Commission de la fonction publique du Canada
Public Service Commission of Canada

COMMISSION DE LA FONCTION PUBLIQUE

RAPPORT

SUIVI DES RECOMMANDATIONS ET SUGGESTIONS DU RAPPORT DE LA GRC SUR LA SÉCURITÉ 1996

Avril 2001

Canada

TABLE DES MATIÈRES

1.0 RÉSUMÉ

La Commission de la fonction publique (CFP) a mis en oeuvre un cadre de contrôle sain pour faire en sorte que les recommandations et les suggestions du rapport présenté par l'équipe d'inspection et d'évaluation de la sécurité (EIES) de la GRC en 1996 soient suivies de manière satisfaisante. Notre conclusion est basée sur une étude de la réponse de la direction, réponse qui a été présentée officiellement par la CFP à la Direction des opérations techniques de la Sous-direction de la sécurité de la technologie de l'information de la GRC le 17 avril 1997. Elle repose également sur un examen du plan d'action et de tous les rapports d'étapes qui ont été préparés par la suite exposant l'ampleur des mesures correctives apportées.

En outre, la Commission de la fonction publique a progressé considérablement en ce qui a trait à la mise en oeuvre de la plupart des 45 recommandations et des huit suggestions contenues dans le rapport présenté par l'EIES de la GRC en 1996. Notre conclusion est basée sur un examen de l'information fournie par le personnel durant ce suivi.

Malgré les progrès considérables qui ont été faits jusqu'ici, il y a toujours des domaines où les recommandations et les suggestions restent à être mises en oeuvre. Plus précisément, dans le domaine de la sécurité de l'organisation et de la sécurité administrative, il faut traiter des questions relatives à la tenue d'une évaluation de la menace et des risques (EMR) couvrant tous les systèmes de la CFP; à la mise à jour et à l'ajustement, au besoin, du plan de reprise des activités (PRA) de la CFP**;** et à la conduite d'un examen annuel de la sécurité pour l'exercice 2001-2002. Dans le domaine de la sécurité technique, les procédures et lignes directrices doivent être finalisées et documentées; elles devraient couvrir des domaines tels que la gestion des problèmes et les processus de résolution de ceux-ci, la façon de traiter les incidents compromettant la sécurité et l'administration quotidienne des opérations de la salle des ordinateurs. Enfin, dans le domaine de la sécurité des logiciels, les recommandations ayant trait à l'identification et à la documentation des activités de surveillance des systèmes, ainsi que celles liées à la terminaison automatique ou à la réauthentification des utilisatrices et utilisateurs inactifs, nécessiteraient la prise de mesures.

La direction de la CFP doit être félicitée pour avoir fait une démarche proactive en demandant que ce suivi ait lieu dans un délai de cinq ans, soit depuis le moment où la première étude a été entreprise par l'équipe d'inspection et d'évaluation de la sécurité de la GRC en 1996. Nous voulons exprimer notre appréciation à la direction et au personnel de la Commission de la fonction publique pour leur aide et leur coopération durant ce suivi.

2.0 CONTEXTE DU SUIVI

En mai 1996, on a fait un examen du fonctionnement du réseau et des installations de soutien de la Commission de la fonction publique (CFP) au 300, avenue Laurier ouest, Ottawa (Ontario). L'examen a été mené par la Sous-direction de la sécurité de la technologie de l'information de la Gendarmerie royale du Canada (GRC) à la demande de l'agent de la sécurité adjoint du ministère (ASM) en collaboration avec le coordonnateur de la sécurité de la technologie de l'information. Le rapport présenté par l'équipe d'inspection et d'évaluation de la sécurité (EIES) de la GRC proposait 45 recommandations et huit suggestions conçues pour améliorer les pratiques de sécurité au sein de la CFP. Les secteurs fonctionnels dont il est question dans le rapport sont ceux de la sécurité organisationnelle et administrative, de la sécurité du personnel, de la sécurité physique et environnementale, de la sécurité technique et de la sécurité des logiciels.

Selon le plan de vérification et d'examen de la Commission pour l'exercice 2000-2001 et conformément à l'exigence du Secrétariat du Conseil du Trésor que tous les ministères et organismes procèdent à des vérifications et/ou des examens de la sécurité avant le 31 mars 2001, l'ASM a demandé qu'on fasse un suivi du rapport présenté par l'EIES de la GRC en 1996. afin de déterminer l'ampleur des mesures correctives nécessaires apportées en réponse aux recommandations et suggestions contenues dans le rapport.

