtenu par subterfuge.

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 gouvernementales doivent prendre toutes les mesures raisonnables pour que les renseignements personnels utilisés à des fins administratives soient aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés. (Voir également la rubrique Exactitude (principe 6 de la *LPRPDÉ*) ci-dessous).

À défaut du consentement de la personne concernée, l'institution gouvernementale doit utiliser

des renseignements personnels uniquement 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 de banque 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*.

(Voir aussi la rubrique Limitation de l'utilisation, de la communication et de la conservation (principe 5 de la *LPRPDÉ*)

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

Critères :

Les institutions gouvernementales doivent s'assurer que leurs programmes de couplage de données sont conçus et réalisés conformément aux principes des pratiques équitables de traitement des renseignements énoncés dans la *Loi sur la protection des renseignements personnels* et à la Politique du Conseil du Trésor sur le couplage de données.

Limitation de l'utilisation, de la communication et de la conservation des renseignements personnels (principe 5 de la *LPRPDÉ*)

Critères :

Les renseignements personnels ne doivent pas être utilisés à d'autres fins 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 ayant servi 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.

Les renseignements dont on n'a plus besoin aux fins précisées doivent être détruits, effacés ou dépersonnalisées.

Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

Exactitude (principe 6 de la *LPRPDÉ*)

Critères :

Les renseignements personnels doivent être suffisamment exacts, complets et à jour afin de 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 ce ne soit nécessaire pour atteindre les fins auxquelles ils ont été recueillis.

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

Critères :

Les renseignements personnels qui relèvent d'une institution gouvernementale 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*.

L'alinéa 8(2)*f*) de la *Loi sur la protection des renseignements personnels* autorise une institution gouvernementale (fédérale) à communiquer des renseignements personnels au gouvernement d'un pays étranger, à une organisation internationale d'états ou de gouvernements ou à toute institution d'un tel gouvernement pour l'application des lois ou pour la tenue d'enquêtes licites.

De telles communications doivent être régies par un accord écrit entre les parties..

Communication – Ententes d'échange de renseignements personnels (critères élaborées à partir de diverses sources)

Critères et considérations :

1. Parties à l'entente
Est-ce que l'entente : a) identifie clairement les organismes publics, les niveaux de gouvernement ou d'autres organisations qui participent à cet échange de renseignements personnels? b) nomme tous les entrepreneurs ou fournisseurs de services qui ont accès aux renseignements personnels?

2. Autorisation

Est-ce que l'entente :

a) définit l'autorisation légale – la Loi, l'accord ou le traité qui permet aux parties de conclure une entente pour la mise en commun ou l'échange de renseignements personnels?
b) définit l'autorisation légale qui régit les différents programmes ou activités des parties de cette entente?

3. Objet de l'entente

Est-ce que l'entente :

a) définit l'objet général de l'échange de renseignements?
b) indique si l'échange de renseignements personnels sera à sens unique ou réciproque?
c) décrit, pour chacun des objets ou des motifs énoncés dans l'entente, les éléments de données ou renseignements personnels à mettre en commun ou à échanger?
d) établit la différence entre les éléments de données échangés dans une entente réciproque – les parties utilisent-elles différents éléments de données?
e) indique si des identificateurs de clients communs sont utilisés et, dans l'affirmative, en quoi ils consistent? identifie les sources de renseignements personnels?

4. Responsabilisation

Est-ce que l'entente :

a) précise les responsabilités de chacune des parties quant au respect des modalités de l'entente et désigne une personne responsable pour chacune des parties?
b) indique clairement qui a le contrôle légal des renseignements personnels échangés?
c) indique si les parties utilisent des pratiques et des procédures communes pour se conformer aux différentes parties de l'entente?
d) explique que chacune des parties aura la responsabilité de répondre aux demandes de consultation ou de correction des renseignements personnels dont elles disposent?
e) précise que chaque partie sera responsable des gestes de ses employés, agents ou entrepreneurs quant à l'utilisation, à la communication et à la destruction des renseignements personnels assujettis à l'entente et aux lois en matière de protection de la vie privée qui s'appliquent?
f) indique si les renseignements personnels échangés sont assujettis à d'autres lois, règlements ou lignes directrices en matière d'accès à l'information et de protection des renseignements personnels en plus de celles que doit respecter le fournisseur des renseignements? (Remarque : aux États-Unis, les lois en matière de protection de la vie privée s'appliquent habituellement aux citoyens et aux résidents permanents seulement.)

