Vérification intégrée de la sécurité de la technologie de l'information à DRHC (DSC et RHDCC)

Rapport final
Projet n° 6577/04

Direction de la vérification et de l'évaluation
Politique et orientation stratégique
Développement social Canada

Équipe de projet :

Directeur général :	*J. Blain*
Directeur de vérification, TI :	*P. LePage*
Gestionnaire de vérification, TI :	*M. Winterburn*
Membres de l'équipe, TI :	*K. Allen*
	F-M. Brière
Consultants, TI :	*Centre de la sécurité des télécommunication (CST)*
	Electronic Warfare Associates (EWA)

octobre 2004

SDC-A-003-10-04F
(also available in English)

Dénégation générale de responsabilité
Veuillez noter que l'information qui serait habituellement retenue en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* ne figure pas dans le rapport suivant.

Papier
ISBN : 0-662-74298-2
Nº de cat. : SD34-7/2005F

PDF
ISBN : 0-662-74299-0
Nº de cat. : SD34-7/2005F-PDF

HTML
ISBN : 0-662-74300-8
Nº de cat. : SD34-7/2005F-HTML

Table des matières

Sommaire

L'évaluation intégrée de la sécurité de la technologie de l'information (STI) de DRHC (DSC et RHDCC) a été menée en trois étapes ou phases. Ses objectifs, qui avaient été approuvés par le Comité de vérification et d'évaluation (CVE) de DRHC, consistaient à fournir à la haute direction du ministère une évaluation des éléments suivants :

1) le cadre de régie de la STI;
2) les vulnérabilités internes de la STI : évaluation sur place de la vulnérabilité technique (EPVT);
3) les vulnérabilités externes de la STI : vérification de la sécurité des réseaux actifs (VSRA).

La STI peut se décrire brièvement comme la structure de contrôle établie pour gérer l'intégrité, la confidentialité et la disponibilité des données et des ressources de la TI. Cette structure de contrôle doit s'appuyer sur un cadre de gestion et une structure de régie appropriés, que vient compléter une protection technologique adéquate. Puisque les attaques livrées contre les systèmes informatiques sont de plus en plus sophistiquées, il est quasiment impossible pour un grand service de TI, quel qu'il soit, d'être complètement immunisé en tout temps contre les attaques et leurs conséquences possibles, et DRHC ne fait pas exception à la règle. Néanmoins, consciente de sa responsabilité de protéger les renseignements confidentiels et personnels que détient le ministère au sujet de ses clients, la haute direction de DRHC a autorisé la tenue de cette vérification, qui lui permettra de déterminer les zones sensibles de la STI à laquelle elle pourrait apporter des améliorations.

La vérification a permis de relever un certain nombre d'éléments positifs qui caractérisent l'environnement de la STI à DRHC, mais également des éléments susceptibles d'être améliorés. Heureusement, la plupart des améliorations à apporter à la STI relèvent de la compétence de DRHC, qui a simplement besoin de « peaufiner » les mesures déjà en place.

Dans le cadre de l'évaluation de la phase I (ayant porté sur le cadre de régie de la STI), qui s'est déroulée principalement entre octobre 2003 et mars 2004, la Direction de la vérification et de l'évaluation (DVE) a examiné les contrôles en matière de gestion et de personnel ainsi que les contrôles opérationnels et techniques qui caractérisent la STI à DRHC par rapport au cadre ministériel de régie de la STI. De plus, les progrès réalisés par DRHC pour régler les problèmes signalés à la suite de deux vérifications précédentes (Bureau de la vérificatrice générale, avril 2002, et Vérification interne de DRHC, septembre 1999) ont aussi été examinés.

La phase I a permis de conclure que la plupart des éléments nécessaires à un cadre de régie de la STI existaient à DRHC, notamment :

- un protocole d'entente entre l'agent de sécurité du ministère et la Direction des systèmes, qui définit les responsabilités de chaque partie en matière de STI;
- un comité de régie de la STI;
- un modèle de STI ministériel selon lequel les problèmes reliés à la STI sont traités tout au long de la phase initiale et de la phase subséquente du cycle de vie des projets;
- les autorisations de sécurité appropriées pour les administrateurs des réseaux locaux (RL);
- des copies de sauvegarde des données qui sont faites régulièrement;
- une confirmation indépendante attestant que DRHC a donné suite de façon appropriée aux problèmes relevés à la suite de la vérification de la STI, effectuée par le BVG en 2002.

Au nombre des améliorations à apporter, mentionnons la nécessité d'établir la version définitive d'un programme de sensibilisation à la STI au sein de DRHC, de le mettre en œuvre et de le tenir à jour. Pour ce qui est de l'aspect non technique de la STI, un solide programme de sensibilisation est souvent considéré comme le fondement le plus important sur lequel repose un programme de STI efficace; la STI est la responsabilité de tous. Au moment où la présente vérification était en cours, des plans de poursuite des activités n'avaient pas été établis pour quelques programmes essentiels à la mission. DRHC doit également passer en revue la façon dont les mots de passe sont utilisés pour accéder à ses systèmes, et plus particulièrement le nombre de mots de passe qui existent, les politiques qui les régissent et les solutions techniques qui faciliteraient la vie des membres du personnel qui doivent mémoriser de multiples mots de passe pour différents systèmes.

Dans le cadre de la phase II (EPVT) et de la phase III (VSRA), la DVE a collaboré avec le Centre de la sécurité des télécommunications (CST) pour faire une évaluation de la posture de DRHC en matière de sécurité (EPS), afin de déterminer quels systèmes et quelles vulnérabilités du réseau pourraient être exploités. DRHC et le CST ont conclu un protocole d'entente régissant la réalisation des essais techniques. Outre ce protocole, une autorisation ministérielle a également été obtenue pour la réalisation de l'EPS.

Au cours de la phase II, la DVE et le CST ont fait une évaluation de la vulnérabilité interne des systèmes de DRHC pour en déterminer les points faibles. Les résultats ont permis de constater que les mesures de sécurité en ce qui a trait aux défenses périmétriques du ministère sont susceptibles d'être améliorées. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] Il n'existe aucun processus global de gestion de la configuration, de sorte que les configurations ne sont pas uniformes entre les régions. La plus grande partie du trafic interne passe par [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.].

Lors de la phase III, la DVE et le CST ont fait une évaluation de la vulnérabilité externe des systèmes de DRHC en vue de déterminer la vulnérabilité des réseaux périmétriques de DRHC face à des attaques électroniques. Les tests qui ont été menés simulaient des attaques du genre de celles auxquelles on peut s'attendre d'un agent de menace (à savoir un « pirate informatique ») qui aurait ciblé les réseaux de DRHC. Les résultats ont révélé que les défenses périmétriques des systèmes de DRHC sont suffisamment solides. Toutefois, d'autres moyens d'exploiter les points sensibles de certains systèmes de DRHC ont été découverts, portant ainsi atteinte à l'intégrité du réseau interne de DRHC. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] L'évaluation permet donc de conclure que la posture de DRHC en matière de sécurité est susceptible d'être améliorée.

En conclusion, compte tenu de la complexité et de la fréquence accrues des attaques dont font l'objet les systèmes informatiques, il faut s'attendre à ce que, dans un environnement de TI aussi vaste et aussi diversifié que celui de DRHC, certains éléments doivent être améliorés pour renforcer la STI. La vérification, qui bénéficiait du soutien de la direction, a été réalisée en vue de repérer ces éléments, qu'il revient maintenant à DRHC de classer par ordre de priorité et d'améliorer. Les constatations tirées de l'évaluation et les recommandations qui en découlent ne peuvent garantir qu'aucune personne ni entité non autorisée n'accédera jamais aux systèmes et aux réseaux de DRHC, mais elles devraient aider le ministère à élaborer une stratégie globale d'atténuation du risque en matière de STI et d'améliorer son environnement de STI.

1.0 Introduction

1.1 Contexte

Note : Une fois la vérification amorcée, DRHC a été scindé en deux ministères, soit DSC et RHDCC, le 12 décembre 2003. Ainsi, lorsqu'il est question de DRHC dans le présent rapport, l'information se rapporte à la fois à DSC et à RHDCC.

La vérification intégrée de la sécurité de la technologie de l'information (STI) à DRHC (DSC et RHDCC), qui s'est déroulée en trois phases, avait pour objet de fournir à la haute direction du ministère une évaluation indépendante relative à trois éléments :

1) le cadre de régie de la STI;
2) les vulnérabilités internes de la STI : évaluation sur place de la vulnérabilité technique (EPVT);
3) les vulnérabilités externes de la STI : vérification de la sécurité des réseaux actifs (VSRA).

Les objectifs, la portée, les normes et la méthodologie de l'évaluation, qui ont été approuvés par le Comité de vérification et d'évaluation (CVE) de DRHC, se trouvent à l'annexe A.

La STI peut se décrire brièvement comme la structure de contrôle établie pour gérer l'intégrité, la confidentialité et la disponibilité des données et des ressources de la TI. Cette structure de contrôle doit s'appuyer sur un cadre de gestion et une structure de régie. Au cours de la phase I, les contrôles en matière de gestion et de personnel ainsi que les contrôles opérationnels et techniques de la STI à DRHC ont été examinés par rapport au cadre ministériel de régie de la STI.

Dans le contexte de ces contrôles, un suivi des problèmes signalés à la suite de deux vérifications précédentes de la STI a également été effectué. En septembre 1999, la Vérification interne de DRHC a fait une évaluation de la STI au ministère. Selon ses constatations, DRHC avait besoin de rationaliser sa structure et ses processus organisationnels de manière à gérer la STI à tous les niveaux, et d'accroître les connaissances de tout son personnel en matière de STI tout en le sensibilisant davantage à cet égard. En avril 2002, à l'issue d'une vérification de la STI qui visait notamment DRHC, le Bureau de la vérificatrice générale (BVG) a présenté des conclusions semblables, en précisant qu'aux termes de la Politique du gouvernement sur la sécurité, un rapport sur l'efficacité de la STI à l'échelle du gouvernement devait être déposé au plus tard en 2004. La vérification qui fait l'objet du présent rapport aidera le ministère à satisfaire à cette exigence. Enfin, la phase I a donné lieu au recensement de systèmes de DRHC (p. ex., les adresses IP), qui allaient être utilisés pour les besoins des tests techniques des phases II et III. Pendant la phase II (EPVT), nous avons fait une évaluation de la vulnérabilité interne des systèmes de DRHC pour déterminer les points faibles des systèmes et des ressources d'information du ministère. Au cours de la phase III (VSRA), nous avons fait une évaluation de la vulnérabilité externe des systèmes du ministère, de manière à déterminer la vulnérabilité de ses réseaux périmétriques face à des attaques électroniques.

Pour se préparer à cette vérification, la Direction de la vérification et de l'évaluation (DVE) de DSC a consulté des représentants :

- des Services de vérification de la TI au BVG;
- des Services des opérations gouvernementales au Secrétariat du Conseil du Trésor (SCT);
- du Bureau du dirigeant principal de l'information au SCT;
- de la Direction de la sécurité technique à la Gendarmerie royale du Canada (GRC);
- du Centre de la sécurité des télécommunications (CST), qui a fait équipe avec la DVE pour mener les tests techniques au cours des phases II et III.

Le travail sur le terrain s'est déroulé d'octobre 2003 à mars 2004 pour la phase I; du 2 au 16 février 2004 pour la phase II; et de mars à septembre 2004 pour la phase III.

2.0 Constatations de la phase I — cadre de régie de la STI

2.1 Contrôles de gestion

2.1.1 La structure de gestion de la STI a été documentée et intégrée aux programmes de DRHC, et elle est appuyée à tous les niveaux de la gestion

Conformément à la Politique du gouvernement sur la sécurité établie par le Secrétariat du Conseil du Trésor, DRHC a désigné, au sein de la Direction générale des finances et de l'administration (DGFA), un agent de sécurité du ministère chargé de mettre sur pied et de diriger un programme de sécurité qui englobe la STI. Toutefois, étant donné la nature technique de la STI, un protocole d'entente a été conclu entre la DGFA et la Direction générale des systèmes en vertu duquel c'est le SMA, Systèmes, qui assume la responsabilité de la STI.

Au sein de la Direction générale des systèmes, les responsabilités en matière de STI reviennent aux quatre directions des Systèmes :

- Politiques, gestion stratégique et planification (p. ex., politiques, procédures);
- Services de technologie (p. ex., processus, régie, ingénierie de la sécurité);
- Opérations de TI (p. ex., centres informatiques — ordinateurs centraux, serveurs);
- Solutions aux clients (p. ex., élaboration/normes de logiciels).

D'autres directions générales du ministère (p. ex., Assurance-emploi, Programmes de la sécurité du revenu) ont pris une part active à la détermination des besoins en matière de sécurité par le biais d'évaluations des facteurs relatifs à la vie privée, d'évaluations de la menace et des risques et de la mise à jour des profils d'accès aux systèmes qui permettent de lier les fonctions d'un poste à l'accès à l'information appropriée.

Les bureaux régionaux et les bureaux locaux du ministère ont des responsabilités en matière de sécurité physique et de sécurité de la TI dans leurs propres services, responsabilités qui relèvent des agents régionaux de sécurité, du personnel des réseaux locaux et des gestionnaires de programme.