3. 0 OBJECTIFS DU SUIVI

Le suivi du rapport présenté par l'EIES de la GRC en 1996 a pour but de fournir à la direction de la Commission de la fonction publique une évaluation indépendante et de faire rapport sur les éléments suivants :

(a) la pertinence du cadre de contrôle en vigueur portant sur :

(i) la préparation d'une réponse de la direction aux recommandations et suggestions du rapport présenté par l'EIES de la GRC en 1996;

(ii) l'élaboration d'un plan d'action approprié pour mettre en oeuvre les mesures correctives au besoin, et

(iii) la rédaction de rapports d'étapes périodiques pour faire état de la mesure dans laquelle des progrès ont été réalisés dans la mise en oeuvre du plan d'action.

(b) la mesure dans laquelle la direction de la CFP a donné suite aux recommandations et

suggestions contenues dans le rapport présenté par l'EIES de la GRC en 1996.

Les résultats de ce suivi sont présentés à la section 6.0 du présent rapport et font l'objet de deux sous-sections selon les objectifs énumérés ci-dessus. La section 6.1 porte sur l'adéquation du cadre de contrôle qui a été créé par la direction de la CFP pour donner suite aux recommandations et aux suggestions du rapport présenté par l'EIES de la GRC en 1996. La section 6.2 traite des efforts faits par la direction de la CFP afin de mettre en oeuvre ces recommandations et suggestions. Les conclusions exposées dans la section 6.2 sont regroupées selon les mêmes domaines fonctionnels que dans le rapport original de l'EIES. De plus, les conclusions font l'objet d'un renvoi précis par numéro aux recommandations et suggestions précises de l'EIES de la GRC, dans le rapport de 1996.

4.0 PORTÉE DU SUIVI

Ce suivi a eu lieu à l'administration centrale (AC) de la CFP. Il a comporté des entrevues avec le personnel de la Direction de la technologie de l'information et de la Direction des finances et de l'administration. Le suivi n'a pas été mené comme une vérification en regard de critères de vérification particuliers ni n'avait pour but d'obtenir une opinion sur la pertinence des pratiques actuelles de gestion de la sécurité à la CFP. Les résultats du suivi sont basés sur des rapports et d'autres documents pertinents qui ont été fournis par le personnel de la CFP durant la réalisation de l'exercice du suivi. Des recommandations complémentaires ont été incluses dans le rapport de suivi dans les cas où il semble que la mise en oeuvre de la ou des recommandation(s) d'origine permettrait d'améliorer les pratiques de gestion de la sécurité actuelles.

La configuration actuelle du réseau de la CFP — décrite à la section 4.0 ci-dessous — a changé depuis l'évaluation menée par l'équipe d'inspection et d'évaluation de la sécurité (EIES) en 1996. Certaines des recommandations et suggestions contenues dans ce rapport n'ont plus leur raison d'être aujourd'hui. Ces dernières sont notées au passage.

5.0 APERÇU DE LA CONFIGURATION ACTUELLE DU RÉSEAU

Au moment de l'examen de 1996, la topologie de CFP Net consistait en réseaux locaux basés sur des anneaux à jeton interconnectés au moyen d'une artère principale avec divers services reliés directement à ce réseau tels que l'ordinateur principal des SGTI et les serveurs Novell et UNIX organisés en réseau local situés sur divers étages. L'artère principale consistait en trois routeurs Proteon à haute vitesse de modèle CNX600 interreliés. Depuis l'examen de 1996, la configuration physique des contrôleurs réseau, les services de communication, le matériel et les logiciels ont été améliorés. Le réseau Ethernet de la CFP consiste en ports de commutation de Cisco Systems qui assurent une capacité de

commutation à haute vitesse ayant la variabilité dimensionnelle, le rendement et la gérabilité qui permettent de répondre aux besoins de réseautage actuels et futurs. Présentement, le principal commutateur est un Catalyst 5509 multicouches qui sert d'artère principale à Ethernet. Les détails en ce qui a trait à la nouvelle configuration sont exposés dans un rapport intitulé *GTIS - PSC Managed Bandwidth Service, Detailed LAN Architecture Paper - Version 1.0* daté du 17 avril 2000 et rédigé par GE Capital IT Solutions Canada.

Au moment où a lieu ce suivi, la pièce où se trouvent le processeur et le serveur (P100) est toujours le sous-sol de L'Esplanade Laurier. Cependant, le personnel de la salle des ordinateurs a depuis été relogé au 14e étage. La pièce P100 sert maintenant en partie de laboratoire d'assurance de la qualité pour l'essai et la distribution de nouvelles applications.