5. Mécanisme de mise en commun ou d'échange de renseignements personnels

Est-ce que l'entente décrit :

a) les méthodes ou les procédures qui seront utilisées pour échanger des renseignements personnels?
b) le niveau du droit d'accès aux renseignements personnels des différentes parties, en fonction du principe de la nécessité d'accès?

6. Obtention du consentement ou notification de toute partie visée

L'entente comporte-t-elle une disposition :

a) établissant dans quelle mesure (le cas échéant) les personnes auxquelles se rapportent les renseignements ont été avisées de l'échange?

b) faisant mention des exceptions à la règle du consentement?

7. Utilisation des renseignements personnels

Est-ce que l'entente :

a) indique clairement les utilisations qui seront faites des renseignements personnels échangés conformément à l'entente?
b) prévoit des limites ou des interdictions à l'usage secondaire des renseignements à d'autres fins que celles qui sont listées dans l'entente?

8. Communication à des tiers (y compris des entrepreneurs et des sous-traitants)

Est-ce que l'entente :

a) donne une liste des tiers à qui des renseignements personnels peuvent être communiqués ou donne des catégories de tiers?
b) définit clairement les fins et les circonstances dans lesquelles des renseignements personnels peuvent être communiqués à des tiers, ainsi que les procédures à suivre pour de telles communications?
c) autorise la communication de renseignements personnels à d'autres fins que celles qui sont précisées (p. ex., à des fins de recherche et de statistiques, ou encore à des fins de planification de programmes, de prévisions ou d'évaluation)?
d) précise que les modalités de l'entente s'appliquent à toute communication à un tiers, notamment l'exigence pour les tiers de se conformer aux principes équitables de traitement de l'information afin de protéger les renseignements personnels?

9. Exactitude

Est-ce que l'entente :

a) indique les mesures qui seront prises pour garantir que les renseignements personnels sont exacts, complets et à jour?
b) comporte une clause relative au traitement des demandes de correction?
c) précise en quoi consiste la demande de correction doit être communiquée aux parties qui obtiendront les renseignements?
d) renferme une clause selon laquelle les parties doivent vérifier les renseignements personnels auprès de l'organisme qui les a fournis avant de les utiliser pour prendre des décisions sur une personne?

10. Sécurité

Est-ce que l'entente :

a) comporte les garanties et les contrôles essentiels pour les différentes fonctions - administratives, personnelles, techniques, des TI et physiques - qui vont permettre d'assurer la sécurité des renseignements personnels échangés (p. ex., mesures de sécurité pour la transmission des renseignements personnels et mesures visant à prévenir l'accès, l'utilisation ou la communication non autorisé)?
b) nécessite une évaluation de la menace et des risques (EMR), y compris une évaluation des risques pour les renseignements personnels des citoyens qui pourraient résulter de l'entente?

11. Conservation et destruction

Est-ce que l'entente :

a) précise la durée de la période de conservation des renseignements personnels échangés et indique si les renseignements doivent être retournés à l'expéditeur ou détruits par les destinataires selon des procédures sécurisées?
b) indique ce qu'on fera des renseignements personnels échangés lorsque l'entente arrivera à échéance?

12. Couplage de données

L'entente prévoit-elle un couplage des données ou des activités d'établissement de profils par l'une ou l'autre des parties suite à l'échange des renseignements personnels?
(Remarque : voir la *Politique du Conseil du Trésor sur le couplage de données*)

13. Évaluation des facteurs de risque relatifs à la vie privée

L'entente sur l'échange de renseignements définit-elle un type d'entente nouveau ou différent pour l'échange de renseignements personnels qui justifierait une évaluation des facteurs relatifs à la vie privée selon la politique du Conseil du Trésor?

14. Utilisation ou communication non autorisée

Est-ce que l'entente :

a) établit des procédures de notification en cas d'utilisation ou de communication non autorisée des renseignements échangés?
b) prévoit que la partie responsable de l'infraction devrait immédiatement en informer l'autre partie?
c) précise les conséquences de l'utilisation ou de la communication non autorisée des renseignements personnels échangés?