Même si le ministère a documenté et intégré adéquatement sa structure de gestion de la STI et qu'il lui accorde le soutien voulu, certains problèmes ont été relevés.

Le comité directeur du cadre de gestion de la protection des renseignements personnels (CDCGPRP) de DRHC, qui a des pouvoirs décisionnels, est chargé d'examiner les enjeux de la protection des renseignements personnels. Selon les procès-verbaux de

récentes réunions, le mandat du CDCGPRP fait l'objet d'un examen à l'issue duquel des responsabilités en matière de sécurité y seront intégrées, mais aucune décision n'a encore été prise.

Nous n'avons trouvé aucun comité décisionnaire équivalent pour les enjeux de la STI, mais il existe un comité de gestion de la sécurité de la technologie de l'information (CGSTI). Ce comité consultatif sur la STI a tenu sa première réunion le 27 octobre 2003, mais aucun compte rendu de cette première rencontre n'a encore été publié. Le CGSTI a tenu une deuxième réunion le 27 juillet 2004.

Même s'il est fait mention de la STI dans les plans ministériels, les plans des Systèmes et les plans régionaux, nous n'avons trouvé aucun énoncé officiel de stratégie/de vision en matière de STI au ministère dont ces plans émaneraient ou qu'ils auraient pour objet de concrétiser.

Recommandation n° 1 : Il est recommandé que le nom et le mandat du comité directeur du cadre de gestion de la protection des renseignements personnels soient élargis pour englober la sécurité.

Recommandation n° 2 : Il est recommandé que le comité de gestion de la sécurité de la technologie de l'information :

a) produise un énoncé de stratégie/de vision en matière de STI approuvé par le ministère;
b) rédige des procès-verbaux et des comptes rendus de décisions;
c) se réunisse tous les trois mois;
d) relève du comité directeur du cadre de gestion de la protection des renseignements personnels.

2.1.2 Des politiques et procédures pratiques et utiles relatives à la STI ont été diffusées rapidement aux utilisateurs concernés

Les politiques et procédures en matière de STI se trouvent dans le réseau intranet du ministère. Différents auteurs, dont les Systèmes, la DGFA, etc., y ont contribué, et elles sont appuyées et communiquées aux intéressés par la haute direction. Par exemple, les Systèmes établissent les politiques et les règles concernant les coupe-feu, tandis que la DGFA élabore les politiques et procédures du ministère en matière de STI pour l'utilisation d'Internet et du système de courrier électronique.

Il est vrai que le ministère a diffusé rapidement aux intéressés les politiques et procédures relatives à la STI, mais certaines améliorations pourraient être apportées pour régler les problèmes énumérés ci-après.

Certaines régions ne savaient pas au juste de qui relèvent l'établissement et l'autorisation de la politique en matière de STI. Selon le protocole conclu entre les Systèmes et la DGFA, ce sont les Systèmes (c.-à-d. Politiques, gestion stratégique et planification) qui ont la responsabilité des politiques relatives à la STI. Sur le site Web des Services de

sécurité de la technologie informatique (SSTI), sous la rubrique de la politique, des processus et de la régie, on constate que les responsabilités des SSTI comprennent l'établissement des politiques, des normes et des lignes directrices pertinentes, mais non pas leur approbation. Le CGSTI ne peut pas approuver les politiques relatives à la STI puisque c'est un comité consultatif.

Il existe bel et bien des politiques en matière de STI, mais notre examen a révélé qu'elles n'avaient pas été approuvées par la haute direction. De plus, sur les 30 politiques et procédures en matière de STI qui ont été recensées dans les sites Web des Systèmes et d'autres sites, six étaient à l'état d'« ÉBAUCHE », une remontait à 1999, une autre à 2000, deux à 2001, et deux autres n'étaient pas datées.

Recommandation n° 3 : Il est recommandé :

a) que le ministère confie à une entité de régie appropriée (p. ex., le CGSTI, le CDCGPRP, etc.) la responsabilité d'approuver les politiques en matière de STI;
b) que les Systèmes présentent les « ÉBAUCHES » des politiques en matière de STI à cette entité de régie pour approbation.

Les régions demandent des procédures/lignes directrices nationales en matière de STI pour régler des problèmes/questions qui, selon elles, sont encore en suspens, notamment des politiques sur l'accès, la mobilité, etc. Comme des politiques de ce genre n'ont pas encore été approuvées à l'échelle nationale, certaines régions ont adopté leurs propres politiques, ce qui peut entraîner des incohérences entre les régions. Nous avons, au même titre que le Centre de la sécurité des télécommunications qui a fait équipe avec nous pour les tests techniques des phases II et III de la vérification, relevé des différences entre les régions au chapitre de la configuration des ordinateurs de bureau, des systèmes de réseaux locaux (RL) et des serveurs.

Recommandation n° 4 : Il est recommandé que les Systèmes, en collaboration avec les régions, déterminent les besoins en matière de politiques et procédures de STI et élaborent des politiques et procédures nationales en conséquence.

2.1.3 La gestion des risques est un processus officiel de gestion, qui a été intégré aux méthodes de gestion des Systèmes et qui englobe la STI

Les Systèmes ont tenu des séances de gestion des risques en 2003. Il en est ressorti que la sécurité/la protection des renseignements personnels présentaient des risques élevés. Des profils ont été établis pour la DG des Systèmes, parallèlement à des stratégies d'atténuation des risques qui font l'objet d'un suivi.

Les quatre Centres de technologie de l'information (CTI) du ministère ont récemment mené des évaluations de la menace et des risques. Parallèlement à ces évaluations, des séances formelles de gestion des risques ont été organisées par les Systèmes. Comme on l'a vu précédemment, différentes DG du ministère (Assurance-emploi, Programmes de la sécurité du revenu, etc.) s'emploient à déterminer les risques en matière de STI en faisant des évaluations des facteurs relatifs à la vie privée et des évaluations de la menace et des risques.

Certaines des régions que nous avons visitées ont adopté des processus de gestion des risques, qui ont par la suite été intégrés à leur exercice de planification opérationnelle. Ces processus comprennent des plans d'action fondés sur le principe voulant que la STI représente un risque important.

2.1.4 Des vérifications et des examens officiels portant sur la STI ont été effectués, et leurs conclusions se retrouvent dans des plans d'action

Des vérifications et des examens officiels portant sur la STI ont été réalisés, et des plans d'action connexes ont été établis. Ces vérifications et ces examens ont été menés par la Vérification interne du ministère, les SSTI des Systèmes, les Opérations des CTI ainsi que le Bureau de la vérificatrice générale. Le Secrétariat du Conseil du Trésor et le Bureau de la vérificatrice générale reçoivent les rapports de vérification qui concernent la STI à l'interne, car ils font tous deux partie du Comité de vérification et d'évaluation, l'entité du ministère à qui sont présentés les rapports de vérification et d'examen.

2.2 Contrôles opérationnels

2.2.1 Les politiques et procédures relatives à la STI décrivent les rôles et responsabilités de DRHC à cet égard, ainsi que les services qui s'y rattachent

Les politiques et procédures relatives à la STI définissent les rôles et responsabilités par l'entremise d'éléments comme le protocole conclu entre la DGFA et les Systèmes, les descriptions de travail des administrateurs des RL au ministère (à l'échelle nationale, régionale et locale) et les postes d'agent de liaison régional pour la sécurité de la technologie de l'information. Les politiques et procédures en matière de STI décrivent également un grand nombre d'autres composantes comme la politique du ministère en matière de coupe-feu [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], les lignes directrices de la TI pour le regroupement des services de sécurité et de protection des renseignements personnels, les exigences en matière de mots de passe ainsi que les accords sur les niveaux de service (région de l'Ontario).

2.2.2 Les rôles et responsabilités ainsi que les services en matière de STI ont été confiés à des personnes et à des groupes compétents; toutefois, ceux-ci ne disposent pas toujours des ressources nécessaires à l'exécution de leur mandat

Nous nous sommes assurés que les rôles et responsabilités en matière de STI, qui sont énumérés ci-dessous, ont été confiés à des personnes et à des groupes compétents :

i) la formation et la sensibilisation en matière de STI;
ii) la détermination des biens liés à la TI;
iii) les enquêtes de sécurité (y compris pour les contrats);
iv) la sécurité physique et la protection des employés;
v) la planification de la continuité/de la reprise des opérations;
vi) les enquêtes sur les incidents relatifs à la sécurité.

Nous nous sommes également assurés que les rôles et responsabilités en matière de STI sont exposés clairement en ce qui a trait :

i) aux fonctions relatives à la STI de l'agent de sécurité du ministère;
ii) aux fonctions des Systèmes en matière de STI;
iii) aux exploitants des systèmes (p. ex., l'Assurance-emploi, les Programmes de la sécurité du revenu, etc.);
iv) au personnel à l'échelle nationale, régionale et locale.

Les représentants nationaux et régionaux de la STI à qui nous avons parlé se sont dits généralement satisfaits des ressources dont ils disposent pour remplir leur mandat.

Nous avons toutefois observé que le groupe responsable du contrôle de la protection de l'information (CPI) au ministère faisait exception. Ce groupe a été récemment mis sur pied pour détecter les problèmes relatifs à la STI, les régler et faire rapport à leur sujet, y compris au sujet de virus comme Nachi et Blaster qui ont « infecté » le ministère. À notre avis, le groupe CPI a un rôle essentiel à jouer, mais il ne dispose pas encore d'un plan faisant état des ressources dont il a besoin pour remplir son mandat.

Les moyens de gérer les infections causées par ce type de virus sont à la fois de nature préventive et de nature réactive. Parmi les mesures préventives, on retrouve des logiciels [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], qui font en sorte que les anti-virus sont toujours activés et qui confirment que les configurations sont protégées (c.-à-d. que les ports vulnérables sont fermés). Toutefois, lorsque de nouveaux virus (p. ex. Sasser) réussissent à « infecter » le ministère, il faut recourir à d'autres mesures réactives; ainsi, les administrateurs de RL doivent se rendre physiquement à chaque ordinateur afin d'éradiquer les virus.

Recommandation n° 5 : Il est recommandé que les Systèmes élaborent un plan (comprenant les ressources) à l'intention du groupe responsable du contrôle de la protection de l'information.

2.2.3 L'analyse des répercussions sur les opérations, l'évaluation de la menace et des risques, le plan de continuité des opérations, le plan antisinistre ainsi que le plan d'intervention en cas d'urgence ne sont pas tous documentés et à jour et n'ont pas tous été testés

Nous avons constaté que le bureau de l'agent de sécurité du ministère au sein de la DGFA a réuni les plans de continuité des opérations (PCO) des programmes nationaux et des régions. En plus d'être documentés, les PCO sont à jour et ils ont été testés, en ce sens qu'ils ont été actualisés et révisés au cours de la dernière année. Nous avons également trouvé des exemples de plans de continuité des opérations qui ont été récemment appliqués et qui se sont révélés efficaces. De plus, on trouve sur le site Web des Systèmes les plans de continuité des opérations documentés et à jour (exercice 2002-2003) pour les quatre CTI du ministère. Une évaluation de la menace et des risques a par ailleurs été faite récemment (exercice 2002-2003) pour tous les CTI.

Toutefois, nous avons constaté que certaines applications logicielles/Internet essentielles à notre mission et récemment mises en œuvre au [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]; la direction a pris des mesures à ce sujet. Les plans de continuité des opérations de trois des quatre CTI ont été testés intégralement. Même si le [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] a fait une simulation de son plan en février 2004, celui-ci n'a pas été testé intégralement (dans une perspective opérationnelle), mais il devrait l'être au quatrième trimestre de 2004.

Recommandation n° 6 : Il est recommandé que les Systèmes continuent de tester avec toute la diligence possible les plans de continuité des opérations :

a) de toutes les applications logicielles essentielles à la mission [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.];
b) du [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.].

À l'issue de la vérification de la STI qu'il a menée en 2002, le Bureau de la vérificattice générale avait recommandé la réalisation d'une évaluation globale de la menace et des risques. En conséquence, le groupe des SSTI aux Systèmes a entrepris une analyse de sensibilité au cours de l'exercice précédent. Il s'agit de la première étape d'une évaluation plus générale de la menace et des risques (EMR) qui doit être amorcée au cours du présent exercice (2004-2005). Même si des EMR ont été réalisées lorsque de nouvelles modifications importantes ont été apportées aux applications ou aux infrastructures, nous n'avons trouvé aucun critère ou base de référence à l'échelle du ministère qui permettrait de déterminer dans quelles circonstances une EMR devrait être menée en cas de changements de grande envergure. Selon les discussions que nous avons eues avec des représentants des groupes d'applications logicielles du ministère, la réalisation d'une EMR est souvent discrétionnaire ou aléatoire. L'absence de critères ou de base de référence précisant dans quels cas de telles évaluations doivent être réalisées, pourrait faire en sorte que les EMR ne soient pas effectuées au moment opportun.

Recommandation n° 7 : Il est recommandé que les Systèmes, en collaboration avec l'agent de sécurité du ministère, établissent des critères et des bases de référence spécifiques qui permettraient de déterminer dans quelles circonstances une évaluation de la menace et des risques doit être réalisée.