6.0 RÉSULTATS DÉTAILLÉS DU SUIVI

6.1 Pertinence du cadre de contrôle de la CFP

Un cadre de contrôle pertinent a été mis en application par la direction de la CFP pour s'assurer que l'on donnerait vraiment suite aux recommandations et suggestions du rapport présenté par l'EIES de la GRC en 1996. Notre conclusion est basée sur les faits suivants :

- un plan d'action détaillé a été élaboré et soumis par la CFP à la Direction des opérations techniques, Sous-direction de la sécurité de la technologie de l'information, GRC le 17 avril 1997;
- le plan d'action a été coordonné par l'analyste principal de la sécurité de la CFP; il regroupait chacune des 45 recommandations et des huit suggestions sous forme de projets portant des titres et descriptions connexes;
- on avait attribué un niveau de priorité à chacun des regroupements de projets;
- un bureau de première responsabilité a été identifié pour la mise en oeuvre des mesures correctives nécessaires pour chacun des regroupements de projets;
- le plan d'action contenait un tableau relatif aux ressources appropriées qui consistait en échéances ou dates repères ainsi que les ressources qu'on comptait utiliser pour donner suite aux recommandations se rapportant à chaque regroupement de projets;

- le plan d'action a été approuvé par le vice-président, Direction générale de la gestion ministérielle et la secrétaire générale;

- des rapports d'étapes ont été préparés périodiquement par l'analyste principal de la sécurité; il a exposé clairement les progrès réalisés durant des périodes choisies ainsi que toute nouvelle priorité à prendre en compte.

Recommandations complémentaires :

Aucune.

6.2 Étendue des progrès réalisés

6.2.1 SÉCURITÉ DE L'ORGANISATION ET SÉCURITÉ ADMINISTRATIVE

Un examen de la description de poste de l'agent ou l'agente de sécurité du ministère (ASM) confirme qu'un lien a maintenant été établi entre celui-ci et la sécurité informatique. De plus, les descriptions de travail du personnel-clé responsable de la gestion de la sécurité à la Commission, tel que le directeur général, Direction de la technologie de l'information (DTI), le gestionnaire, Services technologiques, DTI, et le directeur, Administration, de la Direction des Finances et de l'Administration indiquent que les responsabilités de la gestion de la sécurité ont maintenant été définies. Un administrateur pour chaque réseau local a également été nommé en fonction d'une liste fournie par le gestionnaire, Services technologiques, DTI (recommandations 1 et 2).

Une politique officielle sur la sécurité a été promulguée par la Division de l'administration (recommandation 3). La section 3.1.3 de cette politique traite des énoncés de la sensibilité pour toutes les applications traitées sur le réseau de la CFP (recommandation 4a). Cependant, on n'y trouve aucun énoncé de classification indiquant le niveau de confidentialité maximum pouvant être accepté par le réseau de la CFP (recommandation 4b). Il se peut qu'un tel énoncé ait été diffusé antérieurement au personnel de la CFP peu de temps après l'examen fait en 1996 par l'EIES. Le gestionnaire, Services technologiques, DTI convient qu'un énoncé rappelant aux utilisatrices et utilisateurs de la CFP et au personnel contractuel le niveau de confidentialité qui peut être accueilli sur le réseau de la CFP pourrait être publié à nouveau.

Le guide de classification et de désignation a été mis à jour et on a défini trois niveaux d'information désignée : A, B et C (suggestions 1 et 2).

On a instauré un mécanisme de contrôle pour s'assurer que les contrats de services, y compris les contrats pour les services et l'équipement de TI, contiennent des renseignements détaillés sur les exigences en matière de sécurité relatives à l'information appartenant à la CFP. L'intranet de la CFP permet aux gestionnaires d'utiliser un contrat générique pour l'achat de services. L'article 21 de ce contrat générique contient de l'information détaillée se rapportant aux exigences en matière de sécurité. Tous les contrats doivent être revus par une agente ou un agent chargé des contrats de la Division des services administratifs avant d'être approuvés (recommandations 5 et 6).

Le gestionnaire, Services technologiques, DTI a indiqué que, même si une évaluation de la menace et des risques (EMR) a été faite pour les systèmes d'information sur les cadres de direction de la CFP, le 13 mai 2000, on n'a pas fait d'EMR pour tous les systèmes de la CFP. La section 3.1.4 de la politique sur la sécurité de la CFP traite de l'obligation d'avoir un examen annuel de l'EMR (recommandation 7). On n'a pas créé de tableau récapitulatif indiquant le niveau de priorité, la date à laquelle on prévoit compléter le travail et des remarques permettant de mesurer les progrès dans ce domaine (suggestion 3).