15. Différends

L'entente expose-t-elle un processus à suivre pour régler les différends relatifs à l'entente?

16. Vérifications

Est-ce que l'entente :

a) comprend une clause permettant des vérifications périodiques des méthodes d'échange afin de garantir la conformité aux modalités de l'entente?
b) exige que les résultats de telles vérifications soient communiqués à l'autre partie?
c) précise que des outils et méthodes d'établissement de pistes de vérification seront utilisés pour faire le suivi des modifications, consultations et communications des données?
d) mentionne le droit de la commissaire à la protection de la vie privée d'accéder aux renseignements détenus par des institutions gouvernementales fédérales à des fins d'enquêtes et de vérification en vertu de la *Loi sur la protection des renseignements personnels*?
   Remarque : d'autres entités peuvent avoir des compétences légales similaires.

17. Modification/Renouvellement et annulation

Est-ce que l'entente :

a) prévoit que les modifications et les renouvellements doivent se faire par écrit et avec l'accord de toutes les parties?
b) peut être annulée par l'une ou l'autre des parties?

18. Changements ayant une incidence sur l'entente

Est-ce que l'entente :

a) prévoit que les parties doivent fournir une notification écrite de tout changement législatif, régulatoire ou stratégique qui a une incidence sur ses modalités?

19. Délai

L'entente prévoit-elle un délai?

a) pour sa durée?
b) pour l'examen par les parties?

20. Définitions

L'entente comporte-t-elle des définitions d'expressions qui pourraient être uniques à l'entente?

21. Pouvoir de signature et personnes-ressources

Est-ce que l'entente :

a) doit absolument être signée par les « dirigeants » des organismes publics (ou par les responsables à qui on a délégué la responsabilité de signer de telles ententes) et par d'autres responsables à des niveaux équivalents d'autres organisations?

b) renferme les noms, titres, adresses et numéros de téléphone des responsables de chaque partie chargés d'administrer les différents aspects de l'entente?

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

Critères :

Les renseignements personnels qui sont recueillis, utilisés, communiqués, conservés ou détruits pour le compte d'une institution gouvernementale, ou dans le cadre d'un contrat avec une institution gouvernementale, doivent être gérés conformément aux principes du traitement équitable 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 gouvernementale, le contrat doit préciser que les renseignements personnels sont réputés être sous le contrôle de l'institution gouvernementale 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 manipuler 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.

(Pour plus de précisions sur les critères, voir la liste de vérification ci-dessus pour les ententes d'échange de renseignements personnels.)

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

Critères :

Les institutions gouvernementales doivent mettre en place les 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 l'utilisation, à la communication, à la modification ou à la destruction non autorisée.

Courriels et télécopies :

> 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 exploités, ou encore reçus par erreur par une personne qui n'est pas autorisée à recevoir des données. 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 (p. ex. message crypté, télécopieur sécuritaire) et qu'il se trouve dans un endroit protégé.

Les institutions gouvernementales doivent donc mettre en place des mesures de sécurité qui vont garantir la confidentialité des renseignements personnels transmis par voie électronique.

Mesures de sécurité (principe 7 de la *LPRPDÉ*)

Critères :

Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol, ainsi que contre l'accès, la communication, la reproduction, l'utilisation ou la modification non autorisé.

Les organisations doivent protéger les renseignements personnels, peu importe la forme sous laquelle ils sont conservés.

Remarque : La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la répartition et du format des renseignements, ainsi que des méthodes de conservation.

Un niveau de protection plus élevé doit être prévu pour les renseignements de nature plus délicate.

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 de sécurité et un accès sélectif en fonction de la nécessité d'accès; des mesures techniques, par exemple, l'usage de mots de passe et du chiffrement.

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.

Conservation et destruction des renseignements personnels (paragraphes 4(1) et (2) et paragraphe 6(1) de la *Loi sur la protection des renseignements personnels*)

Critères :

Les renseignements doivent être conservés et détruits selon les calendriers de conservation et de destruction approuvés.

À moins que la loi ne le prévoie autrement, ou qu'une personne n'aie déjà donné son consentement, les renseignements personnels ayant servi à rendre une décision qui touche directement cette personne doivent être conservés pendant au moins deux ans à compter de la date à laquelle ils ont été utilisés pour la dernière fois.