2.2.4 Il existe un processus d'intervention approprié en cas d'incident

Nous avons constaté l'absence d'une définition formelle de ce qui constitue un incident en matière de STI. Toutefois, les incidents et problèmes touchant la TI sont signalés par l'entremise de l'InfoService national (ISN) du ministère. L'ISN transmet le problème au « groupe de résolution » compétent (qui peut comprendre les administrateurs de RL, les SSTI, l'agent de sécurité du ministère et des groupes de contrôle de la protection de l'information) en constituant un dossier d'incident dont il fait le suivi jusqu'à la résolution du problème. Il peut s'agir de problèmes de matériel ou de logiciels (y compris les virus). Les incidents de nature délicate (p. ex., les cas d'usage abusif d'Internet) sont signalés à l'agent de sécurité du ministère/de la région aux fins d'une enquête, et, s'il y a lieu, l'entité compétente en est saisie (p. ex., superviseur, Ressources humaines, GRC, etc.) afin que soient appliquées des mesures disciplinaire. Nous avons également constaté que, conformément aux exigences de la Politique du gouvernement sur la sécurité, les incidents touchant la sécurité sont consignés et archivés.

Recommandation n° 8 : Il est recommandé que les Systèmes, en collaboration avec l'agent de sécurité du ministère, définissent clairement ce qui constitue un incident se rapportant à la STI et fassent connaître cette définition à tout le personnel.

2.2.5 On n'attache pas suffisamment d'importance à la STI dans le cycle de développement des systèmes du ministère

Le cycle de vie des projets (CVP) du ministère, qu'on trouve sur le site Web des Systèmes, mentionne la sécurité pour la première fois à l'étape de la conception (la troisième étape). Cependant, dans son rapport de 2002 sur la STI, le Bureau de la vérificatrice générale recommandait que la sécurité soit prise en compte dès la première étape, comme l'ont fait les SSTI des Systèmes dans leur site Web. Par ailleurs, les SSTI ont récemment mis au point un modèle de STI qui énonce toutes les exigences à respecter à chacune des six étapes du CVP. Même si ce modèle a été présenté au comité général de gestion des Systèmes, qui l'a approuvé, il n'a pas encore été adopté et implanté dans le CVP des systèmes.

Recommandation n° 9 : Il est recommandé que les Systèmes :

a) implantent le modèle de STI des Services de sécurité de la technologie de l'information;
b) mettent à jour la page de leur site Web portant sur le cycle de vie des projets, afin de tenir compte des nouvelles exigences en matière de STI.

Il existe au ministère un comité d'examen des projets (CEP) dont « le rôle est de favoriser la réussite des projets par le biais des pratiques exemplaires en ce qui a trait aux examens périodiques, à l'évaluation des risques ainsi qu'aux méthodes et aux outils uniformisés du cycle de vie des projets ». Le rôle du CEP englobe notamment les exigences en matière de STI et les résultats attendus (p. ex., évaluation de la menace et des risques, consultation de l'agent de sécurité du ministère, contrats, etc.). Comme les membres du CEP ne se sont pas réunis depuis plus d'un an, à notre avis, il y a un risque que certains projets ministériels ne tiennent pas compte des pratiques exemplaires et compromettent les exigences en matière de STI. Par exemple, nous croyons savoir que certains projets, notamment [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], n'ont pas tenu compte suffisamment tôt des exigences en matière de STI dans le CVP, de sorte que lesdites exigences ont été passées en revue et modifiées après la signature des contrats avec les fournisseurs. De telles pratiques « après-coup » pourraient se révéler coûteuses pour le ministère à bien des égards.

Recommandation n° 10 : Il est recommandé que les Systèmes réactivent le comité d'examen des projets (ou un mécanisme de régie semblable) pour veiller au respect des exigences en matière de STI.

2.3 Contrôles concernant le personnel

2.3.1 Aucun programme national de sensibilisation à la STI n'a encore été mis en œuvre à l'intention du personnel du ministère

Selon des représentants du Centre de la sécurité des télécommunications, un des éléments qui a « le plus grand impact » en ce qui concerne la STI est la sensibilisation, qui donne le ton et établit la culture en matière de sécurité au sein d'un organisme. Le 24 mars 2004, les SSTI ont organisé un forum de sensibilisation à la STI avec des représentants ministériels (y compris les CTI, les régions et l'agent de sécurité du ministère), afin de discuter d'une approche graduelle pour la mise en œuvre d'un programme national de sensibilisation à la STI. Les SSTI ont également affiché l'ébauche d'un « programme de sensibilisation à la STI » sur leur site Web (mai 2004). Selon notre analyse de ce « programme », il s'agit d'un programme pratique et exhaustif. Nous félicitons les SSTI de cette initiative et nous appuyons la mise en œuvre d'un programme de sensibilisation à la STI à l'échelle du ministère.

Recommandation n° 11 : Il est recommandé que les Systèmes établissent la version définitive d'un programme ministériel de sensibilisation à la sécurité de la technologie de l'information et le mettent en œuvre à l'échelle nationale.

2.3.2 Les politiques et procédures en matière de STI qui touchent le personnel (p. ex., courriels, utilisation appropriée des ordinateurs, etc.) ont été communiquées régulièrement aux personnes intéressées

Comme nous l'avons déjà indiqué, il existe de nombreuses politiques et procédures relatives à la STI, dont certaines concernent expressément le personnel. Elles ont été communiquées régulièrement au personnel, que ce soit de la part du SMA, Systèmes ou d'autres membres de la direction, y compris les administrateurs de RL, par l'entremise de courriels, d'écrans flash, de communications générales et de sites Web.

2.3.3 Des enquêtes d'autorisation de sécurité sont effectuées pour la plupart des membres du personnel qui ont accès aux données du ministère, ainsi que pour des personnes qui n'appartiennent pas à l'effectif du ministère (p. ex., des fonctionnaires provinciaux, des membres d'autres organismes gouvernementaux, des sous-traitants), mais des problèmes ont été constatés concernant les autorisations de sécurité qui venaient à échéance et les autorisations pour les fonctionnaires provinciaux

Toutes les régions que nous avons visitées respectaient les exigences de la Politique du gouvernement sur la sécurité voulant que tous les employés, y compris les étudiants et les sous-traitants, aient l'autorisation de sécurité appropriée avant d'exercer leurs fonctions. L'agent de sécurité du ministère nous a confirmé que les sous-traitants auxquels le ministère a recours avaient les autorisations de sécurité appropriées, ce que nous avons d'ailleurs pu observer nous-mêmes.

Les autorisations de sécurité ont des dates d'échéance établies en fonction du niveau d'autorisation (les cotes « Secret » expirent au bout de dix ans, les cotes « Très secret » au bout de cinq ans, etc.). Conformément à la Politique du gouvernement sur la sécurité, le processus suivi par le ministère en ce qui concerne l'expiration des autorisations de sécurité prévoit la « mise à jour régulière des cotes de fiabilité et des cotes de sécurité ». Après avoir analysé les statistiques relatives à l'expiration des autorisations de sécurité, nous avons conclu que toutes les régions respectent assez bien ce processus [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].

Recommandation n° 12 : Il est recommandé que [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].

Des membres du personnel des bureaux régionaux et de l'administration centrale (y compris l'ASM) nous ont appris que [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], la Politique du gouvernement sur la sécurité stipule que « les ministères doivent appliquer cette politique [du gouvernement sur la sécurité] lors du partage de renseignements et d'autres biens du gouvernement du Canada avec d'autres gouvernements (p. ex., étrangers, provinciaux, territoriaux et municipaux), des organismes internationaux, des établissements d'enseignement et des organismes du secteur privé […] et les ministères doivent limiter l'accès aux renseignements classifiés et protégés et aux autres biens aux seules personnes qui ont besoin de les connaître et qui ont la cote de fiabilité ou de sécurité appropriée ».

Recommandation n° 13 : Il est recommandé que l'agent de sécurité du ministère et les agents de sécurité régionaux :

a) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.];
b) si tel n'est pas le cas, qu'ils déterminent les mesures correctives qui peuvent être prises.

Nous avons également analysé les autorisations de sécurité de tous les administrateurs de RL de la région de la capitale nationale, et confirmé qu'elles étaient appropriées.

2.3.4 Le ministère tient un registre de tous les articles liés à la TI qui sont utilisés par le personnel en poste ou quittant le ministère

Les administrateurs de RL ont un registre/inventaire du matériel. Les licences d'utilisation des logiciels, le matériel (sur place et à l'extérieur, par exemple les ordinateurs portatifs, les ordinateurs personnels utilisés à la maison) et l'accès aux ordinateurs centraux des CTI sont tous consignés par écrit et gérés. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]

Les employés qui quittent le ministère doivent remplir le formulaire ADM 5017, Certificat de fin d'emploi, pour faire en sorte que tout le matériel lié à la TI soit pris en compte. De plus, le formulaire doit être signé par le gestionnaire du centre de responsabilité dont relevait l'employé qui part; le gestionnaire le transmet ensuite aux RH pour les besoins du traitement final. Toutefois, le formulaire ne mentionne pas expressément le retrait des droits/moyens d'« accès logique » aux systèmes du ministère, comme les mots de passe, les noms d'utilisateur, [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], etc. En ne verrouillant pas « l'accès logique » d'un ancien employé, le ministère s'expose au risque que cet employé puisse accéder à des systèmes auxquels il n'a plus besoin ni le droit d'avoir accès.

Recommandation n° 14 : Il est recommandé que le le formulaire ADM 5017, Certificat de fin d'emploi, soit révisé pour veiller à ce que « l'accès logique » d'un employé qui quitte le ministère soit verrouillé.

2.4 Contrôles techniques

2.4.1 Des mesures de protection relatives à la STI (p. ex,. coupe-feu, antivirus) font l'objet d'un maintien, d'un suivi (p. ex., attaques électroniques) et de mises à niveau (le cas échéant), mais elles sont susceptibles d'être améliorées

DRHC a mis en place des mesures de protection relatives à la STI, et le ministère en assure le maintien, le suivi et la mise à niveau en protégeant ses réseaux au moyen de coupe-feu, en s'assurant que ses logiciels antivirus sont à jour, en installant des filtres aux passerelles de messageries, en contrôlant la distribution, l'authentification et le cryptage des logiciels [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], etc., et en faisant un suivi des attaques électroniques provenant de l'extérieur.

Comme on l'a vu au paragraphe 2.2.2 ci-dessus, un groupe de CPI a été mis sur pied récemment afin de détecter les problèmes se rapportant à la STI, de les régler et de faire rapport à leur sujet, y compris au sujet des virus. Il est également possible de mobiliser l'équipe d'intervention d'urgence pour les failles dans l'infrastructure, un service national multidisciplinaire, si le ministère est aux prises avec des virus. Les responsables du projet antivirus, quant à eux, ont mis au point des outils (p. ex., [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]) pour protéger le ministère contre les virus. DRHC a également recours aux [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] pour protéger les ordinateurs personnels de bureau et les serveurs, et de nouveaux outils visant à renforcer la sécurité au sein du ministère font l'objet d'un examen. Nous avons aussi constaté que des fonctionnaires du ministère consultent diverses sources d'information sur les mesures de protection liées à la STI, notamment l'équipe de réaction en informatique, le Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC), les avis du SANS Institute, ainsi que [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].

Il s'agit là de bonnes pratiques, mais nous avons relevé des éléments susceptibles d'être améliorés.

Les CTI ont récemment acheté de nouveaux disques de données pour les ordinateurs centraux qui exécutent certaines des grandes applications du ministère, comme l'assurance-emploi et les prêts aux étudiants. Conformément au contrat d'achat, le fournisseur ([L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]) est tenu d'offrir du soutien technique en ligne, notamment le suivi et la détection des problèmes concernant ces disques, au moyen d'un logiciel qui établit automatiquement des communications commutées entre [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].

Recommandation n° 15 : Il est recommandé que les Systèmes :
a) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.];
b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.];
c) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.].

Des sources bien renseignées nous ont confié qu'il y a des [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].

Recommandation n° 16 : Il est recommandé que les Systèmes adoptent une politique/directive stipulant que seule la technologie autorisée par le ministère (p. ex. les serveurs) peut être connectée au réseau, et qu'ils veillent à son application.

En visitant les bureaux locaux, nous avons constaté que dans certains cubicules utilisés par les représentants du service à la clientèle du ministère pour accueillir ou interviewer les clients, les ordinateurs sont placés de telle façon que les clients y ont accès par l'arrière. Un tel accès aux ordinateurs non protégés des employés pourrait avoir des conséquences, comme la destruction de biens appartenant au gouvernement; de plus, les clients pourraient avoir accès aux ports qu'on trouve à l'arrière des ordinateurs personnels, compromettant ainsi la sécurité. Certaines régions que nous avons visitées ont admis le problème et ont pris des mesures pour protéger ces ordinateurs, et ainsi limiter les possibilités que les clients y aient accès.

Recommandation n° 17 : Il est recommandé que les Systèmes adoptent une politique/directive stipulant que tous les ordinateurs du personnel doivent être protégés et que des mesures doivent être prises pour empêcher le public/les clients d'y avoir accès.

D'après les normes de l'industrie, il faut faire des tests périodiques de pénétration interne et externe sur les systèmes de TI, comme le précise d'ailleurs le mandat des SSTI. Nous avons constaté que ce genre de test est mené de façon ponctuelle, mais nous n'avons trouvé aucun plan/calendrier prévoyant des tests périodiques de pénétration interne et externe pour le réseau.