Lorsqu'ils entrent en communication avec le réseau de la CFP, les utilisatrices et utilisateurs sont informés des règles et règlements se rapportant à l'accès et à l'utilisation des ressources du réseau. En outre, les énoncés de politique exposés dans la section 3 de la politique sur la sécurité de la CFP fournissent de l'information additionnelle relativement à ces règles et règlements (recommandation 8).

En ce qui a trait aux incidents compromettant la sécurité, la section G de la politique sur la sécurité (intitulée « Glossaire ») clarifie maintenant, en termes génériques, ce qui constitue un tel incident et mentionne à qui il faut faire rapport de ces incidents (recommandation 9).

La CFP n'a pas fait d'examen annuel de la sécurité et n'a pas de plan de reprise des activités (PRA) ajusté ou mis à jour chaque année (recommandations 10 et 11). Le gestionnaire, Services technologiques, DTI nous a informés qu'un examen annuel de la sécurité devra être fait durant l'exercice 2001-2002 et que la haute direction de la CFP reconnaît maintenant la nécessité de mettre à jour le PRA.

Recommandations complémentaires :

Les recommandations ci-après contenues dans le rapport présenté par l'EIES de la GRC en 1996 se rapportent à la gestion organisationnelle et à

la sécurité administrative. Elles n'ont toujours pas été appliquées et il faudrait leur donner suite :

(a) nouvelle publication d'un énoncé à l'intention des utilisatrices et utilisateurs de la CFP pour leur rappeler le niveau de confidentialité maximum possible sur le réseau de la CFP (recommandation 4b);

(b) conduite d'une évaluation de la menace et des risques (EMR) portant sur tous les systèmes de la CFP (recommandation 7);

(c) conduite de l'examen annuel de la sécurité pour l'exercice 2000-2001 (recommandation 10); et

(d) mise à jour et ajustement, au besoin, du plan de reprise des activités le plus récent (recommandation 11).

Consulter la rubrique « Sécurité de l'organisation et sécurité administrative » du tableau « Recommandations complémentaires et réponse de la direction » à la page 14.

6.2.2 SÉCURITÉ DU PERSONNEL

La CFP a mis en oeuvre un programme de sensibilisation à la sécurité pour les nouveaux membres du personnel en distribuant une trousse d'orientation sur la sécurité. La DTI réalise en outre une publication paraissant aux deux semaines intitulée « Trucs et conseils » pouvant servir à guider les nouveaux utilisateurs et les nouvelles utilisatrices dans l'utilisation des outils de CFPNet. La recommandation 12 du rapport de l'EIES exige que les administrateurs et administratrices du réseau local reçoivent de la formation plus poussée sur la sécurité à la fois en ce qui a trait à l'utilisation du système et les procédures de sécurité traitant des rapports et du traitement des incidents compromettant la sécurité et, également, en ce qui concerne l'observation de la politique. Suite aux entrevues avec le gestionnaire, Services technologiques, DTI, tous les administrateurs et toutes les administratrices du réseau local reçoivent une formation périodique à la fois sous forme de cours offerts régulièrement par la GRC et dans le cadre de leur travail. De l'information additionnelle sur la façon dont les incidents compromettant la sécurité doivent être traités est fournie aux sections 3.1.10, 3.1.11 et 3.1.12 de la politique sur la sécurité (recommandation 12).

Recommandations complémentaires :

Aucune.

6.2.3 SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

Une inspection matérielle des installations de la salle des ordinateurs (P100) a été entreprise et toutes les recommandations contenues dans le rapport présenté par l'EIES de la GRC en 1996 ont été prises en compte. À titre d'exemple, les boutons de coupure de courant ont été marqués, un plan de sécurité-incendie est affiché sur plusieurs murs, les extincteurs sont vérifiés périodiquement et des dispositifs de relèvement du plancher ont été installés à chacune des portes d'évacuation de la pièce P100. Les membres du personnel de la salle des ordinateurs ayant été relocalisés au 14e étage, les recommandations se rapportant à la formation du personnel en matière d'utilisation des extincteurs (recommandations 15 et 16) ne s'appliquent plus. Un système de surveillance est en place; il relie la pièce de la salle de l'ordinateur/serveur au poste de travail du commissionnaire au rez-de-chaussée en cas d'incendie ou d'accès non autorisé. Les bandes de sauvegarde sont maintenant entreposées à divers endroits hors du site et les sections 3.4.7 et 3.4.8 de la politique sur la sécurité traitent maintenant de l'élimination des supports informatiques (recommandations 13, 14, 15, 16, 17, 18, 19 et 20).