Les dossiers doivent être disposé ou détruits selon la classification de leur sécurité.

Accès aux renseignements personnels (principe 9 de la *LPRPDÉ*)

Critères :

Une organisation doit, sur demande, indiquer à une personne si elle détient des renseignements personnels la concernant. Les organisations sont invitées à fournir la source de l'information.

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 le faire de la façon 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 (entrepreneur), l'organisation doit s'assurer d'obtenir du tiers des copies des documents relatifs à la demande d'accès pour examen et communication à la personne concernée.

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 à un coût minime ou gratuitement. 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 prouve que des renseignements personnels sont inexacts ou incomplets, l'organisation doit apporter les modifications nécessaires à ces renseignements. Les modifications peuvent exigées des corrections ou le retrait d'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.

Possibilité de porter plainte suite au non-respect des principes (principe 10 de la *LPRPDÉ*)

Critères :

Toute personne doit pouvoir déposer une plainte pour non-respect des principes énoncés ci-dessus en communiquant avec la ou les personnes chargées de faire respecter ces principes au sein de l'organisation concernée.

Les organisations doivent mettre en place des procédures pour recevoir et traiter les plaintes et les demandes de renseignements concernant leurs politiques et leurs pratiques de gestion des renseignements et y donner suite. Les procédures relatives aux plaintes devraient être

facilement accessibles et simples à appliquer.

Les organisations doivent informer les personnes qui présentent une demande de renseignements ou déposent une plainte de l'existence de procédures pertinentes (y compris le droit de déposer une plainte auprès du Commissariat à la protection de la vie privée).

Une organisation doit faire enquête sur toutes les plaintes. Si une plainte est jugée fondée, l'organisation doit prendre les mesures appropriées, y compris (au besoin) la modification de ses politiques et de ses pratiques.

AUTRES CRITÈRES DE VÉRIFICATION

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

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 Loi qu'ont les personnes chargées de l'administrer pour le compte de l'institution et, dans une moindre mesure, des employés de l'institution.

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 de renseignements personnels.

L'institution gouvernementale 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.

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

Critères :

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.

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

ANNEXE C

LISTE D'ACRONYMES	
ACRONYME	**NOM**
AAMD	Accord d'assistance mutuelle en matière douanière
AC	Administration centrale
ACIA	Agence canadienne d'inspection des aliments
ADRC	Agences des douanes et du revenu du Canada
ANRR	Analyste régional du renseignement
ARR	Agent régional du renseignement
CER	Composante d'évaluation des risques
CIC	Citoyenneté et Immigration Canada
CNER	Centre national d'évaluation des risques
CPVP	Chef de la protection de la vie privée
CRG	Composante de requête globale
CVDS	Cycle de vie de développement de systèmes
DN	Date de naissance
EFVP	Évaluation des facteurs relatifs à la vie privée
ÉMR	Évaluation de la menace et des risques
EXPRES	Programme d'expéditions rapides et sécuritaires
GRUP	(Système de) gestion du risque lié aux utilisateurs privilégiés
ID	Identification
IPV	Information préalable sur les voyageurs
IIVRE	Initiative d'identification des voyageurs à risque élevé
LIPI	Ligne d'inspection primaire intégrée
LPRPDÉ	*Loi sur la protection des renseignements personnels et les documents électroniques*
PE	Protocole d'entente
RIS	Rapport d'incident relatif à la sécurité
SAD	Système d'acquisition de données
SASLIP	Système automatisé de surveillance à la ligne d'inspection primaire
SCD	Système de contrôle des départs
SCT	Secrétariat du Conseil du Trésor
SGIED	Système de gestion de l'information des enquêtes des douanes
SGR	Système de gestion du renseignement
SIED	Système intégré d'exécution des douanes
SRTA	Système de réservation des transporteurs aériens
SRE	Système de rapport des événements
SSOBL	Système de soutien des opérations des bureaux locaux
TEJ	Traité d'entraide juridique
TI	Technologie de l'information
UE	Union européenne
UCP	Unité de ciblage des passagers
U.S. CBP	United States Customs & Border Protection Agency
U.S. NTC	United States National Targeting Centre
U.S. DHS	United States Department of Homeland Security
U.S. TECS	United States Treasury Enforcement Communications System
ZLA	Zone de lecture automatique