Recommandation n° 18 : Il est recommandé que les Systèmes fassent régulièrement des tests de pénétration interne et externe pour le réseau du ministère.

2.4.2 Des contrôles d'accès logique ont été mis en œuvre, mais ils pourraient être améliorés

Au ministère, les contrôles d'accès logique sont déterminés par le matériel et les logiciels utilisés (en d'autres mots, ils dépendent de la plateforme). L'environnement des ordinateurs centraux et celui des serveurs, par exemple [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], etc., contrôlent activement l'accès logique au moyen de noms d'utilisateur, de mots de passe, de listes de contrôle d'accès, de profils et d'autres méthodes. L'ébauche d'une politique sur les mots de passe et les noms d'utilisateur a été réalisée.

Nous avons constaté que même si le ministère a mis en œuvre des contrôles d'accès logique, des améliorations peuvent y être apportées.

Jusqu'à maintenant, dans l'environnement [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], nous n'avons trouvé aucune preuve montrant que des vérifications ont été effectuées au sein du ministère pour veiller au respect de la norme gouvernementale selon laquelle les mots de passe doivent compter huit caractères alphanumériques et être changés tous les 90 jours. En collaboration avec le Centre de la sécurité des télécommunications, nous avons découvert que près de la moitié (49 p. 100) des 34 891 mots de passe examinés comptent moins de 8 caractères [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]. Pour l'instant, le Ministère n'a pas de politique officielle et n'a pas non plus adopté de solution technique pour veiller à ce que la norme gouvernementale concernant les mots de passe soit respectée.

Recommandation n° 19 : Il est recommandé que les Systèmes adoptent une politique et prévoient une solution technique pour veiller à ce que la norme gouvernementale concernant les mots de passe soit respectée.

Dans les bureaux régionaux, certains employés utilisent différentes applications (p. ex., E/C, AE, SNSE, SGD, etc.) qui sont exécutées sur différentes plateformes (p. ex., [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], etc.), chacune nécessitant un mot passe et un nom d'utilisateur différents. Nous avons appris qu'un même employé peut avoir besoin de 12 mots de passe pour son travail, et il est difficile de se souvenir de chacun. On nous a dit que les employés notent souvent leurs mots de passe et les « cachent » sous leur clavier, leur ordinateur, leur téléphone, dans un tiroir de leur pupitre, etc. On nous a dit également que les employés choisissent souvent les mêmes mots de passe pour différentes applications et qu'ils choisissent des mots de passe faciles à deviner. Par conséquent, l'environnement des mots de passe et noms d'utilisateur de DRHC [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]. Un projet d'ouverture de session unique à des fins de gestion de la sécurité devait régler certains de ces problèmes, mais il n'a finalement pas été lancé, faute de financement. Même si l'adoption d'une politique et d'une solution technique se révélait utile pour veiller à ce que la norme gouvernementale concernant les mots de passe soit respectée (Recommandation n° 19 ci-dessus), cela ne réglerait pas pour autant le problème des nombreux mots de passe dont certains employés ont besoin ni la façon dont ils les « cachent ».

Recommandation n° 20 : Il est recommandé que les Systèmes adoptent une solution technique pour réduire le nombre de mots de passe dont les employés ont besoin pour accéder à de multiples systèmes.

Aux fins de l'administration de la sécurité des ordinateurs centraux des [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], un progiciel de sécurité appelé [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] produit une liste sur papier de tous les utilisateurs qui accèdent aux divers systèmes centraux. Les représentants des [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] transmettent régulièrement cette liste aux gestionnaires de centre

de responsabilité (CR) compétents du ministère, qui doivent l'examiner et la mettre à jour le cas échéant (c'est-à-dire confirmer, supprimer, ajouter, modifier, etc., l'accès des utilisateurs aux ordinateurs centraux du [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]). Toutefois, les gestionnaires de CR ne sont pas tenus de retourner la liste corrigée aux [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]; rien ne les oblige à confirmer que la liste des [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] reflète fidèlement leurs besoins en matière d'accès. L'analyse que nous avons faite de la liste produite par [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] avec des gestionnaires de CR nous a permis de constater que certains utilisateurs qui ne devraient plus avoir accès aux systèmes centraux y ont encore accès.

Recommandation n° 21 : Il est recommandé que les gestionnaires de centre de responsabilité examinent et mettent à jour les listes [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] dans les deux semaines suivant leur réception et qu'ils les retournent promptement aux [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].

L'impression des listes [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], produites par les [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], et leur distribution aux CR se font manuellement, mais il semble qu'une application Web serait plus économique et plus efficace.

Recommandation n° 22 : Il est recommandé que les Systèmes examinent la possibilité d'afficher les listes [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] sur un site Web.

2.4.3 L'accès aux salles d'ordinateurs ou de serveurs est contrôlé

L'accès à toutes les salles d'ordinateurs ou de serveurs que nous avons examinées était limité aux personnes autorisées par le biais de cartes et de clés; elles étaient équipées de systèmes d'alarme et des rapports de l'accès pouvaient être produits. Toutefois, le grand nombre de personnes qui ont accès à certains des [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] que nous avons visités dans les régions est une source de préoccupation. Le ministère compte [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] où sont regroupés ses serveurs, ce qui permet d'offrir un meilleur soutien à l'infrastructure nationale. L'architecture repose sur un modèle régional selon lequel chaque région dispose d'un ou de plusieurs [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] pour fournir les services opérationnels. Compte tenu de notre préoccupation, les régions que nous avons visitées sont en train de réexaminer l'accès aux [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].

Recommandation n° 23 : Il est recommandé que les Systèmes et les régions limitent l'accès à leurs [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] aux seules personnes qui en ont besoin.

2.4.4 Les données sont sauvegardées régulièrement

Tous les [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] et les [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] que nous avons visités sauvegardent régulièrement les données et conservent les copies de sauvegarde hors site.

2.4.5 DRHC n'a pas adopté de paramètres pour évaluer l'efficacité de sa STI

Même si divers rapports sont produits au sujet de la TI (p. ex., [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*], etc.), le suivi des tendances et la surveillance des activités se font souvent de façon ponctuelle. Toutefois, en ce qui concerne expressément la STI, nous n'avons trouvé aucun ensemble formel de paramètres, comme des indicateurs clés du rendement, qui font l'objet d'analyses par rapport à des normes ou à des critères prédéterminés aux fins de l'évaluation de l'efficacité de la STI.

Recommandation n° 24 : Il est recommandé que les Systèmes établissent des paramètres aux fins de l'évaluation de l'efficacité de la STI.

2.5 Suite donnée aux conclusions de vérifications précédentes

2.5.1 SVIGR, septembre 1999

Nous affirmions, dans la section 2.1.4 qui précède, que « des vérifications et des examens formels de la STI avaient été réalisés et que les observations avaient été prises en compte au moment de l'établissement des plans d'action », ceux-ci ayant été élaborés avec les meilleures intentions, compte tenu de l'information disponible à l'époque. Cependant, à l'issue de notre vérification, force nous est de constater que certains plans d'action n'ont pas toujours donné les résultats escomptés.

En septembre 1999, nous avons fait une vérification de la STI à DRHC et en avons conclu que le Ministère devait :

- rationaliser sa structure et ses processus organisationnels de manière à gérer la STI à tous les niveaux;
- accroître les connaissances de tout son personnel en matière de STI tout en le sensibilisant davantage à cet égard.

Compte tenu des résultats de la vérification que nous présentons ici, nous concluons que même si DRHC a réalisé des progrès pour rationaliser sa structure et ses processus organisationnels de manière à gérer la STI, il reste encore des améliorations à apporter. Même si nous affirmons dans la section 2.2.2 que les rôles et responsabilités en matière de STI ont été documentés et attribués, ils demeurent quelque peu fragmentés, en ce sens qu'ils ne fonctionnent pas toujours de façon unifiée et transparente pour maximiser les synergies. Comme nous l'avons indiqué dans la section 2.1.1, nous croyons que d'autres améliorations pourraient être apportées afin de renforcer la cohésion de la structure de régie de la STI; des progrès ont toutefois été réalisés (p. ex,. la création du comité de gestion de la sécurité de la technologie de l'information). Enfin, nous avons également mentionné dans les sections 2.3.1 et 2.3.2 que des progrès ont été réalisés au chapitre de l'amélioration de la sensibilisation et des connaissances de tout le personnel de DRHC en matière de STI, et de l'élaboration de l'ÉBAUCHE d'un programme ministériel de sensibilisation à la STI (dont nous recommandons la mise en œuvre à l'échelle nationale).

2.5.2 BVG, avril 2002

En avril 2002, le Bureau de la vérificatrice générale a mené une vérification de la STI à DRHC, en relevant les mêmes éléments que ceux que nous avions constatés dans notre vérification de 1999, à savoir la nécessité :

- d'améliorer le cadre de régie de la STI *(sections 2.1.1 et 2.1.2)*;
- de mener des évaluations des risques à grande échelle *(section 2.1.3)*;
- d'offrir aux employés une formation pertinente afin de les sensibiliser à la STI *(sections 2.3.1 et 2.3.2)*;
- de s'assurer que la sécurité des TI est prise en compte au début du cycle de développement des systèmes *(section 2.2.5)*;
- d'effectuer des vérifications et des examens de la STI, notamment des essais techniques de vulnérabilité *(section 2.1.4)*;
- de régler d'autres problèmes *(section 2.0 — Constatations)*.

Essentiellement, les explications que nous donnons dans la section 2.5.1 s'appliquent également aux remarques du BVG. Nous indiquons aussi *(entre parenthèses)* les sections du présent rapport dans lesquelles nous commentons plus précisément les éléments déjà relevés par le BVG.

En outre, le BVG avait eu recours aux services de la firme Electronic Warfare Associates (EWA) pour mener des tests techniques (de vulnérabilité) de la STI à DRHC lors de sa vérification d'avril 2002. Pour déterminer quelle suite avait été donnée aux constatations faites à l'issue des tests du BVG (réalisés par EWA), nous avons eu recours à la même firme pour la présente vérification. EWA a conclu que, « dans l'ensemble », DRHC avait pris des mesures satisfaisantes en ce qui a trait aux vulnérabilités d'Internet indiquées dans le rapport du BVG […] et avait réglé adéquatement les problèmes relevés lors de l'évaluation des vulnérabilités du système téléphonique.

3.0 Constatations de la phase II — vulnérabilités internes de la STI (évaluation sur place de la vulnérabilité technique)

3.1 Introduction

Du 2 au 16 février 2004, la DVE, en collaboration avec le Centre de la sécurité des télécommunications, a fait à une évaluation de la vulnérabilité interne (EPVT) des systèmes de DRHC pour déterminer les points vulnérables des systèmes et des ressources d'information du ministère.

L'EPVT comprenait les éléments suivants :

- un exercice de découverte du réseau et une évaluation des vulnérabilités;
- une évaluation des règles régissant les coupe-feu;
- une évaluation des mots de passe;
- un exercice de découverte du RL sans fil 802.11b/a;
- un examen de la politique sur les dispositifs mobiles.

3.2 Constatations et recommandations

Selon les résultats de cette évaluation, la posture de DRHC en matière de sécurité à l'intérieur de ses défenses périmétriques pourrait être améliorée. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] Plusieurs systèmes d'exploitation et applications [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]. Il n'existe aucun processus global de gestion de la configuration, de sorte que les configurations ne sont pas uniformes entre les régions. La plus grande partie du trafic interne passe par [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]. Un grand pourcentage des menaces est lié à des vulnérabilités internes auxquelles il faudrait accorder la priorité.

DRHC devrait examiner ces problèmes, les classer par ordre de priorité et les régler selon un modèle de la menace et des risques. Par exemple, certains des systèmes évalués comportent des vulnérabilités qui [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] et qui devraient être considérées comme étant prioritaires.

Voici un sommaire des recommandations pour chacun des volets de l'EPVT :

- Exercice de découverte du réseau et évaluation des vulnérabilités :
  - [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];

- [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
- Tenir à jour une liste des hôtes connectés aux réseaux de DRHC;
- Veiller à ce que les services soient protégés adéquatement par l'utilisation de mots de passe;
- Procéder régulièrement à des exercices de découverte du réseau, au balayage des ports et à l'évaluation des vulnérabilités;
- [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
- Renforcer la convention d'appellation des noms du système pour éviter de révéler leurs fonctions réseaux aux utilisateurs non autorisés;
- [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
- Rendre plus difficile l'installation de logiciels;
- [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];

- Évaluation des règles régissant les coupe-feu :
  - Passer en revue et actualiser la politique sur les coupe-feu;
  - Passer en revue les règles de trafic pour le personnel de soutien et s'assurer qu'une procédure appropriée de gestion des changements est en place afin de conserver une liste à jour et exacte;
  - Recommander qu'un routeur de dépistage ou de filtrage soit utilisé pour bloquer l'accès à des services inutilisés par les interfaces non sécurisées des coupe-feu;
  - Intégrer aux routeurs de dépistage du fournisseur de service ses propres routeurs de filtrage, qui pourront faire l'objet d'une surveillance et occasionnellement d'un examen, ou mettre en œuvre un processus qui permettrait à DRHC de vérifier les éléments de sécurité et les listes de contrôle de l'accès des routeurs de filtrage du fournisseur de service.
- Évaluation des mots de passe :
  - Actualiser et appliquer la politique sur les mots de passe pour renforcer les règles de sélection des mots de passe;
  - Faire des évaluations régulières des mots de passe dans d'autres zones du réseau et d'autres systèmes pour s'assurer que la politique sur les mots de passe est respectée;
  - Supprimer les [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] de tout système lorsqu'ils ne sont pas utilisés;
  - S'abstenir d'assigner des mots de passe aux comptes [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] (comptes système) parce que ces comptes ne devraient pas être accessibles à partir du réseau et qu'ils devraient offrir peu de privilèges, voire aucun.
- Exercice de découverte du RL sans fil 802.11b/a :
  - [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
  - [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
  - [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];

- Mettre en place un réseau privé virtuel ou un RL sans fil protégé [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
- Adopter et appliquer une politique régissant les réseaux sans fil;
- Faire régulièrement des exercices de découverte pour détecter la présence de nouveaux points d'accès non autorisés.