Recommandations complémentaires :

Aucune.

6.2.4 SÉCURITÉ TECHNIQUE

Comme il a été noté précédemment dans la section 4.0 de ce rapport de suivi, la CFP a actualisé la configuration du matériel et des logiciels du réseau (recommandation 21).

Le chef, Services des contrats et gestion du matériel, a fourni une liste (datée du 17 octobre 2000) du matériel et de l'équipement de communications ainsi que des services du réseau local dont on a fait l'inventaire récemment (recommandation 22). Le logiciel Basset Pro est utilisé actuellement pour aider le personnel à rassembler et à maintenir les stocks de matériel et l'équipement de communications (suggestion 4).

En ce qui concerne l'accès au système et l'autorisation, la Direction de la technologie de l'information utilise un ensemble de tableaux d'autorisations à trois paliers qui expose les privilèges d'accès précis pour divers groupes d'utilisateurs et d'utilisatrices en ce qui a trait à l'autorisation, la création, la modification et l'annulation du contrôle d'accès. La

plupart des utilisateurs et utilisatrices se font donner un mot de passe à six caractères plutôt qu'un formulaire de compte et d'accès à compléter qui avait été recommandé dans le rapport présenté par l'EIES de la GRC en 1996 . Les mots de passe des utilisateurs et utilisatrices sont conçus de manière à n'être connus que de l'utilisatrice autorisée ou de l'utilisateur autorisé; ils sont changés tous les 60 jours et, quand ils ont été utilisés une fois, ne peuvent l'être de nouveau. Ces mots de passe ne peuvent faire l'objet d'aucun autre processus de connexion automatique (recommandations 23, 24 et 25).

Certains analystes techniques au sein de la DTI ont des privilèges de contrôle d'accès spéciaux pour les fonctions de gestion des systèmes ou des applications. On leur a attribué des mots de passe uniques plus longs et plus complexes que les mots de passe à six caractères ordinaires (recommandation 26).

L'administration du contrôle d'accès se fait en un endroit central au moyen de CFPNet (suggestion 5). Cependant, la suggestion d'utiliser un mot de passe généré par l'ordinateur que l'on peut trouver dans le Bulletin de la GRC n'est plus pertinente (suggestion 6).

Quand une utilisatrice autorisée ou un utilisateur autorisé entre en communication avec le réseau de la CFP, le message d'accueil a été modifié afin que le mot de bienvenue soit enlevé (recommandation 27).

Les énoncés de politiques reliés aux opérations informatiques se trouvent à la section 3.7.5 du manuel de politiques de la CFP. Cependant, les procédures d'opération détaillées couvrant des activités telles que l'expurgation des supports effaçables, le contrôle de l'entretien à distance, le transfert de la maintenance opérationnelle, l'analyseur de réseau local pour le dépannage du réseau, le rapport sur les incidents compromettant la sécurité, etc. n'ont pas été documentées complètement. Le ou la titulaire d'un nouveau poste au sein de la section Architecture et normes de la DTI, celui d' « analyste de gestion », se verra assigner des responsabilités pour le développement et la documentation des procédures d'exploitation (recommandation 28).

Trois niveaux de désignation de sécurité ont été établis en vertu des sections 4 et 5 du *Guide de désignation et de classification des renseignements.* Les exigences pour marquer l'information de nature délicate et pour déclassifier et déclasser l'information délicate sont exposées aux sections 6 et 8 respectivement. Suite à la visite qui a été faite dans la salle des ordinateurs (pièce P100), la désignation de sécurité a été inscrite sur les caisses et les contenants conservés en entreposage (recommandation 29).

Au moment où ce suivi a lieu, les fonctions de gestion des problèmes exposant des activités telles que l'établissement de rapports, l'enregistrement, le suivi et la résolution de problèmes reliés à la sécurité n'ont pas fondamentalement été examinées, mises à jour et documentées (recommandation 30 et suggestion 7).

En outre, les processus de contrôle du changement, y compris la définition des responsabilités et le contrôle des activités de maintenance et des changements dans la configuration, ne sont pas tous réalisés. Comme on l'a noté ci-dessus, le ou la titulaire du nouveau poste d'« analyste de gestion » au sein de la section Architecture et normes de la DTI, aura la responsabilité du développement et de la documentation de ces procédures (recommandation 31)

En ce qui a trait aux incidents compromettant la sécurité, la responsabilité de revoir le journal d'exploitation et le journal portant sur la sécurité ainsi que le coupe-feu Borderware a été attribuée à deux analystes techniques principaux de la DTI (recommandations 32b et 32c). Cependant, les activités eu égard à ce qui est considéré comme un incident compromettant la sécurité à la CFP — même si elles sont largement définies dans la section G de la politique sur la sécurité de la CFP — n'ont pas été documentées. De ce fait, ces activités ne répondent pas aux exigences minimales qui ont été énumérées dans le rapport de 1996 de l'EIES (recommandation 32a).

Dans le cadre de la recommandation 10, la section 6.2.1 du présent rapport traitait de la nécessité de faire un examen annuel de la sécurité. Si l'on se place du point de vue du matériel, des communications et des opérations, les activités qui doivent avoir lieu dans le cadre d'un examen annuel de la sécurité n'ont toujours pas été entreprises (recommandation 33).

Également, comme on le note à la section 6.2.1 de ce rapport de suivi, on a effectué le 13 mai 2000 une évaluation de la menace et des risques (EMR) pour le Système d'information sur les cadres de direction de la CFP. Cependant, on n'a pas réalisé d'EMR pour tous les systèmes en usage à la CFP (recommandation 34).

La section 3.5 de la politique sur la sécurité de la CFP insiste sur la nécessité d'avoir des plans des mesures d'urgence. Les données opérationnelles et le matériel essentiels sont actuellement conservés à un endroit à l'extérieur des locaux et on est actuellement à faire l'inventaire de ces données et de ce matériel (recommandation 35).

Recommandations complémentaires :

Les recommandations ci-après contenues dans le rapport présenté par l'EIES de la GRC en 1996 relativement à la sécurité technique n'ont toujours pas été appliquées et il faudrait leur donner suite :

(a) exécution des procédures courantes, y compris l'expurgation des supports effaçables, le contrôle de la maintenance à distance, le transfert de la maintenance opérationnelle, l'utilisation de l'analyseur de réseau local pour le dépannage du réseau de la CFP et l'établissement de rapports sur les incidents compromettant la sécurité (recommandation 28);

(b) documentation des processus de gestion visant à inclure les rapports, l'enregistrement, le suivi et la résolution de problèmes et d'incidents reliés à la sécurité (recommandation 30);

(c) définition détaillée de ce qui constitue un incident compromettant la sécurité (recommandation 32a);

(d) détermination et documentation des activités à entreprendre dans le cadre d'un examen annuel de la sécurité (recommandation 33); et

(e) réalisation d'une évaluation de la menace et des risques (EMR) portant sur tous les systèmes de la CFP (recommandation 34).

Consulter la rubrique « Sécurité technique » du tableau «Recommandations complémentaires et réponse de la direction » à la page 15.

6.2.5 SÉCURITÉ DES LOGICIELS

La responsabilité à l'égard du maintien du stock de logiciels est documentée dans la liste des fonctions contenues dans la description de travail du gestionnaire, Services techniques, DTI (recommandation 36a). En outre, un inventaire des logiciels et des données ainsi que des logiciels des systèmes, des logiciels de bases de données, des logiciels d'application et des logiciels de contrôle de l'accès a été complété il y a un an avant le début du nouveau millénaire (recommandations 36b et 36c).

La nécessité de faire un examen annuel de la sécurité au sein de la CFP est mentionnée au préalable à la section 6.2.1 de ce rapport dans le cadre de la recommandation 10. En

outre, conformément à la recommandation 33, la nécessité de définir certaines activités dans le cadre de l'examen annuel de la sécurité du matériel et de l'équipement de communications est mentionnée à la section 6.2.4. En ce qui concerne la sécurité des logiciels, aucune activité n'a été définie relativement à la conduite d'un examen annuel (recommandation 37).

L'identification des logiciels de la CFP contenant de l'information privilégiée est maintenant terminée (recommandation 38). L'utilisation de ces logiciels, tels que les programmes et les produits utilisés pour la maintenance des bases de données, est maintenant restreinte à plusieurs analystes techniques qui travaillent au sein de la DTI. De plus, l'accès à un utilitaire ou à un programme, tels que les serveurs de réseau ou les programmes de bases de données, est restreint en fonction des besoins qu'en ont ces analystes pour exercer leurs fonctions (recommandations 44 et 45).