- Examen de la politique sur les dispositifs mobiles :
  - [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
  - Utiliser un réseau privé virtuel dont la fonction de cryptage est approuvée par le Centre de la sécurité des télécommunications, ainsi qu'un coupe-feu individuel pour l'accès à Internet;
  - Mettre la politique à jour pour y traiter des questions relatives à l'installation de logiciels par les usagers, à la navigation sur le Web à des fins personnelles et à la mise à niveau des logiciels au moyen des ensembles de services et des correctifs les plus récents, etc.

4.0 Constatations de la phase III — vulnérabilités externes de la STI (Vérification de la sécurité des réseaux actifs)

4.1 Introduction

Du 8 mars au 1er septembre 2004, la DVE, en collaboration avec le Centre de la sécurité des télécommunications, a fait une évaluation de la vulnérabilité externe (VSRA) des systèmes de DRHC, pour déterminer les risques de vulnérabilité des réseaux périmétriques du ministère à des attaques électronique et tester les capacités de réaction et d'intervention de DRHC en pareilles circonstances.

La VSRA comprenait les éléments suivants :

- un balayage et un sondage d'exploration des réseaux;
- un sondage d'exploration des dispositifs sans fil;
- un sondage d'exploration des modems connectés au réseau téléphonique public commuté (RTPC);
- une attaque d'ingénierie sociale;
- l'exploitation des vulnérabilités des hôtes internes;
- le décodage de mots de passe et la réutilisation de mots de passe;
- la détection des activités de la VSRA;
- un nettoyage.

4.2 Constatations et recommandations

L'équipe de la VSRA a mené les activités auxquelles se livrerait un attaquant qui aurait ciblé les réseaux de DRHC. Même si ces pseudo-attaques ont montré que les défenses périmétriques des systèmes sont suffisamment solides, l'exploitation des vulnérabilités des protocoles de niveau supérieur a compromis le réseau interne. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]

[L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] Selon les résultats de l'évaluation, la posture de DRHC en matière de sécurité pourrait donc être améliorée.

Les recommandations suivantes sont soumises à l'examen de DRHC; elles permettraient d'améliorer la sécurité de ses réseaux et de réduire les risques que des personnes non autorisées puissent y accéder :

- Continuer d'assurer la sécurité des dispositifs périmétriques;
- [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
- [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];

- Passer en revue et faire respecter la politique sur les mots de passe :
  - Remplacer les protocoles d'authentification des mots de passe par des mécanismes à deux facteurs pour tous les services de réseau sensible;
  - Mettre sur pied un programme de sensibilisation à l'intention des utilisateurs, assorti d'instructions visant à réduire la réutilisation des mots de passe.
- Crypter le trafic de nature délicate qui passe par le Web;
  - [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];
- Installer des coupe-feu internes :
  - Le réseau interne devrait être protégé par des coupe-feu internes qui restreignent le trafic aux transmissions autorisées en vertu de la politique de sécurité du réseau;
  - Prévoir un journal d'exploitation pour repérer les intrusions ou les activités internes de balayage et de sondage d'exploration;
- Mettre sur pied un programme de sensibilisation à la sécurité à l'intention des utilisateurs:
  - Prévoir des points de contact pour le signalement des problèmes et la façon de traiter les courriels non sollicités et les courriels accompagnés, par exemple, de fichiers Zip protégés par des mots de passe et d'autres fichiers de type dangereux;
- Désactiver les services internes qui ne sont pas nécessaires;
- Installer un système de détection des intrusions dans les réseaux internes :
  - Parallèlement aux coupe-feu internes, les systèmes de détection des intrusions peuvent empêcher un attaquant de compromettre les réseaux internes de DRHC sur une grande échelle;
- Étalonner et contrôler le trafic aux points de sortie;
- Éliminer toute information non nécessaire des bandeaux :
  - Imposer des limites à l'information fournie pour les services externes afin de réduire la quantité d'information qui pourrait être utile à un attaquant qui passerait par Internet.

Annexe A

Objectifs, portée, normes et méthodologie

Objectifs

Phase I — Le cadre de régie de la STI à DRHC

La première phase consistera à évaluer les contrôles de la STI à DRHC, à faire le suivi des questions soulevées à la suite des deux vérifications antérieures de la STI et à documenter la création d'une carte réseau des systèmes de DRHC, qui servira aux essais techniques des phases II et III.

Le cadre de régie de la STI à DRHC sera évalué par rapport à quatre principes de contrôle de la STI, qui reposent sur les éléments fondamentaux de la Politique du gouvernement sur la sécurité établie par les Services des opérations gouvernementales au Secrétariat du Conseil du Trésor; la Norme de gestion de la sécurité de la TI établie par la Direction du dirigeant principal de l'information au Secrétariat du Conseil du Trésor; la Norme de sécurité technique dans le domaine de la technologie de l'information de la GRC; et la norme ISO/CEI 17799 sur la STI. Ces principes de contrôle de la STI s'inspirent des normes applicables aux objectifs de contrôle dans les domaines de l'information et des technologies connexes établies par l'Association des professionnel(le)s en Vérification et Contrôle des Systèmes d'Information (APVCSI), normes qui sont reconnues internationalement.

a) Contrôles de gestion
b) Contrôles opérationnels
c) Contrôles concernant le personnel
d) Contrôles techniques

Pendant la première phase, on évaluera la suite donnée par DRHC aux questions soulevées dans deux rapports précédents de vérification de la STI, l'un provenant du BVG (avril 2002) et l'autre, des SVIGR (septembre 1999).

Enfin, les SVIGR documenteront la création d'une carte réseau des systèmes de DRHC, qui servira de base à la conduite des essais techniques des phases II et III.

Phase II — Vulnérabilités internes de la STI : évaluation sur place de la vulnérabilité technique

La deuxième phase aura pour objet d'évaluer la vulnérabilité interne des systèmes de DRHC de manière à déterminer les points vulnérables des systèmes et des ressources d'information du ministère.

Phase III — Vulnérabilités externes de la STI : vérification de la sécurité des réseaux actifs

La troisième phase aura pour objet d'évaluer la vulnérabilité externe des systèmes de DRHC de manière à déterminer les risques de vulnérabilité des réseaux périmétriques du ministère à des attaques électroniques, et à tester la capacité de réaction et d'intervention de DRHC en pareilles circonstances.

Au besoin, les SVIGR formuleront des recommandations visant à améliorer le cadre de régie de la STI à DRHC ainsi que la sécurité interne et externe des réseaux.

Portée

La vérification intégrée de la sécurité de la TI à DRHC consistera à évaluer les éléments de nature non technique (cadre de régie) et technique (évaluations internes et externes). L'administration centrale de DRHC [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] et les régions du Québec, de l'Ontario, de l'Alberta/T.N.-O./Nunavut et de la Colombie-Britannique/Yukon seront visitées au cours de cette vérification. En consultation avec certains responsables de la sécurité de la TI au ministère, les systèmes à évaluer seront déterminés et des « listes d'objectifs » seront établies pour les schémas de réseau, les systèmes d'exploitation, les adresses IP, les numéros de téléphone, les RL sans fil, les téléphones cellulaires, les PDA et autres dispositifs sans fil utilisant le protocole IEEE 802.11b.

Normes

Les normes de vérification qui suivent s'inspirent des normes relatives aux objectifs de contrôle dans les domaines de l'information et des technologies connexes (COBIT) de l'APVCSI, qui sont reconnues à l'échelle internationale et qui sont avalisées par d'autres groupes comme PricewaterhouseCoopers, IBM et le groupe Gartner.

Phase I : Normes — Cadre de régie de la STI à DRHC

a) Contrôles de gestion
- La structure de gestion de la STI doit être documentée, intégrée aux programmes de DRHC et appuyée à tous les niveaux de la gestion.
- Des politiques et des procédures pratiques et utiles en matière de STI doivent être diffusées rapidement aux utilisateurs concernés.
- La gestion des risques doit être un processus officiel de gestion de la STI intégré aux méthodes de gestion de DRHC.
- Des vérifications et des examens officiels de la STI doivent être effectués, et les conclusions de ces exercices doivent se retrouver dans des plans d'action.

b) Contrôles opérationnels
- Les politiques et procédures relatives à la STI doivent décrire les rôles et responsabilités (R/R) ainsi que les services en matière de STI au sein du ministère.

- Les R/R et la prestation des services en matière de STI doivent être confiés aux personnes et aux groupes disposant des ressources nécessaires à l'exécution de leur mandat.
- L'analyse des répercussions sur les opérations liées à la STI, l'évaluation de la menace et des risques, le plan de continuité des opérations, le plan antisinistre et le plan d'intervention en cas d'urgence sont documentés, à jour et ont été testés.
- On doit disposer d'un processus d'intervention efficace en cas d'incident.
- On tient compte de façon appropriée de la STI dans le cycle de développement des systèmes de DRHC.

c) Contrôles concernant le personnel
   - Un programme national de sensibilisation à la STI doit être mis en œuvre à DRHC.
   - Les politiques et procédures en matière de STI qui ont trait au personnel (p. ex., mots de passe, utilisation appropriée des ordinateurs, etc.) sont communiquées au personnel.
   - Des enquêtes de sécurité doivent être effectuées pour tout membre du personnel ayant accès aux données de DRHC, y compris le personnel des autres ministères et les sous-traitants.
   - DRHC doit tenir un registre de tous les articles liés à la TI qui sont utilisés par le personnel en poste ou quittant le ministère.

d) Contrôles techniques
   - Des mesures de protection relatives à la STI (p. ex., coupe-feu, antivirus) doivent être maintenues (suivant les besoins), suivies (p. ex., attaques électroniques) et mises à niveau (le cas échéant).
   - Des contrôles de l'accès logique doivent être mis en œuvre.
   - L'accès aux salles d'ordinateurs ou de serveurs doit être contrôlé.
   - Les données doivent être sauvegardées régulièrement.
   - DRHC doit adopter des paramètres pour évaluer l'efficacité de sa STI.

Les SVIGR sont d'avis que l'utilisation des normes énumérées ci-dessus pour évaluer le cadre de régie de la STI à DRHC, leur permettra également de suivre les progrès du ministère en ce qui a trait aux questions soulevées à l'occasion de deux vérifications antérieures de la STI.

Dans son rapport sur la STI (chapitre 3, avril 2002), le BVG a souligné la nécessité de :

- voir à améliorer le cadre de régie de la STI;
- procéder à des évaluations générales des risques;
- offrir aux employés une formation appropriée pour les sensibiliser à la STI;
- veiller à ce que la STI entre en ligne de compte dès le début du cycle de développement des systèmes;
- procéder à des vérifications et à des examens de la STI (y compris des tests de vulnérabilité technique);
- donner suite à d'autres questions.

L'évaluation de la STI menée par les SVIGR (septembre 1999) soulignait la nécessité :

- de rationaliser la structure et les processus organisationnels de DRHC de manière à gérer la STI à tous les niveaux;
- d'accroître les connaissances de tout le personnel de DRHC en matière de STI tout en le sensibilisant davantage à cet égard.

Les SVIGR mettront au point une carte réseau des systèmes de DRHC qui déterminera les coupe-feu, routeurs, commutateurs, concentrateurs, serveurs d'application et autres composantes de réseau essentielles, y compris l'information concernant les sous-réseaux et les adresses IP pour chacun des dispositifs du réseau. Cette carte servira à définir les dispositifs qui seront visés aux phases II et III.

Les normes employées pour les tests techniques des phases II et III consistent en méthodes et activités utilisées fréquemment par des agents de menace (p. ex., les pirates informatiques, les virus, etc.) cherchant à compromettre le fonctionnement d'un système. La page suivante présente un bref aperçu des normes qui seront utilisées pour aider DRHC à repérer toute vulnérabilité existante ou éventuelle.