Parmi les méthodes les plus récentes de développement des systèmes et de cycle de vie en usage à la CFP, il y a la méthode « Rational Uniform Process - RUP », un produit de la compagnie Rational. Cette méthode a été recommandée par le Conseil du Trésor et d'autres ministères du gouvernement fédéral l'utilisent (recommandation 39).

L'exigence de signaler au coordonnateur ou à la coordonnatrice de la sécurité les problèmes relatifs aux logiciels ou aux données a été identifiée dans la description de poste du gestionnaire, Services technologiques, DTI (recommandation 40).

Le regroupement des responsabilités en ce qui a trait à la surveillance de la bibliothèque de logiciels dans un secteur de responsabilité et l'utilisation d'une bibliothèque de logiciels commune n'a jamais été entrepris (suggestion 8).

Au moment de son examen en 1996, l'EIES de la GRC avait noté que les fonctions d'un poste alors vacant portaient sur l'assurance de la qualité et l'essai des systèmes et les essais pour utilisateurs et utilisatrices. On considérait alors que l'assurance de la qualité et les essais constituaient des fonctions distinctes de celles du développement des applications, des essais et de la mise en oeuvre en direct. Actuellement, quand une nouvelle application est élaborée à la CFP, elle est entièrement testée par le personnel au sein de la section des Applications, DTI, avant d'être mise en ligne par les Services technologiques, DTI (recommandation 41).

À l'heure actuelle, la DTI ne met pas mis fin automatiquement à la séance de travail d'un utilisateur inactif ou d'une utilisatrice inactive et cette personne n'a pas à se faire réauthentifier par le système de la CFP après une période prédéfinie d'inactivité

(recommandation 42).

Les Services technologiques de la DTI supervisent l'utilisation de l'Internet ainsi que du couvre-feu Borderware sur une base de 24 heures par jour. Cependant, d'autres applications de systèmes, le courrier électronique par exemple, ne sont surveillées que périodiquement. Les activités précises couvrant la surveillance des systèmes et les mécanismes de protection, y compris les activités qui constituent un incident compromettant la sécurité , n'ont pas été documentées. Comme on l'a noté ci-dessus, un nouveau poste au sein de la section de l'Architecture et des normes (celui d' « analyste de gestion ») se verra assigner des responsabilités pour le développement et la documentation de ces activités (recommandation 43).

Recommandations complémentaires :

Les recommandations ci-après déjà contenues dans le rapport présenté par l'EIES de la GRC en 1996 ont trait à la sécurité des logiciels. Elles n'ont toujours pas été appliquées et il faudrait leur donner suite :

(a) détermination et documentation des activités à entreprendre dans le cadre d'un examen annuel de la sécurité (recommandation 37);

(b) terminaison automatique de la séance de travail d'un utilisateur ou d'une utilisatrice, ou l'obligation pour cette personne de se réauthentifier après l'expiration d'une période d'inactivité prédéfinie (recommandation 42); et

(c) documentation des activités de surveillance des systèmes incluant les activités qui constituent des incidents compromettant la sécurité (recommandation 43).

Consulter la rubrique « Sécurité des logiciels » du tableau « Recommandations complémentaires et réponse de la direction » à la page 16.

7.0 RECOMMANDATIONS COMPLÉMENTAIRES ET RÉPONSE DE LA DIRECTION		
Recommandations complémentaires	**Responsabilité**	**Réponse de la direction et plan d'action**
Sécurité de l'organisation et sécurité administrative *(a) nouvelle publication d'un énoncé s'adressant aux utilisateurs et utilisatrices du niveau de sensibilité maximum qui peut être supporté par le réseau de la CFP (recommandation 4b);*	Directeur général, Technologie de l'information	(a) La politique actuelle de la CFP en matière de sécurité, élaborée après la vérification de 1996 de l'EIES, contient des renseignements sur la classification et la désignation de sécurité. Les Services de sécurité de la CFP sont en train d'élaborer une série de séances de sensibilisation à la sécurité qui auront lieu régulièrement. Ces séances auront pour but de sensibiliser les employés et employées de la CFP à la classification et la désignation de sécurité. ***Date cible : le 31 août 2001***
(b) conduite d'une évaluation de la menace et des risques (EMR) couvrant tous les systèmes de la CFP (recommandation 7);		(b) Plusieurs EMR de systèmes d'applications (SIEx, SSIR, ELS, RP) ont été réalisées depuis la vérification de 1996 de l'EIES. D'autres EMR distinctes seront effectuées pour les nouveaux systèmes d'application et seront financées dans le cadre du cycle normal de développement. ***Date cible : en cours*** Toutefois, une EMR pour l'infrastructure de réseau et l'Internet est requise. Une demande de financement général d'environ 50 000 $ sera faite à la mi-exercice pour cette initiative. ***Date cible : selon le financement***
(c) conduite de l'examen annuel prévu de la sécurité pour l'exercice 2001-2002 recommandation 10); et		(c) L'environnement de sécurité de la CFP est très stable et nous n'avons pas eu d'incidents importants sur ce plan. Par conséquent, on ne croit pas qu'il y ait lieu d'effectuer un examen annuel de la sécurité. Toutefois, conformément à la politique gouvernementale en matière de sécurité, on recommande qu'un examen de la sécurité ait lieu tous les cinq ans. ***Date cible : mi-2002***