Phase II : Normes — Vulnérabilités internes de la STI : vérification sur place de la vulnérabilité technique

a) Balayage du réseau et de l'hôte
   - Découvrir les dispositifs actifs du réseau de DRHC et autres services (p. ex., TCP, PNU, etc.) qui font l'écoute intersigne du processus de découverte du réseau.

b) Balayage de détection des vulnérabilits du réseau
   - À l'aide d'un scanneur permettant de détecter les vulnérabilités du réseau, balayer les dispositifs actifs relevés au cours du processus de découverte du réseau.

c) Évaluation des routeurs
   - Examiner la sécurité de la configuration et du fonctionnement des fichiers de configuration des routeurs.

d) Analyse de commutation de RL
   - Évaluer la version de commutateurs utilisée par DRHC en insistant sur la sécurité des commutateurs comme tels et en analysant leur capacité à protéger le réseau.

e) Découverte des points d'accès sans fil
   - Relever les points d'accès au RL IEEE 802.11b sans fil dans les locaux de DRHC en utilisant les outils de découverte des points d'accès IEEE 802.11b sans fil.

f) Examen des politiques relatives aux dispositifs mobiles
   - Évaluer le degré de conformité des politiques/procédures de DRHC relatives aux dispositifs mobiles.

g) Évaluation des mots de passe
   - Évaluer la politique en vigueur relative aux mots de passe pour les systèmes de DRHC au moyen des outils de vérification et de récupération des mots de passe.

h) Découverte de l'accès commuté/détection d'accès entrant
   - Rechercher les modems, télécopieurs et autres dispositifs non protégés et/ou non autorisés dans une série déterminée de numéros de téléphone.

Phase III — Vulnérabilités externes de la STI : vérification de la sécurité du réseau actif (VSAR)

a) Balayage des réseaux
   - Dresser la carte réseau périmétrique de DRHC au moyen du balayage des dispositifs du réseau et du détecteur d'accès entrant (pour démontrer comment un « agent de menace » pourrait dresser la carte réseau de DRHC à l'insu du ministère).

b) Sondage d'exploration des réseaux
   - Explorer les réseaux et les ordinateurs de DRHC afin de déterminer les systèmes d'exploitation et les services offerts par chacun des dispositifs découverts (afin de démontrer comment un « agent de menace » pourrait en faire autant sans être découvert).

c) Détermination des vulnérabilités
   - Rechercher les vulnérabilités possibles liées aux dispositifs, services et systèmes d'exploitation de DRHC.

d) Recherche et développement en matière d'exploitation
   - Déterminer les points vulnérables (qui permettent de contourner les mesures de protection et d'exploiter un accès normalement interdit), y compris les réseaux et les dispositifs sans fil.

e) Activités d'exploitation
   - Déterminer le degré d'exploitation en procédant à la totalité ou à une partie des activités suivantes :
     - Mettre à niveau l'accès à l'administrateur ou au répertoire central;
     - Installer une porte dissimulée;
     - Installer un renifleur de réseau;
     - Examiner l'information essentielle d'un dispositif de réseau;
     - Utiliser un dispositif de réseau en guise de « tremplin »;
     - Télécharger un dossier-signet.

Méthodologie

Conformément aux directives du Conseil du Trésor sur la vérification interne, une assurance sera fournie par le biais d'entrevues avec le personnel qui s'occupe de STI ou qui est visé par la STI à l'échelle nationale, régionale et locale. On procédera à des examens et à des échantillonnages de la documentation (p. ex., politiques/procédures relatives à la STI, registres de coupe-feu, évaluations de la menace et des risques, autorisations de sécurité, rapports d'intervention en cas d'incident, etc.).

Les SVIGR prévoient effectuer cette vérification comme suit :
Phase I – 3e trimestre (03/04); Phase II – 4e trimestre (03/04); Phase III – 1er trimestre (04/05).

Les SVIGR collaboreront étroitement avec les Systèmes pour veiller à ce que des mesures de protection appropriées soient en place au moment des évaluations des vulnérabilités internes et externes.

Annexe B

Plans d'action de la direction

* Indique une mesure qui sera mise en œuvre en fonction de la disponibilité du financement. Des stratégies de remplacement seront élaborées dans l'éventualité où le financement ne serait pas disponible.

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Phase I			
Recommandation n° 1 : Il est recommandé que le nom ou le titre et le mandat du Comité directeur du cadre de gestion de la protection des renseignements personnels (CDCGPRP) soient élargis pour englober la sécurité.	À l'occasion de la présentation du CPO en juin dernier, la sécurité a été ajoutée aux responsabilités du CDCGPRP. La Direction générale de la gestion moderne et des politiques (PGSP) s'interroge quant à savoir si la sécurité sera officiellement comprise dans le mandat du cadre de gestion de la protection des renseignements personnels. Nada Semaan abordera la question à la prochaine réunion du CDCGPRP. De plus, la Direction générale des systèmes a entrepris un examen complet de toutes les structures de régie, y compris les structures internes de la Direction générale, en plus de vérifier que tous les liens sont établis avec les structures de régie ministérielle.	31 mars 2005	DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 2 : Il est recommandé que le comité de gestion de la sécurité de la technologie de l'information : a) produise un énoncé de stratégie/vision en matière de STI approuvé par le ministère; b) rédige des procès-verbaux et comptes rendus de décisions; c) se réunisse tous les trois mois; d) relève du CDCGPRP.	a) - d) Les ordres du jour et les procès-verbaux des réunions sont accessibles aux fins d'un examen à toutes les parties au sein du ministère. Les réunions se tiennent à la demande des coprésidents ou du secrétaire de séance à chaque trimestre ou plus fréquemment, au besoin. Les structures de prise de décision et de production de rapports font actuellement l'objet d'un examen par les gestionnaires de la Direction des services techniques (DST). Les résultats seront divulgués une fois l'examen terminé et les processus et structures de production des rapports établis. Architecture et génie participera à l'élaboration des énoncés de vision et de stratégie. De plus, la Direction générale des systèmes a entrepris un examen complet de toutes les structures de régie, y compris les structures internes de la Direction générale, en plus de vérifier que tous les liens sont établis avec les structures de régie ministérielle.	Mars 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
Recommandation n° 3 : Il est recommandé que : a) le Ministère confie à une entité de régie appropriée (p. ex., le CGSTI, le CDCGPRP, etc.) la responsabilité d'approuver les politiques en matière de STI; b) les Systèmes présentent les « ÉBAUCHES » des politiques en matière de STI à cette entité de régie pour approbation.	a) - b) La Direction générale des systèmes procède actuellement à l'examen des structures de régie, y compris le CGSTI, et travaille à l'élaboration d'un processus qui permettra de recourir aux autorités appropriées lorsque différents moyens d'action doivent être approuvés. Jusqu'à maintenant, plusieurs ébauches de politiques ont été élaborées. Des mesures ont été prises afin de peaufiner et de mettre à jour ces politiques, au besoin. Chacune des ébauches de politique sera soumise au processus d'approbation.	Mars 2005	DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 et DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 4 : Il est recommandé que les Systèmes, en collaboration avec les régions, déterminent les besoins en matière de politiques et de procédures de STI et élaborent des politiques et procédures nationales en conséquence.	La Direction générale des systèmes va de l'avant avec un cadre de politiques national complet en matière de TI, qui permet d'établir les politiques de sécurité de la TI comme un élément essentiel aux activités de la Direction générale des systèmes. Ce cadre englobe la structure nationale de DSC, qui comprend les régions. Un cadre et une politique sur la sécurité de la TI ont été présentés au Comité de gestion supérieure (CGS) et au Comité de gestion collective (CGC) en octobre 2004.	Mars 2005	DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 et DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705
Recommandation n° 5 : Il est recommandé que les Systèmes élaborent un plan (comprenant les ressources) à l'intention du groupe responsable du contrôle de la protection de l'information (CPI).	Le Centre de protection de l'infrastructure (CPI) a été créé en octobre 2003 pour diriger les activités de dépannage des Opérations de l'AC en matière de virus à l'échelle nationale. Les ressources du centre proviennent exclusivement de l'AC; toutefois, le centre compte beaucoup sur la collaboration des ressources régionales pour remédier aux intrusions de virus lorsqu'elles se produisent. Après une année de fonctionnement, l'AC reconnaît la nécessité d'examiner le rôle du CPI – en ce qui concerne les fonctions, les outils et les niveaux de ressources – afin que le réseau informatique de DSC et de RHDCC soit sécuritaire. Grâce à l'expérience acquise jusqu'à maintenant, nous comprenons qu'une collaboration plus étroite entre les ressources de l'AC et des régions est essentielle afin de protéger comme il se doit le réseau de DSC et de RHDCC. À cette fin, le CPI élaborera un plan d'action en collaboration avec les groupes régionaux responsables de la sécurité de la TI au cours du dernier trimestre de l'exercice en cours.	Dernier trimestre de 2004-2005	DG princ., Opérations - Dave Holdham 934-0341 Mike Snider 997-8118

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
* **Recommandation n° 6 :** Il est recommandé que les Systèmes continuent de tester avec toute la diligence possible les plans de continuité des activités :	Au cours du présent exercice, certains PCO ont été mis à l'essai, alors que d'autres sont en voie d'élaboration :	Printemps 2005	
a) de toutes les applications logicielles essentielles à la mission [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*];	a) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] Des serveurs supplémentaires seront offerts avant la fin de l'année financière. Deux exercices sont prévus cette année : un exercice sur papier, en novembre, et une reprise complète au printemps.		DG princ., Opérations - Dave Holdham 934-0341 Réjean Poitras 994-4183
b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*].	b) Un PCO exhaustif a été mis à exécution [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] en mai 2004 [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]. L'exercice a été couronné de succès. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*]		DG princ., Opérations - Dave Holdham 934-0341 Réjean Poitras 994-4183

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 7 : Il est recommandé que les Systèmes, en collaboration avec l'agent de sécurité du ministère, établissent des critères et bases de référence spécifiques qui permettraient de déterminer dans quelles circonstances une évaluation de la menace et des risques (EMR) doit être réalisée.	Les SSTI travailleront en collaboration avec l'agent de sécurité du ministère afin d'élaborer les critères et les bases de références d'une EMR, qui seront inclus dans le modèle de processus de sécurité de la TI.	Mars 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705
Recommandation n° 8 : Il est recommandé que les Systèmes, en collaboration avec l'agent de sécurité du ministère, définissent clairement ce qui constitue un incident se rapportant à la STI et fassent connaître cette définition à tout le personnel.	Les Services techniques nationaux (STN) sont représentés au sein du CGSTI. Des lignes directrices sur la conduite des enquêtes administratives ont été élaborées et tiennent compte des incidents se rapportant à la sécurité de la TI. Les Ressources humaines ont transmis ces lignes directrices à toutes les régions. Les SSTI élaboreront des définitions et les soumettront au CGSTI à des fins d'examen et d'approbation; on estime cependant que les définitions normalisées pour le gouvernement du Canada devraient être établies par le Conseil du Trésor.	Mars 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., Opérations - Dave Holdham 934-0341 Mike Snider 997-8118 et ASM, DGFA - André Lefebvre 997-1935

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 9 : Il est recommandé que les Systèmes : a) adoptent le modèle de STI des Services de sécurité de la technologie de l'information (SSTI); b) mettent à jour leur page Web portant sur le cycle de vie d'un projet afin de tenir compte des nouvelles exigences en matière de STI.	a) La Sécurité de la TI travaille à l'intégration du modèle de TI des SSTI dans le CDS et le CVP. b) Le Bureau de gestion de projet des Systèmes fera référence au processus de la sécurité de la TI dans les mises à jour du cycle de vie d'un projet.	En cours En cours	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 DG princ., PGSP - Nada Semaan 997-1620 P. Charlsworth 953-3159
Recommandation n° 10 : Il est recommandé que les Systèmes réactivent le comité d'examen des projets (ou un mécanisme de régie semblable) pour veiller au respect des exigences en matière de STI.	Le cadre du CEP a été présenté au CGS et au CGC, et approuvé par ceux-ci. La première réunion a eu lieu en octobre 2004.	Octobre 2004	SMA, Systèmes - Serge Rainville 997-6481 Ron Ramsey 997-8037

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
* **Recommandation n° 11 :** Il est recommandé que les Systèmes établissent la version définitive d'un programme ministériel de sensibilisation à la sécurité de la technologie de l'information et le mettent en œuvre à l'échelle nationale.	Les SSTI tiennent actuellement des consultations avec des experts régionaux et nationaux en la matière, puisque nous commençons, en collaboration avec le CPI et les régions, la mise en œuvre d'un programme de sensibilisation à la sécurité destiné à différentes organisations dont la taille est semblable à celle de DSC et de RHDCC. Remarque : DSC ne possède plus de structure régionale depuis que les régions relèvent des Systèmes nationaux.	Mars 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 SMA, Systèmes - Serge Rainville 997-6481 Ron Ramsey 997-8037
Recommandation n° 12 : Il est recommandé que l'agent de sécurité du ministère et l'agent de sécurité régional de l'Ontario mettent à jour les autorisations de sécurité pour la région de l'Ontario.	La Sécurité régionale est responsable des autorisations de sécurité de ses employés. L'agent de sécurité du ministère, sur les conseils des agents de sécurité régionaux, détient l'autorité finale pour accorder, révoquer ou refuser une cote de fiabilité. Le processus relatif aux cotes de fiabilité nécessite qu'une vérification du casier judiciaire soit effectuée par la GRC (le corps de police choisi par le SCT). Si la GRC demande l'identification formelle d'un employé (candidat), celui-ci devra fournir ses empreintes digitales au corps policier qui en fera l'analyse. Actuellement, le délai de traitement de la GRC est de 180 jours. La haute direction a été informée de la situation et elle est avisée de tout changement concernant les délais de traitement de la GRC.	Terminé	ASM, SFA - André Lefebvre 997-1935

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 13 : Il est recommandé que l'agent de sécurité du ministère et les agents de sécurité régionaux : a) déterminent si les fonctionnaires provinciaux qui ont accès à l'information ministérielle (en d'autres termes, à l'information du gouvernement du Canada) ont les autorisations de sécurité nécessaires; b) si tel n'est pas le cas, qu'ils déterminent les mesures correctives à prendre.	a) - b) Les gouvernements provinciaux ne disposent pas de systèmes d'autorisation de sécurité pour leurs employés. Dans les centres où les locaux sont partagés avec des employés des gouvernements provinciaux, on rappelle souvent aux employés fédéraux qu'ils doivent utiliser les mesures de protection appropriées relativement aux renseignements protégés et classifiés. Il faut notamment s'abstenir d'échanger des renseignements protégés ou classifiés contenus dans les banques de données fédérales et s'assurer que de tels documents sont entreposés et manipulés conformément aux politiques du ministère et du SCT. Cette question a fait l'objet de discussions au sein du Comité du groupe de travail sur l'intégrité du ministère et a été portée à l'attention de la haute direction.	Terminé	ASM, FSA - André Lefebvre 997-1935
Recommandation n° 14 : Il est recommandé que le formulaire ADM 5017 du ministère, Certificat de fin d'emploi, soit révisé pour veiller à ce que « l'accès logique » d'un employé qui quitte le ministère soit verrouillé.	Le Certificat de fin d'emploi sera modifié afin d'inclure le verrouillage de l'accès aux systèmes ministériels.	Fin de l'exercice 2004-2005	ASM, SFA - André Lefebvre 997-1935

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 15 : Il est recommandé que les Systèmes : a) vérifient [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]; il est recommandé que les Systèmes : b) mettent en place des pistes de vérification pour contrôler [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] à l'intérieur du système et s'assurent que [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] qui ont accès à des données sur les clients ont les autorisations de sécurité appropriées.	a) et b) Les Systèmes se sont assurés qu'on ne peut en aucune façon [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]. L'accès est impossible sur le plan technique; par conséquent, les listes de contrôle ne sont pas requises.	Terminé	DG princ., DST - Dave Adamson 956-5487 Pierre Lafrance 953-0702

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 16 : Il est recommandé que les Systèmes adoptent une politique/directive stipulant que seule la technologie autorisée par le ministère (p. ex. les serveurs) peut être connectée au réseau, et qu'ils veillent à son application. **Identique à la Recommandation n° 1(c) — Phase II – Sous-ensemble de la Recommandation n° 4**	Des politiques sur l'utilisation du réseau sont actuellement en place. De plus, dans le cadre des initiatives de renouvellement des politiques de la Direction générale, toutes les politiques seront passées en revue afin de s'assurer que des plans de contrôle sont en place afin de soutenir ces politiques. Toutes les politiques à venir doivent comprendre des plans de contrôle.	Mars 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
Recommandation n° 17 : Il est recommandé que les Systèmes adoptent une politique ou une directive stipulant que tous les ordinateurs du personnel doivent être protégés et que des mesures doivent être prises pour empêcher le public d'y avoir accès.	Les Systèmes sont d'accord avec cette recommandation et s'assureront que le nouveau mécanisme de haut niveau relatif à la politique de sécurité de la TI du ministère prévoit cette mise en œuvre. Un document préliminaire doit être élaboré d'ici la fin du présent exercice.	Mars 2005	DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 et DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705
Recommandation n° 18 : Il est recommandé que les Systèmes fassent régulièrement des tests de pénétration interne et externe pour le réseau du ministère.	Les SSTI font des tests périodiques sur les systèmes nouveaux et existants dans le cadre d'un processus d'évaluation de la vulnérabilité, en faisant appel à des ressources internes et externes ainsi qu'aux programmes et aux outils les plus modernes et les plus sophistiqués pour faire en sorte d'avoir en place les meilleurs processus qui soient.	[L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
* **Recommandation n° 19 :** Il est recommandé que les Systèmes adoptent une politique et prévoient une solution technique pour veiller à ce que la norme gouvernementale concernant les mots de passe soit respectée.	La politique relative aux mots de passe fait présentement l'objet d'un examen par le CGSTI. Cette politique sera également soutenue par [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.].	Mars 2006	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
Recommandation n° 20 : Il est recommandé que les Systèmes adoptent une solution technique pour réduire le nombre de mots de passe dont les employés ont besoin pour accéder à de multiples systèmes.	Un projet a été proposé dans le but d'instaurer un processus qui servira à élaborer et à mettre en œuvre [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] afin de suivre cette recommandation. (Même produit que pour la Recommandation n° 19) • [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.]* • Les Opérations de TI travailleront en collaboration avec le groupe Architecture et génie afin de mettre en œuvre la phase II lorsque le projet aura été financé et structuré.	Mars 2006 Phase I terminée	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et René Lalande 997-8693

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 21 : Il est recommandé que les gestionnaires de centres de responsabilité s'assurent que leurs [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] soient traitées dans les deux semaines suivant leur réception et qu'ils les retournent promptement aux CTI.	La Direction générale des systèmes approuve cette recommandation et redoublera d'efforts afin d'effectuer régulièrement des suivis avec les CTI dans le but de s'assurer que tout est exécuté en temps opportun.	En cours	DG princ., Opérations - Dave Holdham 934-0341 Guy Belleperche 997-4115
Recommandation n° 22 : Il est recommandé que les Systèmes examinent la possibilité d'afficher [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] sur un site Web.	Les Systèmes examineront la possibilité d'afficher [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]. La date cible pour l'étude de faisabilité a été fixée au mois d'avril 2005.	Avril 2005 (étude)	DG princ., Opérations – Dave Holdham 934-0341 Guy Belleperche 997-4115 et René Lalande 997-8693
Recommandation n° 23 : Il est recommandé que les Systèmes et les régions limitent l'accès à leurs centres de solution aux seules personnes qui en ont besoin.	[L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	Terminé	SMA, Systèmes - Serge Rainville 997-6481 Ron Ramsey 997-8037 et DG princ., Opérations - Dave Holdham 934-0341 R. Poitras 994-4183

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Recommandation n° 24 : Il est recommandé que les Systèmes établissent des paramètres aux fins de l'évaluation de l'efficacité de la STI.	Les Systèmes appuient cette recommandation et établiront des paramètres afin de soutenir le processus de la STI. (Outil d'autoévaluation du SCT visant à évaluer la conformité)	Septembre 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705
Phase II			
Les recommandations suivantes ont été formulées :			
1(a) Tous les systèmes d'exploitation (SE), les hôtes et les serveurs sur lesquels les ensembles de service et les correctifs de sécurité les plus récents n'ont pas été installés doivent être mis à jour *(découverte du réseau et des services et évaluation de la vulnérabilité du réseau)*.	1(a) Les Systèmes travaillent continuellement à relever tous les dispositifs connectés au réseau et à leur apporter des correctifs. Étant donné le rôle essentiel que jouent certaines des applications hébergées relativement à la prestation des services, certains correctifs nécessitent une mise à l'essai approfondie avant d'être mis en œuvre dans l'environnement de production. Le fait que bon nombre de ces hôtes soient situés dans des segments protégés du réseau atténue le risque que la mise en œuvre des correctifs et des ensembles de service soit retardée.	1(a) Terminé	DG princ., Opérations - Dave Holdham 934-0341 Guy Belleperche 997-4115
1(b) Les hôtes ou les serveurs qui n'ont pas été soumis au balayage [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] doivent également être évalués et mis à jour, au besoin (*évaluation de la vulnérabilité du réseau)*.	1(b) Le rapport de vérification ne mentionne pas d'hôtes ou de serveurs spécifiques qui n'étaient pas inclus dans le balayage. Tous les systèmes doivent régulièrement faire l'objet d'un balayage.	1(b) Terminé	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
1(c) Les hôtes et les serveurs [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] doivent être évalués afin de déterminer s'il est nécessaire de conserver ce [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(découverte du réseau et des services et évaluation de la vulnérabilité du réseau)*. **Identique à la Recommandation n° 16 — Phase I**	1(c) Les Systèmes ont l'intention de [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] dans le cadre de leurs activités régulières. Un plan est en place afin d'inventorier et d'analyser le matériel actuel et les serveurs [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]. Une approche facilitant la mise à niveau a été déterminée lorsqu'il était possible de le faire, et une analyse approfondie est requise pour les logiciels de tiers exploités sur ces serveurs. Malheureusement, aucun financement n'a été accordé pour ce projet jusqu'à maintenant.	1(c) Terminé	DG princ., Opérations - Dave Holdham 934-0341 René Lalande 997-8693
1(d) Il faut rendre plus difficile l'installation de logiciels afin d'améliorer la sécurité du réseau (*évaluation de la vulnérabilité du réseau*). **Identique à la Recommandation n° 2(c) — Phase II (ci-dessous)**	1(d) Il est clair que cette recommandation concerne le renforcement des plates-formes et des applications. Des processus ont été adoptés pour l'installation de différentes composantes visant à renforcer la sécurité de toutes les versions de serveur. Le processus de demande d'installation de composantes (DIC) pour les versions de serveur comprend bon nombre d'éléments recommandés à l'heure actuelle [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.], par les pratiques exemplaires de l'industrie et par les organismes responsables. Les normes de renforcement sont établies par le BPR responsable et appliquées de façon universelle à moins que des exemptions ne soient accordées par la direction.	1(d) En cours	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 René Lalande 997-8693 et DG princ., Solutions clients - Ron Meighan 994-0749

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
1(e) Les politiques relatives à la règle d'affectation des noms doivent être intensifiées afin d'empêcher la divulgation involontaire de renseignements qui pourraient intéresser un utilisateur non autorisé *(découverte du réseau et des services).* **Identique à la Recommandation n° 2(c) de la Phase II**	1(e) Les Systèmes soutiennent pleinement la mise en œuvre d'une règle d'affectation des noms non descriptive pour tous les biens exposés sur des réseaux internes ou externes. Les Systèmes s'assureront que le nouveau mécanisme de haut niveau relatif à la politique de sécurité de la TI du ministère prévoit cette mise en œuvre. Un document préliminaire devrait être rédigé d'ici la fin du présent exercice.	1(e) Question stratégique : Mars 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 et DG princ., Solutions clients - Ron Meighan 994-0749
1(f) Des balayages réguliers des services et de la découverte du réseau doivent être effectués afin d'assurer la configuration appropriée des réseaux, des hôtes et des services de DRHC *(découverte du réseau et des services)*.	1(f) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	1(f) En cours [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] : 4e trimestre – si les plates-formes sont prêtes.	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., Opérations - Dave Holdham 934-0341 Guy Belleperche 997-4115 et DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579
1(g) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(découverte du réseau et des services)*.	1(g) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] d'ici la fin de l'année financière et assureront une coordination continue en collaboration avec les groupes de soutien régionaux de niveau 2.	1(g) Mars 2005	DG princ., Opérations - Dave Holdham 934-0341 Guy Belleperche 997-4115

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
1(h) Des évaluations de la vulnérabilité doivent être effectuées régulièrement afin de s'assurer que les systèmes sont à jour et sécuritaires (*évaluation de la vulnérabilité du réseau*).	1(h) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	1(h) En cours	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705
Les recommandations suivantes ont été formulées :			
2(a) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(découverte du réseau et des services et évaluation de la vulnérabilité du réseau).* **Identique à la Recommandation n° 2(b) — Phase III**	2(a) Les SSTI et le groupe Architecture et génie approuvent la recommandation et travailleront en collaboration avec les Opérations et les Applications afin de s'assurer que la connectivité entre le matériel du réseau respecte les exigences établies en matière de sécurité pour le chiffrement des données, et ce, en utilisant des outils dont l'usage a été approuvé par les organismes responsables du gouvernement du Canada et les pratiques standard de l'industrie lorsqu'il est utile et possible de le faire. Des technologies appropriées existent et sont mises en œuvre au fur et à mesure que des besoins sont déterminés.	2(a) En cours Nouvelles mises en œuvre lorsqu'elles surviennent, mises à niveau lorsqu'elles sont déterminées.	DG princ., DST- Dave Adamson 956-5487 Dave Beach 956-9705
2(b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(découverte du réseau et des services et évaluation de la vulnérabilité du réseau)*. **Identique à la Recommandation n° 2(e) — Phase II (ci-dessous)**	2(b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	2(b) En cours	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 Nicole Gratton 956-8579 et DG princ., Opérations de TI - Dave Holdham 934-0341

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
2(c) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(découverte du réseau et des services et évaluation de la vulnérabilité du réseau)*. **Identique à la Recommandation 1 d) — Phase II**	2(c) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	2(c) Mars 2005	DG princ., DST - Dave Adamson 956-5487 René Lalande 997-8693
2(d) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(découverte du réseau et des services et évaluation de la vulnérabilité du réseau)*. **Identique à la Recommandation 2 e) — Phase II (ci-dessous)**	2(d) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	2(d) Ordinateurs de bureau d'ici mars 2005; autres plates-formes à suivre.	DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
2(e) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(découverte du réseau et des services et évaluation de la vulnérabilité du réseau)*. **Identique à la Recommandation n° 2(d) — Phase II (qui précède)**	2(e) Les SSTI travaillent en collaboration avec les gestionnaires des produits et des plates-formes afin de mettre en œuvre des principes de renforcement. Cette recommandation sera prise en compte dans le cadre de ces efforts. Le travail de renforcement touchera d'abord les ordinateurs de bureau standard du ministère puis les autres plates-formes. Les gestionnaires des produits ou des plates-formes en seront responsables.	2(e) Ordinateurs de bureau d'ici mars 2005; autres plates-formes à suivre.	DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579
2(f) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] (*découverte du réseau et des services et évaluation de la vulnérabilité du réseau)*.	2(f) Les SSTI travaillent en collaboration avec les gestionnaires des produits et des plates-formes afin de mettre en œuvre des principes de renforcement. Cette recommandation sera prise en compte dans le cadre de ces efforts. Le travail de renforcement touchera d'abord les ordinateurs de bureau standard du ministère puis les autres plates-formes. Les gestionnaires des produits ou des plates-formes en seront responsables.	2(f) Ordinateurs de bureau d'ici mars 2005; autres plates-formes à suivre.	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 Autres directeurs, A et G