Recommandations complémentaires	Responsabilité	Réponse de la direction et plan d'action
(d) mise à jour et ajustement au besoin, du plus récent plan de reprise des activités (recommandation 11).	Directeur général, Finances et administration	(d) Cette question a été étudiée (DTI et DFA) et la recommandation reçoit le plein soutien des deux groupes. La portée du plan de reprise des activités sera revue et des options seront identifiées, tout comme les répercussions financières. ***Date cible : le 31 mars 2002***
Sécurité technique	Directeur général, Technologie de l'information	
(a) procédures courantes comprenant l'expurgation des médias effaçables, le contrôle de la maintenance à distance, le transfert de la maintenance opérationnelle, le recours à l'analyseur de réseau local aux fins du dépannage du réseau de la CFP et le signalement des incidents compromettant la sécurité (recommandation 28);		(a) Ces activités sont réalisées en grande partie dans le cadre des opérations quotidiennes normales de la DTI. Cependant, elles n'ont pas été documentées officiellement. La Division des services de technologie de la DTI est en train de préparer un manuel d'exploitation qui énumérera les procédures courantes. ***Date cible : le 26 octobre 2001***
(b) documentation des processus de gestion incluant le rapport, l'enregistrement, le suivi et la résolution des problèmes et incidents compromettant la sécurité (recommandation 30);		(b) Cette activité est incorporée dans l'activité (a) ci-dessus.
(c) définition plus détaillée de ce qui constitue un incident compromettant la sécurité (recommandation 32a);		(c) Cette activité est incorporée dans l'activité (a) ci-dessus.
(d) détermination et documentation des activités qui doivent être entreprises dans le cadre d'un examen annuel de la sécurité (recommandation 33); et		(d) Cette activité est incorporée dans l'activité (c) sous la rubrique Sécurité de l'organisation et sécurité administrative.

Recommandations complémentaires	Responsabilité	Réponse de la direction et plan d'action
(e) réalisation d'une évaluation de la menace et des risques (EMR) couvrant tous les systèmes de la CFP (recommandation 34).		(e) Cette activité est incorporée dans l'activité (b) sous la rubrique Sécurité de l'organisation et sécurité administrative.
Sécurité des logiciels	Directeur général, Technologie de l'information	
(a) détermination et documentation des activités qui doivent être entreprises dans le cadre de l'examen annuel de la sécurité (recommandation 37);		(a) Cette activité est incorporée dans l'activité (c) sous la rubrique Sécurité de l'organisation et sécurité administrative.
(b) terminaison automatique de la séance d'un utilisateur ou d'une utilisatrice, ou obligation pour cette personne de se réauthentifier après l'expiration d'une période prédéfinie d'inactivité (recommandation 42); et		(b) On peut mettre terme automatiquement aux séances des utilisateurs et utilisatrices après une certaine période d'inactivité. Toutefois, les fichiers ou documents ouverts ne sont pas sauvegardés automatiquement. Il n'est pas recommandé d'aller de l'avant avec cette recommandation de l'EIES en raison de la perte possible de données. Comme solution de rechange, on pourrait utiliser un économiseur d'écran qui bloque efficacement l'accès au poste de travail pour protéger l'ordinateur pendant que l'utilisateur ou l'utilisatrice n'est pas à son bureau. ***Date cible : le 31 août 2001***
(c) documentation des activités de surveillance des systèmes y compris des activités qui constituent un incident compromettant la sécurité (recommandation 43).		(c) Cette activité est incorporée dans l'activité (a) sous la rubrique Sécurité technique.