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Les recommandations suivantes ont été formulées :			
3(a) La politique de 2001 sur les coupe-feu (y compris les appendices) doit être examinée et mise à jour (au besoin) afin de tenir compte des services offerts actuellement sur les coupe-feu, et publiée dans un format plus officiel *(évaluation des règles sur les coupe-feu)*.	3(a) Les Systèmes approuvent cette recommandation. Ils prendront les mesures qui s'imposent et mettront à jour la politique actuelle sur les coupe-feu afin de tenir compte des environnements actuels et N+1.	3(a) Décembre 2004	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
3(b) DRHC devrait examiner régulièrement les règles de trafic concernant le personnel de soutien et s'assurer qu'une procédure de gestion des changements appropriée est en place afin de conserver une liste à jour et exacte *(évaluation des règles sur les coupe-feu)*.	3(b) Les Systèmes continuent d'offrir un soutien technique et un soutien d'ingénierie permanents aux équipes responsables du soutien des coupe-feu et de l'application des règles.	3(b) En cours	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705
3(c) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(évaluation des règles sur les coupe-feu)*.	3(c) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	3(c) En cours	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
3(d) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(évaluation des règles sur les coupe-feu)*.	3(d) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	3(d) En cours	DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579 et DG princ., Opérations Dave Holdham 934-0341 Rocky Kreis 953-4470
Les recommandations suivantes ont été formulées :			
4(a) DRHC doit examiner sa politique actuelle sur les mots de passe, y compris son application sur le plan technique, et la mettre à jour en apportant les changements requis afin d'assurer un processus de sélection des mots de passe fiable *(évaluation des mots de passe)*.	4(a) Les SSTI ont présenté des outils d'intervention, sous forme d'ébauche, au CGSTI à des fins d'examen et d'approbation concernant l'utilisation des mots de passe permettant d'accéder au réseau interne du ministère. Pour ce qui est des considérations techniques, consulter la Recommandation n° 19 de la phase I.	4(a) Mars 2006	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
4(b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(évaluation des mots de passe)*.	4(b) Le groupe Architecture et génie approuve cette recommandation et appuie l'examen des mots de passe utilisés sur les autres systèmes du ministère afin de s'assurer qu'ils sont conformes aux pratiques exemplaires et aux normes du ministère et de l'industrie. Des processus, des procédures et des délais seront fournis par la Sécurité de la TI. Ces activités seront mises en œuvre dans le cadre des évaluations périodiques de la vulnérabilité décrites à la Recommandation n° 18 de la phase I.	4(b) Un calendrier sera publié d'ici janvier 2005.	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
4(c) Une évaluation régulière des mots de passe doit être effectuée afin de s'assurer que la politique sur les mots de passe est respectée *(évaluation des mots de passe).*	4(c) Le groupe Architecture et génie approuve cette recommandation et appuie l'examen des mots de passe utilisés sur les autres systèmes du ministère afin de s'assurer qu'ils sont conformes aux pratiques exemplaires et aux normes du ministère et de l'industrie. Des processus, des procédures et des délais seront fournis par la Sécurité de la TI. Ces activités seront mises en œuvre dans le cadre des évaluations périodiques de la vulnérabilité décrites à la Recommandation n° 18 de la phase I. Les Opérations de TI sont d'accord; elles procéderont à cette évaluation.	4(c) Mars 2006	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705
4(d) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(évaluation des mots de passe).*	4(d) Les SSTI travaillent en collaboration avec les gestionnaires des produits et des plates-formes afin de mettre en œuvre des principes de renforcement. Cette recommandation sera prise en compte dans le cadre de ces efforts. Le travail de renforcement touchera d'abord les ordinateurs de bureau standard du ministère puis les autres plates-formes. Les gestionnaires des produits ou des plates-formes en seront responsables.	4(d) Ordinateurs de bureau d'ici mars 2005; autres plates-formes à suivre.	DG princ., Opérations - Dave Holdham 934-0341 G. Belleperche 997-4115
4(e) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] *(évaluation des mots de passe).*	4(e) Les SSTI travaillent en collaboration avec les gestionnaires des produits et des plates-formes afin de mettre en œuvre des principes de renforcement. Cette recommandation sera prise en compte dans le cadre de ces efforts. Le travail de renforcement touchera d'abord les ordinateurs de bureau standard du ministère puis les autres plates-formes. Les gestionnaires des produits ou des plates-formes en seront responsables.	4(e) Ordinateurs de bureau d'ici mars 2005; autres plates-formes à suivre.	DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
Les recommandations suivantes ont été formulées :			
5(a) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(a) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(a) Décembre 2004	DG princ., DST - Dave Adamson 956-5487 Brian Graham 994-3822
5(b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(b) Aucune planification pour le moment.	DG princ., DST - Dave Adamson 956-5487 Brian Graham 994-3822
5(c) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(c) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(c) La date de mise en œuvre sera déterminée en fonction des résultats.	DG princ., Opérations - Dave Holdham 934-0341 Rocky Kreis 953-4470
5(d) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(d) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	5(d) À déterminer	DG princ., DST - Dave Adamson 956-5487 N. Gratton 956-8579
Les recommandations suivantes ont été formulées :			
* 1. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	Le groupe Architecture et génie approuve cette recommandation lorsqu'il est utile et possible de l'appliquer, et prévoira à cet égard un poste budgétaire hors bilan.	Mars 2005	DG princ., DST- Dave Adamson 956-5487 Dave Beach 956-9705

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
2. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	Les SNVD offrent actuellement un [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] pour l'accès à distance des employés, lequel répond aux exigences énoncées.	En cours	DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579
3. La politique de DRHC sur les dispositifs mobiles doit être mise à jour afin de tenir compte des questions se rapportant à l'installation de logiciels par les utilisateurs, à la navigation sur le Web à des fins personnelles et à la mise à niveau des logiciels à l'aide des correctifs et des ensembles de service les plus récents, etc. (*examen de la politique sur les dispositifs mobiles).*	La Direction générale des systèmes convient qu'il est important de tenir compte de ces questions. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] De plus, même si la nouvelle directive relative à la politique sans fil n'aborde pas directement les questions résiduelles, un certain nombre d'autres politiques et initiatives le font, y compris la politique sur l'utilisation du réseau électronique. Toutefois, reconnaissant l'importance de ces questions, la Direction générale des systèmes les abordera à la prochaine itération de la directive relative à la politique sur les dispositifs sans fil ou de directives connexes.	31 mars 2005	DG princ., DST - Dave Adamson 956-5487 Bob Cloutier 953-3938 et DG princ., PGSP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
PHASE III			
a) **Regroupement des serveurs externes** [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	[L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	31 mars 2005 La date de mise en œuvre sera déterminée selon les résultats.	DG princ., DST- Dave Adamson 956-5487 Brian Graham 994-3822 et DG princ., Opérations - Dave Holdham 934-0341 G. Belleperche 997-4115

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
b) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	[L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	30 septembre 2005 La date de mise en œuvre sera déterminée selon les résultats.	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., Opérations - Dave Holdham 934-0341 G. Belleperche 997-4115
c) **Correction des systèmes vulnérables** Mettre à l'essai et appliquer les nouveaux correctifs le plus rapidement possible, d'abord aux systèmes essentiels, puis à tous les autres systèmes. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	Le groupe Architecture et génie doit mettre au point et examiner les protocoles de gestion des correctifs, les examens de laboratoire, les processus, les procédures et les délais. Les Opérations de TI testent et appliquent les nouveaux correctifs le plus rapidement possible, d'abord aux systèmes essentiels, puis à tous les autres systèmes. Consulter la Phase II (1a) et la Recommandation n° 16 de la Phase I.	31 mars 2005 La date de mise en œuvre sera déterminée selon les résultats.	DG princ., DST - Dave Adamson 956-5487 Brian Graham 994-3882 et DG princ., Opérations - Dave Holdham 934-0341 Rocky Kreis 953-4470

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
d) **Protection par mot de passe** [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] Élaborer un programme de sensibilisation à l'intention des utilisateurs, comprenant des directives pour réduire la réutilisation des mots de passe, particulièrement entre des systèmes de partitions différentes, et qui utilisent des protocoles d'authentification différents (p. ex., entre des services de messagerie électronique et des applications intranet sensibles). Une politique sur les mots de passe suffisamment rigoureuse devrait également être établie dans tous les systèmes. Les détails précis de cette politique devraient être déterminés dans le contexte d'une évaluation de la menace et des risques.	Concevoir, élaborer et exploiter le paradigme de gestion des identités au moyen d'un calendrier. Le SSE doit mettre en œuvre le paradigme lorsque le calendrier relatif à la sécurité de la TI sera établi. Consulter la Recommandation n°19 de la Phase I.	Mars 2006 La date de mise en œuvre sera déterminée selon les résultats.	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., Opérations - Dave Holdham 934-0341 G. Belleperche 997-4115

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
e) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	[L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	30 juin 2005 En cours	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., Solutions clients - Ron Meighan 994-0749 Alain Lemay 994-0426
f) * [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	Concevoir, mettre en œuvre et exploiter la stratégie des enclaves de zone conformément au document sur les exigences des zones de base du CST.	31 mars 2006	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., Opérations - Dave Holdham 934-0341 Guy Belleperche 997-4115

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
g) **Programme de sensibilisation à la sécurité à l'intention des utilisateurs** Élaborer un programme de sensibilisation à l'intention des utilisateurs, afin d'aborder certaines des questions soulevées dans ce rapport et de désigner des personnes-ressources auxquelles il est possible de signaler les problèmes qui peuvent indiquer des brèches de sécurité. Les programmes de sensibilisation sur la façon de gérer les courriels non désirés et les courriels qui contiennent des pièces jointes de nature douteuse sont particulièrement importants. [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	La Direction générale des systèmes élaborera et donnera des séances d'éducation et de sensibilisation plus poussées, en assurera l'efficacité et les peaufinera, au besoin. Les Services de formation en informatique (SFI) travailleront en collaboration avec les SSTI une fois que les besoins en matière de formation seront déterminés.	30 juin 2005 Le résultat sera ensuite mis en œuvre.	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., PGSP - Nada Semaan, 997-1620 Rosa Gavillucci 994-1465

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
h) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	[L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] Il faudra tenter de régler ce problème. La solution sera ensuite mise en œuvre par les Opérations de TI.	31 mars 2005 S'il est impossible de trouver une solution de rechange, la date cible ne pourra pas être respectée. La date de mise en œuvre sera déterminée selon les résultats.	DG princ., DST - Dave Adamson 956-5487 Brian Graham 994-3822 Nicole Gratton 956-8579 et DG princ., Opérations - Dave Holdham 934-0341 G. Belleperche 997-4115
i) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information.*] L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] La solution sera ensuite mise en œuvre par les Opérations de TI.	31 mars 2006 La date de mise en œuvre sera déterminée selon les résultats.	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et DG princ., Opérations - Dave Holdham 934-0431 G. Belleperche 997-4115

Recommandations de la DVE	Plan d'action pour la prise de mesures correctives	Date d'achèvement prévue	DG principal responsable – Nom et numéro de téléphone de la personne-ressource de la Direction
j) [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	Nous examinons actuellement des mesures et des outils de prévention afin de limiter de telles attaques. La solution sera ensuite mise en œuvre par les Opérations de TI.	Des dates doivent être déterminées une fois qu'on en saura davantage.	DG princ., DST - Dave Adamson 956-5487 Nicole Gratton 956-8579 et DG princ., Opérations - Dave Holdham 934-0431 Murray Jaques, 953-3398 ou G. Belleperche 997-4115
k) **Supprimer des bandeaux les renseignements inutiles.** [L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.]	L'information retenue peut être exemptée en vertu de l'alinéa 16(2)c) de la *Loi sur l'accès à l'information*.] La solution sera ensuite mise en œuvre par les Opérations de TI.	31 mars 2005	DG princ., DST - Dave Adamson 956-5487 Dave Beach 956-9705 et René Lalande 997-8693 et DG princ., Opérations Dave Holdham 934-0341 G. Belleperche 997-4115

Nom du document de révision : My Documents : \IT Security Audit MAP AED Version Dec 21

Présentations par :
D. Beach, N. Deslauriers, N. Gratton, B. Graham, A. Lefebvre, C. MacIntyre, R. Kries, R. Poitras,
R. Ramsay, D. Beckett, A. Lemay, R. Gavillucci, P.Charlsworth, J. Roberge, B. Cloutier, R. Lalande,
G. Belleperche, R. Meighan, M. Snider, P. Lafrance, M. Jaques